DISCUSSION PAPER ON METHODOLOGICAL PRINCIPLES OF INSURANCE STRESS TESTING

CYBER COMPONENT

EIOPA-BoS-22/514
24 November 2022

European Insurance and
Occupational Pensions Authority

RESPONDING TO THIS PAPER

EIOPA welcomes comments on the "Discussion Paper on Methodological principles of insurance stress testing – Cyber component".

Comments are most helpful if they:

- respond to the question stated, where applicable;
- contain a clear rationale; and
- describe any alternatives EIOPA should consider.

Please send your comments to EIOPA in the provided Template for Comments, by email to <eiopa.stress.test@eiopa.europa.eu> by 28 February 2023.

Contributions not provided in the template for comments, or sent to a different email address, or after the deadline, will not be considered.

PUBLICATION OF RESPONSES

Your responses will be published on the EIOPA website unless: you request to treat them confidentially, or they are unlawful, or they would infringe the rights of any third-party. Please, indicate clearly and prominently in your submission any part you do not wish to be publicly disclosed. EIOPA may also publish a summary of the survey input received on its website.

Please note that EIOPA is subject to Regulation (EC) No 1049/2001 regarding public access to documents[1] and EIOPA's rules on public access to documents[2].

Declaration by the contributor

By sending your contribution to EIOPA you consent to publication of all information in your contribution in whole/in part – as indicated in your responses, including to the publication of the name of your organisation, and you thereby declare that nothing within your response is unlawful or would infringe the rights of any third party in a manner that would prevent the publication.

DATA PROTECTION

Please note that, if personal data are processed (such as contact details including the name of individuals, email addresses and phone numbers), these will not be published. They will only be used by EIOPA to request clarifications, if necessary, on the information supplied. EIOPA, as a

[1] Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (OJ L 145, 31.5.2001, p. 43).
[2] Decision of the Management Board of 20 October 2021 concerning public access to documents (EIOPA-MB-11/051-Rev 1).

European Authority, processes personal data in line with Regulation (EU) 2018/1725[3] on the protection of the individuals with regards to the processing of personal data by the Union institutions and bodies and on the free movement of such data. More information on data protection can be found at https://eiopa.europa.eu/ under the heading 'Legal notice'.

[3] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS

BAU	Business as usual
BI	Business Interruption
BS	Balance sheet
BUS	Bottom-up Survey
CBI	Contingent Business Interruption
CCP	Central Counterparty
CEO	Chief Executive Officer
CRO	Chief Risk Officer
D&O	Director's and Officer's
DORA	Digital Operational Resilience Act
DoS	Denial of Service
E&O	Errors and omissions
EIOPA	European Insurance and Occupational Pensions Authority
ENISA	European Union Agency for Cybersecurity
ESAs	European Supervisory Authorities
ESRB	European Systemic Risk Board
EU	European Union
EUR	Euro
EU-SCICF	pan-European Systemic Cyber Incident Coordination Framework
FSB	Financial Stability Board
GDPR	General Data Protection Regulation
GIMAR	Global Insurance Market Report
GME	Global Monitoring Exercise
GTPL	General Third Party Liability
GWP	Gross Written Premiums
IAIS	International Association of Insurance Supervisors
ICT	Information and Communication Technology
IT	Information Technology
NACE	Statistical Classification of Economic Activities in the European Community
NBB	National Bank of Belgium
NCA	National Competent Authority
OECD	Organisation for Economic Co-operation and Development
OF	Own Funds
ORSA	Own Risk and Solvency Assessment
P&L	Profit and loss
PaaS	Platform as a Service
PI	Professional Indemnity
PRA	Bank of England Prudential Regulation Authority
QRT	Quantitative Reporting Templates
RDP	Remote Desktop Protocol
SaaS	Software as a Service
SCR	Solvency Capital Requirement
SII	Solvency II
ST	Stress Test
TA	Total Assets
TP	Technical Provisions

UL	Unit-linked and index-linked
USD	US Dollar

1 INTRODUCTION

1. Stress testing, in its bottom-up form, almost since the establishment of EIOPA, became a key tool for the assessment of the vulnerability of the European insurance sector.[4] In the fulfilment of its mandate, EIOPA regularly runs and evolves its bottom up stress test framework building on the experience gained from past exercises, the contribution of its stakeholders and the analysis of the best practices implemented by other supervisors, financial institutions and standard setting bodies.
2. In its strive for continuous improvement, EIOPA published in the last three years two discussion papers[5] whose content benefitted from the contribution of the insurance industry, actuarial associations and insurance associations, and generated three methodological papers[6] that were used to design and operationalize the regular EU wide stress test exercises.
3. These papers aim at enhancing and strengthening by a technical and procedural perspective the EIOPA approach to bottom-up stress testing. As such, the information therein should not be considered as fully-fledged technical specifications for a stress test exercise, but rather as a reference to guide the design of future stress tests. Scenarios, shocks and their applications, data collected, will be inspired, but not limited, by the methodological papers according to the objective(s) and scope of each specific exercise.
4. This paper is the third discussion paper of the series and contains the set of theoretical and practical rules, guidelines and approaches to support the design phase of potential future insurance stress tests with a focus on cyber risk.
5. As shown in the EIOPA July 2022 Risk Dashboard, digitalisation and cyber risks have become one of the most important risks for the European insurance sector, with increasing momentum.[7]

[4] A supervisory bottom-up stress test is an exercise run by a supervisor or regulatory authority, in which participating institutions are requested to perform the calculations. The supervisor provides the stress testing framework, methodologies, adverse stress scenarios, prescribed shocks and guidance on the application of the shocks. Participants calculate the impact of the prescribed shocks on their financial position according to the guidance provided and using their own models.

[5] EIOPA (2019), Discussion paper on methodological principles of insurance stress testing. Available at: https://www.eiopa.europa.eu/sites/default/files/publications/consultations/methodological_principle_of_insurance_stress_testing.pdf. EIOPA (2020), Second Discussion Paper on Methodological Principles of Insurance Stress Testing. Available at: https://www.eiopa.europa.eu/content/second-discussion-paper-methodological-principles-insurance-stress-testing_en.

[6] EIOPA (2020) Methodological principles of insurance stress testing. Available at: https://www.eiopa.europa.eu/document-library/methodology/methodological-principles-of-insurance-stress-testing_en?source=search. EIOPA (2021), Methodological principles of insurance stress testing liquidity component. Available at: https://www.eiopa.europa.eu/sites/default/files/financial_stability/insurance_stress_test/methodological-principles-liquidity.pdf. EIOPA (2022), Methodological principles of insurance stress testing – climate change component. Available at: https://www.eiopa.europa.eu/sites/default/files/financial_stability/insurance_stress_test/methodological_principles_of_insurance_stress_testing_-_climate_change_component.pdf.

[7] EIOPA Risk Dashboard July 2022. Available at: https://www.eiopa.europa.eu/sites/default/files/financial_stability/risk_dashboard/july_2022_risk_dashboard.pdf.

These risks have been at high level since January 2022 and this risk level equates only to macro and market risks.

6. Furthermore, as outlined in the EIOPA June 2022 Financial Stability Report, the results of the EIOPA Spring 2022 insurance bottom-up survey (BUS) among supervisors show digitalisation and cyber risks ranking in the third place in terms of materiality, after market and macro risks, but above e.g. credit and profitability and solvency risks.[8] This represents an increase in materiality when compared to the EIOPA Autumn 2021 BUS, which ranked digitalisation and cyber risks in the fifth place. When considering the expected developments in terms of risk materiality over the next year, digitalisation and cyber risks are ranked second, behind macro risks.
7. Cyber security risks are seen as the main driver of the developments in digitalisation and cyber risks (92% of supervisors), followed by cyber underwriting risks (4%). Several supervisors associate the current war between Russia and Ukraine and resulting uncertainty to a potential increase in cyber risks. This adds to an already higher vulnerability of the sector during the Covid-19 pandemic due to an increased reliance on remote work and on digital solutions and infrastructure.
8. Cyber risk is receiving increasing attention by European and global regulators and standard setting bodies over the last two years. The IMF has identified cyber risk as a key threat to financial stability.[9] It estimates that the number of cyberattacks has tripled over the last decade, with financial services being the most affected industry due to the increased digitalisation of its business models. The Covid-19 crisis has accentuated the importance of cyber risk to financial institutions due to the increasing reliance on digital infrastructures and teleworking.
9. Cyber risk has also been chosen by the IAIS and insurance supervisors worldwide as one of the three macroprudential topics to be included in the 2021 collective discussion on systemic risk.[10] As an outcome, it was agreed that in 2022 the IAIS will carry out a special topic on cyber risk as part of their Global Insurance Market Report (GIMAR).
10. In 2020, the European Commission adopted a digital finance package, including a legislative proposal for an EU regulatory framework on digital operational resilience to prevent and mitigate cyber threats in the financial sector (DORA).[11] This proposal aims at filling up a gap left after the regulatory reform that followed the 2008 financial crisis which focused primarily on

[8] EIOPA Financial Stability Report June 2022. Available at: https://www.eiopa.europa.eu/document-library/financial-stability-report/financial-stability-report-june-2022.

[9] Cyber Risk is the New Threat to Financial Stability, Elliott J. and Jenkinson N., IMF, December 2020. Available at: https://blogs.imf.org/2020/12/07/cyber-risk-is-the-new-threat-to-financial-stability/?utm_medium=email&utm_source=govdelivery.

[10] IAIS Global Insurance Market Report (GIMAR) 2021. Available at: https://www.iaisweb.org/uploads/2022/01/211130-IAIS-GIMAR-2021.pdf.

[11] Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014. Final compromise text available at: https://data.consilium.europa.eu/doc/document/ST-10581-2022-INIT/en/pdf.

strengthening financial resilience, leaving ICT risks and their potential detrimental effect on the stability of the EU financial system partly unaddressed.

11. The DORA proposal entails a set of requirements on ICT risk management to be applied by financial entities in the EU. These include requirements on digital operational resilience testing that shall be applied proportionately, i.e. all entities should perform a periodic testing of ICT tools and systems, with advanced testing based on threat-led penetration testing (TLPT) required only for significant entities.[12] The development of such operational resilience testing is out of the scope of this paper.
12. Taking into account the potential systemic risks entailed by the increased outsourcing practices and by the ICT third-party concentration, the Commission's proposal also allocates to the ESAs the responsibility of periodically identifying the ICT third-party service providers that are critical for financial entities. This assessment should be performed based on a set of criteria that include the systemic impact of a large scale operational failure of the third-party provider, the systemic nature of the financial entities relying on the third-party provider and the relevance of the provider for the performance of critical or important functions.
13. Moreover, the ESAs are also encouraged to establish mechanisms to enable the sharing of effective practices across financial sectors to enhance situational awareness and identify common cyber vulnerabilities and risks across-sectors, including through the development of crisis management and contingency exercises involving cyber-attack scenarios. The ESAs, the ECB and competent authorities are also urged to work together to develop and promote best practices.
14. The ESRB recently published a report titled "Mitigating systemic cyber risk" calling for a review of the macroprudential framework with a view to developing capabilities needed to mitigate the risk of financial instability in the event of a systemic cyber incident.[13] In particular, this report identifies the need for a pan-European systemic cyber incident coordination framework (EU-SCICF) to overcome the risk to financial stability stemming from a coordination failure during the response to a systemic cyber crisis. The report also calls for the development of an analytical framework and monitoring indicators, including systemic cyber resilience scenario stress testing. The latter can be designed as a tool that assesses the financial system's operational capability to absorb a severe but plausible cyber incident scenario. An example is the Bank of England Prudential Regulation Authority's (PRA's) cyber stress test framework.[14]

[12] The DORA proposal defines threat led penetration testing as "a framework that mimics the tactics, techniques and procedures of real-life threat actors perceived as posing a genuine cyber threat, that delivers a controlled, bespoke, intelligence-led (red team) test of the entity's critical live production systems".

[13] ESRB (2022), Mitigating systemic cyber risk. Available at: https://www.esrb.europa.eu/pub/pdf/reports/esrb.SystemiCyberRisk.220127~b6655fa027.en.pdf?bd2b11e760cff336f84c983133dd23dc.

[14] The PRA cyber stress test framework aims to assess institutions' capability to operationally absorb a cyber incident within a defined timeframe and to continue services without material economic impact (tolerance for disruption). In 2022, the PRA will be carrying out a cyber stress test of its retail payment system involving a scenario where data integrity is compromised. Source: PRA (2021), Statement

15. So far, there seems to be limited experience with conducting standard bottom-up stress tests with a focus on cyber risk aimed at the supervisory assessment of the financial impact of adverse cyber scenarios. Work in this area seems to be more advanced with regards to the assessment of cyber underwriting risk, with at least three institutions having included cyber underwriting scenarios in their insurance stress tests (the PRA, the National Bank of Belgium (NBB) and the Singapore Monetary Authority (MAS)).[15] In 2016, the MAS included a cyber risk scenario in its industry-wide stress test, which assessed the combined effects of a disruption in insurers' own operations and claims from underwritten cyber policies arising from a cyber attack.
16. This paper aims to set the ground for an assessment of insurers' resilience under severe but plausible cyber incident scenarios, focusing mostly on the financial consequences of such scenarios.[16] It elaborates on two main aspects:

    - The **cyber resilience**, intended as the capability of an insurance undertaking to sustain the financial effect of an adverse cyber-event. The economic impacts should be informed by more operational oriented data on a firm's capability to restore its operations at a sufficient level and in a time horizon which do not generate potential systemic effects on the financial sector and eventually to the real economy;
    - The **cyber underwriting risk**, intended as the capability of an insurance undertaking to sustain the financial impact by a capital and solvency perspective of the materialization of an extreme but plausible adverse cyber scenario impacting the insurance coverages contained in the liability portfolios.

17. The paper does not cover the design of the threat-led penetration tests envisaged in DORA nor of other similar initiatives aimed at finding and exploiting vulnerabilities in the systems supporting the critical functions and services of an entity. It also does not cover the development of the crisis management and contingency exercises allocated to the ESAs by the DORA proposal. The paper is nonetheless inspired by relevant regulation and supervisory experience in these areas.
18. The purpose of this work is three-fold. At first it aims at setting the stage for a discussion on the assessment of the exposure of insurers towards cyber risk. Secondly, it aims at proposing the approaches to design and operationalise a cyber risk assessment in the context of the EIOPA

on the 2022 cyber stress test: Retail payment system. Available at: https://www.bankofengland.co.uk/prudential-regulation/publication/2021/december/cyber-stress-test-2022-retail-payment-system.

[15] PRA General Insurance Stress Test 2022. Available at: https://www.bankofengland.co.uk/prudential-regulation/letter/2022/may/insurance-stress-test-2022. NBB Insurance Stress Test 2022 - Cyber scenario. Available at: https://www.nbb.be/en/financial-oversight/prudential-supervision/areas-responsibility/insurance-or-reinsurance-40. IMF (2020), Cyber Risk Surveillance: A Case Study of Singapore. Available at: https://www.imf.org/en/Publications/WP/Issues/2020/02/10/Cyber-Risk-Surveillance-A-Case-Study-of-Singapore-48947.

[16] For the assessment of insurers' own cyber resilience, financial metrics are complemented by operational metrics aimed at providing context to the monetary impacts.

framework of bottom-up stress testing. The third purpose is to engage with stakeholders and collect their views and suggestions on the subject.

19. EIOPA acknowledges that cyber risk, especially due to the operational nature of its resilience component, departs from the traditional market and insurance specific risks which have been the core constituents of the EIOPA bottom-up stress test exercises. These specificities are carefully considered in all the sections of the paper, e.g. metrics and communication of the results. Hovewer, the economic nature of the impacts that the approach aims primarily at capturing, while limited to the balance sheet of the undertakings, qualifies it as a stress test.
20. The remainder of this paper is organised in 7 sections. Section 2 introduces the main concept of the cyber risk and the twofold aspects for insurers: the cyber underwriting and the cyber resilience. Section 3 presents the key assumptions underlying the design of the scenarios and the application of shocks. Section 4 elaborates on the approach to the identification of the insurers to be included in a cyber risk-based stress test exercise. Section 5 presents a set of scenarios deemed as relevant for a cyber stress test exercise. Sections 6 and 7 elaborate on the guidance for the applications of the identified scenarios both for cyber underwriting and cyber resilience. Specifically, information on the identification of the shocks and their calibration, on how to apply the prescribed shocks, on the relevant metrics to be used to measure the impacts, and on the information to be collected to assess the impacts is provided. Finally, section 8 presents some considerations on the communication of results of stress tests with a focus on cyber risk.

2 CYBER RISK FOR INSURERS

2.1 CYBER RISK: MAIN CONCEPTS

21. There is no standard definition for cyber risk. Standard setting bodies, regulators, industry and associations propose a set of definitions which differ in terms of granularity and scope.
22. The IAIS and the CRO Forum provide an overarching definition of cyber risks as "Any risks that emanate from the use of electronic data and its transmission, including technology tools such as the internet and telecommunications networks. It also encompasses physical damage that can be caused by cybersecurity incidents, fraud committed by misuse of data, any liability arising from data use, storage and transfer , and the availability, integrity, and confidentiality of electronic information – be it related to individuals, companies, or governments."[17]
23. The FSB in its Cyber lexicon operationalises this definition detailing the concept of cyber risk and its quantification "The combination of the probability of cyber incidents occurring and their impact.", where a cyber incident is qualified as "a cyber event that: i) jeopardizes the cyber security of an information system or the information the system processes, stores or transmits; or ii) violates the security policies, security procedures or acceptable use policies, whether resulting from malicious activity or not."[18]
24. The ESRB, has as main concern cyber incidents originating from malicious activity, as these are perceived as having the greatest potential to undermine confidence, but also reflects on the systemic impacts that could result from non-malicious cyber incidents.[19]
25. ENISA defines cyber incident as "Any occurrence that has impact on any of the components of the cyber space or on the functioning of the cyber space, independent if it is natural or human made; malicious or non-malicious intent; deliberate, accidental or due to incompetence; due to development or due to operational interactions. Also, any incident generated by any of cyber space components even if the damage/disruption, dysfunctionality is caused outside the cyber space interactions".[20]

[17] IAIS (2016), Issues paper on cyber risk to the insurance sector. Available at https://www.iaisweb.org/uploads/2022/01/160812-Issues-Paper-on-Cyber-Risk-to-the-Insurance-Sector_final.pdf. CRO Forum (2016), CRO Forum Concept Paper on a proposed categorisation methodology for cyber risk. Available athttps://www.thecroforum.org/wp-content/uploads/2016/06/ZRH-16-09033-P1_CRO_Forum_Cyber-Risk_web-2.pdf.

[18] FSB (2018), Cyber Lexicon. Available at: https://www.fsb.org/wp-content/uploads/P121118-1.pdf.

[19] ESRB (2020), Systemic Cyber risk. Available at: https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf.

[20] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN.

26. ENISA also defines a special category of cyber incident that is especially harmful, called cyber accident, as "as any occurrence associated with cyber space causing significant damage to cyber space or any other asset (has performance impact, requires repairs, replacement) or causing personal injury."
27. In its Guidelines on information and communication technology (ICT) security and governance, EIOPA provides a definition of ICT and security risk as a sub-component of operational risk: "the risk of loss due to breach of confidentiality, failure of integrity of systems and data, inappropriateness or unavailability of systems and data or inability to change ICT within a reasonable time and costs when the environment or business requirements change (i.e. agility).[21] This includes cyber risks as well as information security risks resulting from inadequate or failed internal processes or external events including cyber attacks or inadequate physical security."
28. The malicious nature of cyber risk is captured in the concept of cyber attack, which is defined by EIOPA as "Any type of hacking leading to an offensive/malicious attempt to destroy, expose, alter, disable, steal or gain unauthorised access to or make unauthorised use of an information asset that targets ICT systems."
29. The European Commission, in its proposal for a Digital Operational Resilience Act (DORA), defines an ICT-related incident as an unforeseen identified occurrence in the network and information systems, whether resulting from malicious activity or not, which compromises the security of network and information systems, of the information that such systems process, store or transmit, or has adverse effects on the availability, confidentiality, continuity or authenticity of financial services provided by the financial entity".[22] In this proposal, incidents "with a potentially high adverse impact on the network and information systems that support critical functions of the financial entity" are classified as major ICT-related incidents.
30. In the DORA proposal, ICT-related incidents also comprise cyber-attacks, which are defined as "a malicious ICT-related incident by means of an attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset perpetrated by any threat actor".
31. To enable a common understanding of the core concepts, it is important to lay down definitions for the terminology used in this paper. As EIOPA has already published Guidelines on information and communication technology (ICT) security and governance, the following definitions have been chosen in a consistent form and follow the school of thought that derive cyber security from information security.

[21] EIOPA (2020), Guidelines on information and communication technology security and governance. Available at: https://www.eiopa.europa.eu/document-library/guidelines/guidelines-information-and-communication-technology-security-and_en.

[22] Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014. Available at: https://data.consilium.europa.eu/doc/document/ST-11051-2020-INIT/en/pdf.

32. According to this approach, the following definitions will apply throughout this paper:[23]

- Cyber Security: Preservation of confidentiality, integrity and availability of information stored in and/or of ICT systems themselves.
- Information Security: Preservation of confidentiality, integrity and availability of information and/or information systems. In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved.
- Confidentiality: Property that information is neither made available nor disclosed to unauthorized individuals, entities, processes or systems.
- Integrity: Property of accuracy and completeness.
- Availability: Property of being accessible and usable on demand (timeliness) by an authorized entity.
- ICT System: Set of applications, services, information technology assets, hardware, software or other information-handling components, which includes the operating environment.
- Cyber Attack: Any type of hacking leading to an offensive / malicious attempt to violate the cyber security of ICT systems.
- Hacking: any act by individuals or groups who covertly gain access to a computer system in order to gather information, cause damage, etc.[24]

33. A glossary including a description of more specific cyber resilience terms is included in Annex 9.1 and is used as a reference through the remainder of the paper.

2.2 CYBER RESILIENCE: INSURERS AS DIRECT TARGETS OF CYBER ATTACKS

34. On a general level, cyber attacks can vary to a high degree in terms of motivations, perpetrators, methodologies and impact. Covering all these aspects in full would not only push the scale of this work to an unrealistic level, but also serve little purpose in deriving a sound stress testing methodology. Therefore, in order to arrive at realistic scenarios, assumptions have to be made on cyber threats relevant to the insurance sector.

[23] In this paper, the definitions of ICT and security risk and cyber risk will be used interchangeably.

[24] As defined in CRO Forum (2016), CRO Forum Concept Paper on a proposed categorisation methodology for cyber risk. Available at https://www.thecroforum.org/wp-content/uploads/2016/06/ZRH-16-09033-P1_CRO_Forum_Cyber-Risk_web-2.pdf.

2.2.1 MOTIVATION OF CYBER ATTACKS AGAINST INSURERS

35. On an abstract level, cyber attacks are capable of disrupting the confidentiality, integrity and availability of ICT systems. This can be used to achieve a number of objectives, among which the most relevant and commonly encountered are:

    - **Financial Gain**, for example through direct unauthorized transactions, stealing financial data for fraudulent activities, sale of confidential data, or extortion through threats against an entity's reputation or ICT environment (e.g. ransomware, Denial of Service (DoS).
    - **Espionage**, by compromising confidential data that is stored at the target systems, or obtaining information that can be leveraged for further subversion (e.g. for social engineering purposes).
    - **Sabotage**, can be achieved by deleting or altering sensitive data or targeting the ICT infrastructure itself, as even relatively minor interruptions of availability can have a large impact on some organizations. In extreme cases, by manipulating industrial control systems, severe damage to physical facilities has resulted from cyber attacks.

36. Of these possible motivations, all can plausibly be linked to potential attacks on insurance undertakings. However, the financial sector as a whole is overall one of the most targeted industries[25,26,27] and it is an especially good target for financial gain. Insurance undertakings, in particular, regularly handle a large amount of transactions, customer and payment data. Furthermore, they may hold very sensitive personal and even health related information on private individuals, which can be very effectively monetized in various ways by malicious actors.
37. Cyber attacks with the goal of espionage or sabotage against insurers are conceivable, but would usually only be attempted by specific actors in very specific circumstances, whereas practically any insurer is a viable target for a financially motivated attack at any time. Therefore, the latter category of attacks is most relevant for defining a broadly applicable attack scenario.
38. The possibility of sabotage might need to be re-evaluated in the future, as cyber warfare is becoming a more relevant threat in general and could be conducted by large scale application against a financial market.

2.2.2 PERPETRATORS OF CYBER ATTACKS AGAINST INSURERS

39. The categories of threat actors in the field of cyber security are closely tied to the motivations for attacking certain targets and the methods they can be expected to employ. Common and relevant threat actor profiles include:

[25] FireEye (2021), M-Trends 2021 – Special Report. Available at: https://content.fireeye.com/m-trends.
[26] ENISA (2021), ENISA Threat Landscape 2021. Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021.
[27] IMF (2020), Cyber Risk and Financial Stability: It's a Small World After All. Available at: https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2020/12/04/Cyber-Risk-and-Financial-Stability-Its-a-Small-World-After-All-48622.

- **Criminal Organizations**: These actors are usually motivated by financial gain and responsible for the majority of known cyber attacks. Their sophistication varies, but as the international volume of this criminal industry is constantly growing, so are the capabilities of organized cyber crime syndicates, who are known to field a high level of technical expertise, make use of division of labor and even specialized service providers for e.g. target information, exploits, malware packages, etc.
- **Nation-States**: Certain nation-states have invested in building up significant capabilities in the cyber field, which they have employed for espionage, acts of cyber warfare or even for securing financial gain in some cases. Nation-state associated threat actors are characterized by a very high degree of sophistication in their attacks, but usually select their targets according to a specific agenda.
- **Hacktivists**: These actors are motivated by ideology and usually seek to inflict damage on organizations they perceive to oppose this ideology. Their sophistication varies, through the nature of these actors, their targets are usually specifically selected.
- **Insiders**: The motivation of this threat actor category can vary from financial goals to sabotage for revenge in case of disgruntled ex-employees. As the defining characteristic for an inside threat is some form of pre-existing privileged access to the target environment, their ability to inflict damage is usually quite high.

40. Closely tied to the possibilities for financial gains, criminal organizations are the most relevant threat to insurance undertakings. They are capable of highly sophisticated attacks and due to their opportunistic nature they can target practically any undertaking of the financial sector without warning.
41. Nation-States can deliver extremely dangerous cyber attacks, however they are not very likely to target an insurance undertaking outside of exceptional circumstances.
42. Similarly, hacktivists might target single undertakings or groups out of various ideological reasons, but do not represent a constant threat to the whole insurance industry.
43. Insiders are a difficult category to classify, as it might encompass anything from ex-employees to contractors. However, although insiders can cause considerable damage from their trusted position and the latest "ENISA Threat Landscape" report[28] has identified the possibility of criminal organizations recruiting insiders for securing access to a target, this does not yet seem to be as widespread a threat as pure external attacks.

2.2.3 TYPES OF CYBER ATTACKS AGAINST INSURERS

44. Attackers can use a wide variety of techniques to achieve their objectives. In this sub-chapter, a combined approach is used to single out specific threats faced by European insurance undertakings. Historical data is used to focus on practically relevant techniques and the results

[28] ENISA (2021), ENISA Threat Landscape 2021. Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021.

are compared against the observations on likely motivations and perpetrators made in the sub-chapters above.

45. The "ENISA Threat Landscape 2021" is the latest in a series of annual reports dealing with trend observations on cyber-attacks on European organisations. According to this report, the nine most impactful threats for 2021 were: (i) Ransomware; (ii) Malware (generalized); (iii) Cryptojacking; (iv) E-mail related threats; (v) Threats against data (data breaches); (vi) Threats against availability and integrity (DoS); (vii) Disinformation; (viii) Non-malicious threats; and (ix) Supply-chain attacks.
46. Focusing on methods relevant to attacks by criminal organizations for financial gain, the following observations can be made:

    - Initial compromise with ransomware is often achieved by phishing E-mails or Remote Desktop Protocol (RDP) brute forcing;
    - Financial gain is achieved through various means of extortion, theft and sale of sensitive data or through Cryptojacking;
    - Leverage for extortion is often obtained through deployment of ransomware, theft of sensitive data, or DoS campaigns;
    - These methods are often combined in order to put as much pressure as possible on the target to deliver swift payment.

47. MITRE ATT&CK is a library of attack technologies, which is widely used especially in a technical context.[29] It contains a very granular list of techniques and sub-techniques categorized by various attack stages in which they are used. Also included is data on known real-world uses of these techniques by various threat-actors.
48. Focusing on the stages of initial access and final impact, the following observations can be made:

    - The most frequent vector of initial compromise is phishing by malicious E-mail attachments or links. This is followed by the use of valid credentials, which will often be obtained by social engineering techniques, also including phishing.
    - Less frequent but also known to have been used are direct attacks against web-facing applications and compromise over trusted parties or the supply chain.
    - There are fewer data points on the direct impact achieved in these cyber-attacks, but those that are available suggest a roughly even distribution between deployment of Ransomware, Cryptojacking and interruption of services.

[29] MITRE ATT&CK®. Available at: https://attack.mitre.org/. An overview of the MIRE ATT&CK database and selected information is presented in Annex 9.2.

49. When comparing the analysis of the ENISA and the MITRE ATT&CK information, common basic observations about attacker methodology relevant to the European insurance sector can be derived:

    - Ransomware, DoS, Cryptojacking and theft of data are common monetization models for cyberattacks and are sometimes used in combination.
    - The attackers often leverage social engineering techniques, especially phishing by E-mail to gain initial access, but also resort to attacks against web-facing applications and in some cases against trusted third parties.

2.2.4 IMPACT OF CYBER ATTACKS AGAINST INSURERS

50. There are many ways in which a cyber attack can have serious consequences for an organization. For an European insurance undertaking, the following main impacts would need to be considered:

    - **Direct financial loss:** can e.g. arise from physically damaged or stolen IT-equipment, unauthorized transactions or from the payment of ransom to threat actors.[30]
    - **Financial loss through lost availability:** loss of business and loss of working hours due to unavailable systems.
    - **Financial loss through restoration efforts:** additional working hours and often external support needed to deal with the consequences of an attack.
    - **Financial loss through legal consequences:** especially in case of data breaches, fines can be leveled by data protection authorities on the basis of the GDPR and civil lawsuits can be filed in case of damaged third parties.[31]
    - **Loss of reputation:** existing business relations and future opportunities can be adversely impacted by a loss of reputation arising from a cyber attack and the organization's reaction to it.

51. As stated, financial loss through legal consequences against an insurance undertaking are for now excluded from the perimeter of the paper, but could be considered in specific exercises based on a cost/opportunity analysis.
52. All of the abovementioned impacts can be significant drivers of loss and a lack of historical data makes estimates on impacts difficult. However, depending on the type of attack as discussed in section 2.2.3, expectations on the relevance of possible loss factors have been derived based on expert judgment, as shown in Table 1.
53. In addition to the four scenarios shown by the analysis in section 2.2.3 to be currently relevant in this context, four additional scenarios are included in the table below: Unauthorized

[30] Payment of ransom might not be allowed in certain jursidictions depending on national legislation.
[31] General Data Protection Regulation (GDPR). Legal text available at: https://gdpr-info.eu/.

transaction, Payment infrastructure outage, Data Center/Infrastructure damage and Power outage.

54. These are not prominently ranked by ENISA or the MITRE database, as they are not recurring patterns of cyber attacks. However, due to the large impact these scenarios could have on insurers, they are included on the basis of expert judgment. Furthermore, even though these are not common attack patterns of cyber criminals, especially the likelihood of attacks against IT- or power-infrastructure providers is deemed to have increased in the context of the ongoing war in Ukraine.
55. Of the eight scenarios included in Table 1, five scenarios have been selected for consideration in the further scope of this document. These are further discussed in section 5.

Table 1 – Impact of various cyber resilience scenarios

	Direct Loss	Availability	Restoration	Legal	Reputation
Ransomware	Moderate	High	High	Low	Moderate
DoS	Low	High	Low	Low	Low
Data breach	Low	Low	Moderate	High	High
Cryptojacking*	Low	Moderate	Low	Low	Low
Unauthorised transaction*	Moderate	Low	Low	Moderate	Moderate
Payment infrastructure outage*	Low	Moderate	Low	Moderate	Low
Data Center / Infrastructure damage (cloud outage)	Low	High	Moderate	Low	Low
Power outage	Moderate	High	Moderate	Low	Low

*This scenario was not retained. For the rationale behind this exclusion see section 5.3 of the paper.

2.3 CYBER UNDERWRITING: INSURERS EXPOSED THROUGH UNDERWRITTEN PRODUCTS

56. To manage the financial impact of cyber attacks on their policyholders, insurance undertakings offer cyber insurance products of different types. A distinction can be made between affirmative cyber risk and silent cyber risk. The first kind considers insurance policies which cover explicitly cyber risk either on a stand-alone basis or by means of an add-on cover or a rider.[32] Silent cyber

[32] Policies with cyber as add-on coverage are those for which cyber is explicitly added on top of other risk(s).

however considers traditional insurance policies for mostly non-life products which cover cyber risk implicitly.[33]

2.3.1 CYBER INSURANCE MARKET

57. A global view of the cyber insurance market is not conducted on a regular basis since insurance supervisors typically do not collect separate statistical data on cyber insurance products.[34] The standalone policies are typically reported within broader Lines of Business (e.g. General Third Party Liability insurance for direct and proportional business). However, the IAIS[35] performed estimates for the global cyber insurance market which ranged between 4 and 5 billion USD in 2018.
58. Furthermore, a strong increase in the number of cyber attacks is observed where hostile external data breach and ransomware are amongst the most common incidents. This increase is driven by the increasing geopolitical tension leading to a greater activity from state backed actors.[36] Moreover, the technical requirements for committing cyber attacks have lowered due to the advent of Ransomware-as-a-Service. In this case, out-of-the-box tools are provided which allow to execute attacks without prior knowledge. These considerations lead to an increase in the claims frequency observed by cyber insurers. Cyber security company SonicWall shows[37] that the ransomware attacks it observed more than tripled going from 59.6 million in Q1 2020 to 188.9 million in Q2 2021.
59. An increase in the average cost of cyber attacks is also observed. The average ransom which is paid, observed a stark increase from 2018 to 2020 since the ransomware threat actors chose to focus more on large undertakings and to increase their ransom demands.[38] Given certain high-profile attacks such as the attacks on SolarWinds and Colonial Pipeline, additional investments, legislative and regulatory measures were observed to improve national cyber security. This caused a reorientation of ransomware threat actors to small and medium enterprises as can be seen recently in the observed average ransom payments, which have stagnated. This general increase in ransom payments did however lead to strong increases in claims severity.

[33] EIOPA (2022), Supervisory statement on the management of non-affirmative cyber exposures. Available at: https://www.eiopa.europa.eu/document-library/supervisory-statement/supervisory-statement-management-of-non-affirmative-cyber_en

[34] A new template on cyber underwriting - S.14.03 — Cyber underwriting risk – was proposed by EIOPA as part of the 2020 review of Solvency II.

[35] IAIS (2020), Cyber Risk Underwriting - Identified Challenges and Supervisory Considerations for Sustainable Market Development. Available at: https://www.iaisweb.org/uploads/2022/01/201229-Cyber-Risk-Underwriting_-Identified-Challenges-and-Supervisory-Considerations-for-Sustainable-Market-Development.pdf.

[36] While it is difficult to identify state-backed attacks in case of conflicts, technological research and consulting firms (e.g. Garner, PwC) observed an increase of threats and attacks after the inception of the Russian invasion into Ukraine.

[37] SonicWall, Mid-Year 2021 Cyber Threat Report.

[38] Coveware, Quarterly ransomware report. Available at: https://www.coveware.com/ransomware-quarterly-reports.

60. Higher frequency and severity of claims is reflected into an increase in rates for cyber insurance policies. Marsh indicates that across geographies these increases can be up to 30% on average.[39] It does appear however that a deterioration of profitability is observed in some national markets.[40] For instance, Amrae indicates an increase in the loss ratio from 84% to 167% in the French cyber insurance market from 2019 to 2020. An analysis of BaFin for the cyber reinsurance market shows similarly an increase from 68% to 87%.[41] However, for the direct German cyber insurance market a stable profitability can be observed at 68% and 67% respectively in 2019 and 2020.

2.3.2 AFFIRMATIVE CYBER

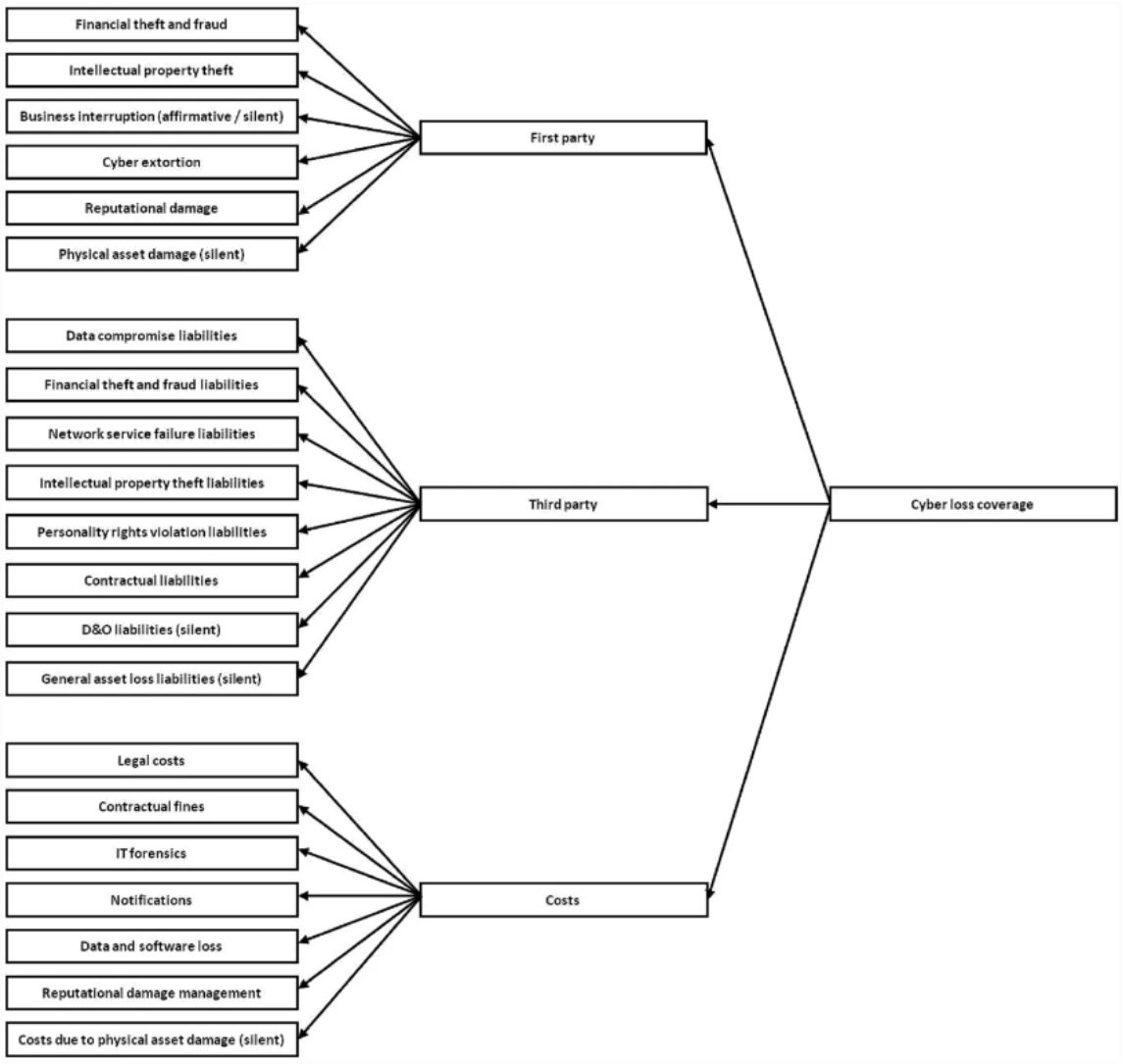
61. For affirmative cyber, typically different kinds of coverage are offered which focus on first-party loss suffered by the policyholder itself, third-party loss for which the policyholder is liable and additional costs (e.g. IT forensics) which occurred because of the cyber incident (Figure 1).

[39] Marsh, Global Insurance Market Index Q1 2021. Available at: https://www.marsh.com/us/services/international-placement-services/insights/global-insurance-market-index-q1-2021.html.

[40] Amrae (2022), Light Upon Cyber Insurance (LUCY). Available at: https://www.amrae.fr/bibliotheque-de-amrae?ref_id=4043&ref_type=publication.

[41] BaFin (2022), A closer look at cyber policies. Available at: https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2021/fa_bj_2112_Cyberpolicen_en.html

Figure 1 - Categories of cyber coverage[42]



62. Typical first-party coverages for standalone cyber policies are the following:

- **Cyber extortion** which reimburses the ransom payment in the case of a ransomware attack.
- **Financial fraud or theft** which reimburses losses for instance due to fraud impacting certain financial transactions (e.g. CEO fraud).
- **Business Interruption (BI)** which reimburses lost operational profits due to the interruption of operations following a cyber attack.
- **Contingent Business Interruption (CBI)** which reimburses the loss of operational profits due to interruption of activities of a supplier or critical vendor following a cyber event.

[42] Wrede D., Stegen T. and von der Schulenburg J., Affirmative and silent cyber coverage in traditional insurance policies: Qualitative content analysis of selected insurance products from the German insurance market, The Geneva Papers on Risk and Insurance - Issues and Practice, 2020. Available at: https://link.springer.com/article/10.1057/s41288-020-00183-6#citeas.

63. Certain third-party coverages include:

- **Incident response costs** covering crisis management or remediation costs following a cyber event.
- **Professional Indemnity** concerning costs related to the failure in providing adequate professional services or products resulting from a cyber event.
- **Director's and Officer's (D&O) liability** compensating claims made against director's and officer's of a policyholder due to e.g. breach of duty or breach of trust following a cyber event.

64. A more exhaustive overview can be found in Annex 9.3 based on the definitions provided by the CRO Forum[43] and the OECD.[44]
65. Typically, it is observed that business interruption coverages can consist of a material part of the insurance claim. Large undertakings might have back-up and incident response plans which allow them to restore data and software in a timely manner. However, small and medium enterprises have typically a less robust ICT risk management without back-up and incident response plans, which implies they might have multiple weeks of interruption of activities and large claims costs. Insurance undertakings have started managing these risks by means of risk underwriting practices and risk limiting setting. Certain undertakings have specific sub-limits for business interruption in their policies and specific deductibles for this coverage.
66. Furthermore, specific economic sectors can be more often the victim of cyber events. This is typically due to the sensitive nature of the data that they dispose (Personal Health Information and Personal Financial Information). These economic sectors are for instance the financial sector, the healthcare sector, and the professional services sector. When this data is breached by the threat actor, it can be used for identity theft, financial theft, or extortion purposes. To this end, certain undertakings have started implementing an exposure management framework where dedicated limits are set per economic sector to avoid a too large exposure to sectors which are prone to cyber attacks.

2.3.3 SILENT CYBER

67. Traditional insurance policies can sometimes also cover cyber risk in an implicit manner. This is often due to policy wording which is open for interpretation and which does not explicitly exclude cyber risk. Analyses of the terms and conditions offered by undertakings has been performed in certain national markets. Based on a 2019 analysis it was possible to conclude that in some cases the total potential exposure to silent cyber can be roughly 80% of the total cyber insurance market with only about 20% resulting from affirmative covers. While the

[43] CRO Forum (2016), Concept Paper on a proposed categorisation methodology for cyber risk. Available athttps://www.thecroforum.org/wp-content/uploads/2016/06/ZRH-16-09033-P1_CRO_Forum_Cyber-Risk_web-2.pdf.
[44] OECD (2017), Supporting an effective cyber insurance market. Available at: https://www.oecd.org/finance/supporting-an-effective-cyber-insurance-market.htm.

situation may have improved, this risk can therefore still be of high materiality. Currently, no wide jurisprudence exists which would demonstrate that cyber is covered by these policies. However, in the current climate with increasing cyber incidents, this implies that there is a large uncertainty that insurance claims would be triggered leading to large financial losses for insurance undertakings.

68. Different products can be impacted by silent cyber:

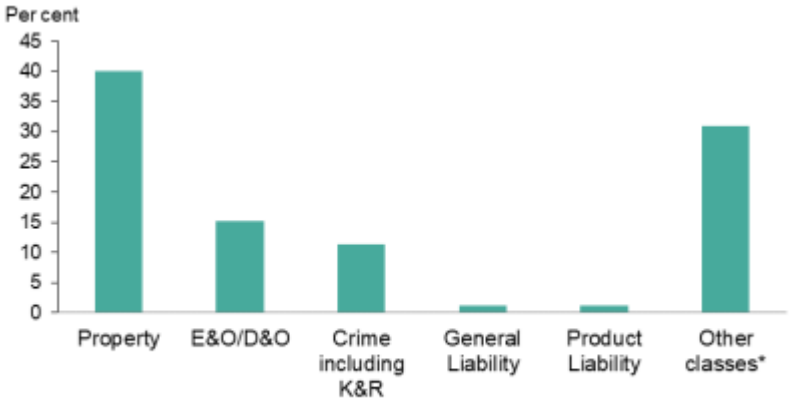
- Firstly, different **General Liability** products will cover liability resulting from inadequate professional services, breach of trust from director's and officer's (for D&O), inadequate products (for product Liability), inadequate technological services e.g. vulnerabilities in software (for Tech E&O). In some national markets, it is observed that cyber risk is often implicitly included in these policies (up to 50% of GTPL policies for some companies).
- **Fire/Property** policies often show more clarity in the policy wording since it is often linked to physical damage with explicit exclusion of cyber risk (e.g. damage on infrastructure). However in some national markets for certain undertakings, up to 10% of insurance policies can show silent cyber. Fire and property policies could result in theft and spoilage of goods under a cyber attack and could also be triggered by manipulation of the control data/software of a heating system/blast furnace leading to overheating and thus fire of the system and the building surrounding it.
- **Business interruption** policies can incorporate non-affirmative cyber. However, the experience of the COVID-19-crisis shows that often these business interruption policies are in the European Union linked to physical damage. Non-damage business interruption policies which have a broader definition of business interruption would allow for silent cyber. For instance, encryption of production data of a food manufacturer could result in uncontrolled processes which damage machines and trigger a business interruption.
- Longer-term interruption of operations for undertakings without back-up and incident response plans can lead to liquidity and solvency difficulties. It has been observed that this can lead in certain cases to defaults and would therefore trigger **Credit insurance** policies.
- **Crime policies including Kidnap & Ransom** can in some cases also cover implicitly cyber extortion. In this case, the ransom payment following a ransomware attack would be covered by this product.
- Also in **Marine, Aviation and Transport** can silent cyber be covered e.g. in the Marine liability cover. A notable example consists of the NotPetya attack which resulted in some container ships being interrupted in a harbor due to the ransomware attack also impacting the port software.

69. Furthermore, cyber risks within certain policies might be silently guaranteed even though the probability of it being triggered is more remote:

- In **Motor Third Party Liability**, cyber attacks might happen due to vulnerabilities in the software used in cars. The most prominent is the hack of a car company in 2015 where it was possible to fully control a car remotely through vulnerabilities found in its digital dashboard software. In a second stage, the car accidents and resulting bodily injuries might lead to **Worker's Compensation** claims.
- Furthermore, a cyber attack on a hospital might lead to an increase in **medical expenses** and **life insurance** policies being triggered.

70. The above list contains the main examples of silent cyber risk, but should not be seen as exhaustive.
71. Undertakings have changed the wording of their policies to manage the silent cyber risk. Typically they used two different approaches, namely excluding cyber from the traditional policies or insuring it explicitly typically in insurance riders or standalone policies. These exclusions are typically relatively recent and have not yet been challenged in courts. A legal risk can therefore exist and it is not excluded that a residual silent cyber risk exists.
72. As an example, Figure 2 shows the distribution of non-affirmative cyber losses by product type as reported in the results of the cyber underwriting scenario of the Bank of England Prudential Regulation Authority (PRA) 2019 Insurance Stress Test.

Figure 2 – Non-affirmative cyber losses product breakdown[45]



(a) Other classes included: credit and surety, legal, political risk and unallocated losses

2.3.4 ACCUMULATION RISK

73. One of the main differences that can arise between cyber resilience and cyber underwriting risk beyond the scope of the cyber attack is also the type of impact. In the case of underwriting risk, a portfolio of policyholders is concerned. This implies that the impact on the individual

[45] Letter sent to participating firms Insurance Stress Test 2019 and Covid-19 stress testing: feedback for general and life insurer, PRA, June 2020. Available at: https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/letter/2020/insurance-stress-test-2019-feedback.pdf?la=en&hash=BF3DF52210D9CBAF6FED788E35DB8530A74B5337.

policyholder can be of lower materiality for the undertaking, but the aggregate impact across the entire portfolio can be large. For operational risk, the impact on the single insurance undertaking is expected to be larger in extreme scenarios.

74. This therefore implies that for an insurance undertaking accumulation risk is of high materiality. These are single or a limited number of cyber incidents which cause insurance claims across a multitude of policyholders. The outage of a critical cloud service provider can be an example of such accumulation risk.
75. There are different types of accumulation risk. A first type concerns the pure IT accumulation risks. These are typically traditional cyber incidents which could impact mostly affirmative cyber covers. A second type consists of the so-called cyber-physical risks. These are cyber incidents which lead to physical events. These would also be expected to have a greater impact on silent cyber.
76. IT accumulation risks could be triggered by:

    - A cyber attack on a cloud service provider leads to an outage. Platform and software providers as well as businesses who use these services observe an interruption of operations.
    - A global ransomware attack infects a multitude of businesses whose data and software is encrypted. During a few days, operations are interrupted. Some undertakings with back-up and incident response plans choose not to pay the ransom and restore their data and software from the back-up. Others do pay the ransom, but generally observe a slower recovery.
    - A Denial of Service attack on a globally used service provider leads to a multitude of businesses not being able to use these services and see their operations impact.
    - A zero-day vulnerability allows threat actors to scale a data breach across a multitude of undertakings leading to breach of privacy compensation, data and software loss and Intellectual property theft.

77. For the cyber-physical risks, the following scenarios are often observed:

    - A cyber attack on the energy grid leading to a power outage with a resulting impact on business, suppliers, critical vendors and families triggering Business Interruption and CBI policies as well as property damage and general liability coverages.
    - A targeted attack against an industrial site could lead to interruption of business, property damage and possibly bodily injuries.

Questions:

Q. 1: 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.

Q. 2: 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.

3 KEY ASSUMPTIONS

78. This section describes the set of key assumptions and exclusions underlying this paper. Given that the knowledge of cyber risk in the context of stress testing is still at an incipient phase, these assumptions and exclusions might be adjusted in the future.
79. For the assessment of insurance undertakings' own cyber resilience, in line with the ESRB approach mentioned in section 2.1, this paper focuses on cyber incidents of a malicious nature, i.e. cyber attacks. While excluded from the perimeter, the treatment of non-malicious events should be similar to that of malicious acts from a stress test perspective (e.g. same scope, metrics). Therefore, specific scenarios based on operational errors could be developed at a later stage.
80. For disruptions caused by an interruption of services by a service provider, no distinction is made between deliberate and non-deliberate actions. This approach is chosen to more comprehensively capture the risks of concentration to third-party service providers. While non-deliberate actions from service providers are also part of the operational risk framework, the consequences for the undertaking should be the same. EIOPA is conscious of the potential inconsistency generated by this assumption in the treatment of entities with full in-house operations and entities with operational models based on out-sourcing. The design of a potential future exercise will consider this aspect in the definition of the scope and in the identification / calibration of shocks, maintaining a level playing field among the participants.
81. Also limited to the cyber resilience, the paper excludes regulatory fines and compensations against legal actions initiated by policyholders upon, for example, data breaches. The rationale lies in the complexity of the modelling (estimations and predictions) which requires a large set of assumptions that might undermine the robustness of the scenario. Additionally, the complexity is increased by the heterogeneity in local legislations. However, regulatory fines and compensations against legal actions might be considered in specific exercises based on a cost/opportunity analysis.
82. Finally, the paper discusses potential payment of ransom for ransomware scenarios in the assessment of both cyber underwriting risk and cyber resilience (see sections 6.4.1 and 7.4.2). However, these payments might not be allowed in some jursidictions depending on national legislation.

Questions:

Q 3: What is your view on the proposed approach regarding operational errors (i.e. considering non-malicious events at a later stage)? Please provide clarification.

Q. 4: 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.

Q. 5: What is your view on the proposed treatment of regulatory fines and compensation against legal actions? Please provide clarification.

4 SCOPE

83. When assessing cyber risk via a stress test exercise, the scope is one of the cornerstones of the exercise and it should be strictly related to its objective.
84. As for the capital stress test, the scope should be selected considering all the other elements of the exercise such as the objective(s), the approach, the time horizon, the scenario and the methodology. When assessing cyber risk, the choice between group and solo undertakings might depend on whether the stress test is assessing cyber resilience risk or cyber underwriting risk. In absolute terms, there is no best option between groups and solos. Both solutions present advantages and disadvantages as shown in Table 2.

Table 2 - Advantages and disadvantages of targeting solo or group undertakings for the purposes of stress testing cyber risk

	Advantages	Disadvantages
Solo	• Target specific business lines (particularly relevant for cyber underwriting risk and non-affirmative exposures) • Country/jurisdiction analysis • Easy to compute the market coverage • Easier application of the shocks (no consolidation at group level needed) • Easier to validate the data • Easier to issue potential recommendations and recovery/resolutions actions (one NCA involved) • More useful as an input to micro-supervision • Easier to test some scenarios that include physical harm (e.g. data center fire, flood, sabotage) • Easier to design cyber resilience scenarios in case of less centralized critical IT systems	• No diversification effect accounted (only relevant for cyber underwriting risk and non-affirmative exposures) • Less informative from a financial stability perspective • Need some coordination work from both the insurance groups and the NCAs in case of participating solos from more than one European country that are part of the same group with the risk of duplicating work (validation activities performed at local level) • Potential limitation in evaluating the impact of reactive post-stress management actions (if they have to be decided at group level) • More difficult to assess the impact of cyber resilience scenarios in case of strongly centralized critical IT systems
Group	• Impact on the systemic groups particularly with regards to the provision of critical services (more informative/useful from a financial stability perspective)	• High complexity in the application and assessment of the shocks with the consequence of the necessity to apply simplification and approximation that could have an

	• Account for full diversification effects (only relevant for cyber underwriting risk and non-affirmative exposures) • Easier to assess the impact of reactive post-stress management actions if needed (if they have to be decided at group level) • Easier to design cyber resilience scenarios in case of strongly centralized critical IT systems • Allows for assessing the impact on non-insurance entities of the group (only relevant for cyber resilience)	impact on the comparability of the results • More complex to design cyber resilience scenarios in case of less centralized critical IT systems • No country based assessment • Harder to identify vulnerabilities of specific entities • Harder to issue potential recommendations and recovery/resolutions actions • Harder to validate the data

85. For cyber resilience scenarios, targeting groups could be more relevant in case of concentration of critical IT systems within the group and if the aim is to assess the impact on financial stability, including potential disruptions to the provision of critical services that are likely to affect other market participants or the real economy. Moreover, by targeting groups the assessment of the potential impact of a cyber attack is extended also to non-insurance entities within the group.
86. For cyber underwriting scenarios, targeting solos could be less complex to analyse the impact on relevant coverages and lines of business.
87. A potential hybrid approach to the scope definition could also be considered as done for the liquidity component of the 2021 EIOPA Insurance Stress Test.[46] An example would be to carry out the analysis at group level for cyber resilience risk and at solo level for cyber underwriting risk (only for those undertakings more exposed to cyber underwriting risk).
88. The identification of the entities to be included in a potential stress test exercise will also account for potential biases that the operational models in-force by the undertakings might generate according to the scenario(s) and shocks specified.

Questions:

Q. 6: 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.

Q. 7: Should stress testing of cyber resilience risk be carried out at group or solo level? Please provide clarification.

[46] EIOPA (2021), Insurance Stress Test 2021 Technical specifications. Available at: https://www.eiopa.europa.eu/sites/default/files/financial_stability/insurance_stress_test/insurance_stress_test_2021/2021-stress-test-technical-specifications-v1.1.pdf.

Q. 8: Should stress testing of cyber underwriting risk be carried out at group or solo level? Please provide clarification.

Q. 9: 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.

4.1 CRITERIA

89. In a traditional stress test exercise the natural reference for selecting the targeted entities is their size in order to achieve the widest coverage possible and to take into account their systemic nature.[47] When it comes to a cyber stress test exercise, in addition to those criteria, other elements could be considered depending on the risks to be assessed (cyber resilience vs cyber underwriting). The application of the criteria is dependent on the information available.
90. For cyber resilience risk, it might be useful to consider those undertakings engaged in critical functions[48], the exposure of the undertakings to critical ICT third-party service providers and the potential impact of a cyber scenario on non-insurance entities of the group providing essential services to the insurance activity (such as asset-management firms, claims management firms, etc.).
91. In terms of cyber underwriting risk, one could consider the cyber insurance market coverage (i.e. affirmative coverages such as cyber standalone policies and policies with cyber as an add-on coverage) and the existence of non-affirmative exposures (i.e. silent cyber).
92. Table 3 makes reference to the criteria that could be considered when selecting the entities to be included in the scope of a stress test exercise with focus on cyber risk, depending on whether the assessment is covering cyber resilience or cyber underwriting risk.

Table 3 - Reference metrics for inclusion of undertakings in the scope of a stress test with focus on cyber risk

	Cyber Resilience	Cyber Underwriting – Affirmative exposures	Cyber Underwriting - Non-affirmative exposures
Reference (benchmark)	Size of the EU market (a sub reference to ensure a Minimum	Size of the EU market for specific non-life lines of	Size of the EU non-life market (a sub reference to ensure a

[47] The concept of wide market coverage was converted into a market coverage at least of 75% of the EEA market based on total assets. However, the reference and the threshold for the coverage were further refined for the liquidity component of the 2021 Stress Test exercise.

[48] The IAIS identifies undertakings engaged in critical functions as those insurers that provide services that are important for the functioning of the financial sector and the real economy and where there are few, if any, readily available substitutes. IAIS (2019), Holistic Framework for Systemic Risk in the Insurance Sector. Available at: https://www.iaisweb.org/uploads/2022/01/191114-Holistic-Framework-for-Systemic-Risk.pdf.

	coverage at country level could be considered as well)	business[49] (a sub reference to ensure a minimum coverage at country level could be considered as well) Reference size of the EU market for standalone cyber policies and policies with cyber as add-on coverage[50] (a sub reference to ensure a minimum coverage at country level could be considered as well) Depending on the choice of scenario a more granular approach based on the risks included in the coverage might be considered	Minimum coverage at country level could be considered as well)
Exposure	Size of the company	Size of the specific non-life line(s) of business Size of the cyber coverage for standalone cyber policies and policies with cyber as add-on coverage Depending on the choice of scenario a more granular approach based on the risks included in the coverage might be considered	Size of the non-life lines of business[51]
Metrics	TA (w/wo UL/IL); GWP, total gross TP (w/wo UL/IL)	Line(s) of business gross TP/ GWP; others: TA (w/wo UL/IL) Cyber coverages gross TP/ GWP	Line(s) of business GWP for non-life; others: TA(w/wo UL/IL)

[49] Specific lines of business to be selected based on the Solvency II lines of business more likely to include cyber coverages (ref. Risk description).

[50] As reported in the template S.14.03 — Cyber underwriting risk to be included as part of the 2020 review of Solvency II. Source: Draft Amended Implementing Technical Standards (ITS) on supervisory reporting and disclosure – ITS on supervisory reporting. Available here: https://www.eiopa.europa.eu/document-library/technical-standard/draft-amended-implementing-technical-standards-its-supervisory_en.

[51] Specific lines of business to be selected based on the Solvency II lines of business more likely to include silent cyber coverages could be considered (ref. section 2).

Questions:

Q. 10: Which are in your view the Solvency II lines of business expected to be more impacted by affirmative cyber underwriting risk?

Q. 11: 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)?

Q. 12: What is your view on the criteria for the selection of the participating entities listed in Table 3? Please provide clarification.

Q. 13: Are there any other relevant criteria not covered in Table 3 or in your answers to the previous questions? Please specify.

5 SCENARIOS

5.1 SCENARIO SELECTION

93. In order to define a cyber risk stress test scenario, one must consider what kind of cyber incident would be the catalyst, the risk factors that can trigger the incident and their possible consequences for the company itself, its clients and any third parties affected.
94. The design of the assumptions underlying a cyber resilience or a cyber underwriting shock may have to differ. On one hand, a cyber incident affecting significantly one or several important companies is already something quite common. These cyber resilience shocks have instant and intense effect on these companies. On the other hand, until now, it is difficult to say that a widespread shock, impacting the cyber underwriting portfolio of several insurance companies, has yet been witnessed. Indeed, a raise in the loss ratio of cyber insurance has been witnessed in the past years, but that change in the market does not have the intensity nor the abruptness of a widespread shock yet. That means that a widespread shock impacting the cyber insurance market would involve a common cause *that may not have been clearly identified until now*. It may involve **new techniques** developed by cyber criminals, but also **new IT practices or usage** happening across one or several industries. Given the pace at which the digital industry is evolving in the late years and given the pace at which new hacking techniques are invented, such an event cannot be considered as unlikely.
95. The scenarios described in this section can be seen as the common core of events that can affect either directly the insurer (cyber resilience), its portfolio (cyber underwriting), or both. The shocks will be then designed differently for cyber resilience and cyber underwriting.
96. For the purpose of this paper and without claiming to be exhaustive, Table 4 presents a set of categories of cyber-incidents, along with the associated risk factors, as a starting point for designing the stress scenarios. The choice of scenarios is guided by the discussion of the implications of cyber risk for insurers presented in section 2, as well as a review of work already published by other supervisors, e.g. the PRA and the NBB.[52]

Table 4 – Categories of cyber incidents and associated risk factors

Cyber Incident	Risk Factors
Data Center / Infrastructure damage (cloud outage)	Physical harm (fire, flood, sabotage…)

[52] PRA General Insurance Stress Test 2022. Available at: https://www.bankofengland.co.uk/prudential-regulation/letter/2022/may/insurance-stress-test-2022. NBB Insurance Stress Test 2022 - Cyber scenario. Available at: https://www.nbb.be/en/financial-oversight/prudential-supervision/areas-responsibility/insurance-or-reinsurance-40.

	Negligent or accidental harmful act Dependency on Cloud/Communications providers
Ransomware	Human factor (phishing, malware, threats…) Internet services (websites, web services, remote access…) Third parties / contractors
Denial of Service (DoS)	Internet services (websites, web services, remote access…) Business-to-business platforms Dependency on Cloud/Communications providers
Data breach	Equipment malfunction / malware Human factor (disgruntled employee, error…) Changes in IT configuration / new services deployment
Power outage	Physical harm (fire, flood, sabotage…) Negligent or accidental harmful act, could be state-backed threat actor

97. In designing potential future stress test exercises' scenario(s), different categories of cyber incidents might be considered in isolation or combined (e.g. ransomware and data breach).
98. Moreover, the categories of cyber incidents considered in this paper are built on the current risk environment and literature. Any potential future exercise will identify the relevant scenario(s) to be tested during the specific design phase and the list provided now serves only as a reference. EIOPA could also consider a collaboration with other European agencies or platforms (e.g. ESRB, ENISA, Joint Cyber Unit), practitioners, academia and model vendors in the design of scenarios, the identification and the calibration of the shocks for future stress test exercises.

5.2 SCENARIO NARRATIVES AND SPECIFICATIONS

99. Following the selection of the relevant scenarios, another important consideration relates to scenario specification, as cyber risk scenarios can be specified at different aggregation levels.
100. For cyber underwriting, the scenario specification and the stress parameters granularity should take into account the intensity of the cyber incident and its duration, as well as the percentage of infected policyholders of the participating undertakings. These parameters

should in turn be translated into a potential increase in claims on cyber policies and impact on new business or increase in termination[53] aspects.

101. For cyber resilience, the stress parameters granularity would also depend on the intensity of the cyber incident and its duration, but also on the percentage of operational units infected of the participating undertaking itself. These parameters are subsequently translated into business interruption cost, total monetary cost of recovery and time elapsed until return to business as usual (BAU).

102. The remainder of this section provides a description of potential scenarios for the various categories of cyber incidents considered in Table 4.

5.2.1 DATA CENTER/INFRASTRUCTURE DAMAGE (CLOUD OUTAGE)

103. Loss of part or of the entire IT infrastructure supporting business operations (i.e. servers, applications, databases, backup storage…) can be caused by natural disaster or misconfiguration affecting service providers, as well as by sabotage, to the main data center of the company.54

104. Depending on the internal structure of the company, this scenario may affect some or all branches of the company. It may also affect voice and mail communication services, thus hampering incident response efforts and, most importantly, it will test the availability and readiness of a Business Continuity Plan.

105. Incident response should take into account whether the company has alternate Data Centers, up to date backups, the time to restore data into a new infrastructure – especially if large amounts of data should be downloaded from the cloud and, if necessary, the time needed to procure new equipment and/or how to proceed with the repairs.

106. Cyber resilience is thoroughly tested in this scenario, as most modern companies rely heavily on their data center for every aspect of their business and, consequently, a severe shock in this area, along with the ransomware scenario are the most challenging to tackle.

107. The impact on cyber underwriting depends mostly on the type of data center affected. If it is one or multiple cloud provider data centers (e.g. Microsoft, Amazon, Google…), the impact could be severe depending on the company's insurance portfolio. On the other hand, damage to a data center owned by the company or, even, to a local/regional data center, would have a much lesser impact, if any. This scenario is more likely to impact small businesses lacking of geographical redundancy than big businesses.

108. Table 5 discusses the likeliness/plausibility and possible impact of this scenario.

[53] Only if we consider second-round effects. In this case, a second-round effect would for example concern the impact caused by the cyber resilience event on new business due to loss of reputation.

[54] Examples illustrating this case include the follow: Foiled Plot to Attack AWS Reflects Changing Nature of Data Center Risk. Available at: https://datacenterfrontier.com/foiled-plot-to-attack-amazon-reflects-changing-nature-of-data-center-threats/. Outage in Dublin Knocks Amazon, Microsoft Data Centers Offline | Data Center Knowledge | News and analysis for the data center industry. Available at: https://www.datacenterknowledge.com/archives/2011/08/07/lightning-in-dublin-knocks-amazon-microsoft-data-centers-offline.

Table 5 – Cloud outage scenario

Likeliness/ plausibility as a cyber resilience scenario	In order to represent a widespread risk, the data center has to be damaged as well as its backup. Such an event affecting an insurer already happened.[55] Such an event impacting several insurers is less likely.
Likeliness/ plausibility as a cyber underwriting scenario	Such an event having a significant impact on a cyber insurance portfolio never happened yet. In order to be of significance, it has to be assumed that a widely used cloud service or data center provider suffers a significant outage.
Possible impact of the scenario on the insurer (cyber resilience)	Outage duration that would trigger business interruption and definitive loss of data.
Possible impact of the scenario on the insurance portfolio	This event will trigger the coverage of business interruption and data reconstruction costs in contracts where the losses coming from data center damage (or cloud outage) are not excluded. Mid-size enterprises market more likely to be impacted. As a secondary effect, if a significant portion of businesses are impacted, a moderate shock on equity market can happen.

5.2.2 RANSOMWARE / DATA THEFT

109. A ransomware attack targeting the employees' computers via phishing or the data center itself through some software vulnerability (e.g. in the company web site), encrypts the computers and spreads all through the organization, or most of it, and triggers the disconnection of the unaffected offices in order to avoid infection.

110. This attack may include threat of public disclosure of sensitive data and/or client data in which cases the scenario would also include dealing with the GDPR[56] national authority.

111. As was the case in the data center damage scenario, the company must determine what services would be affected and their impact on coordinating the incident response efforts and why and how they would keep operative in spite of the attack (e. g. network segregation, limited user privileges…).

112. The availability of backup systems not affected by the encryption (this must be justified) and the ability to clean the affected computers and restore systems and data in a timely fashion are of the utmost importance in this scenario. Also, the company will need the help of experts in the field that, usually, will not be on their payroll and may not be ready to assist at a moment's notice if otherwise engaged.

[55] While a general example would be the OVH fire, an illustrative example specific to the insurance sector could be the case that occurred recently in Spain where there was a Data center outage due to ransomware. As for this Spanish case the cloud was in-house, it is a case of cloud service that is not provided by the major players (Amazon, Google, Microsoft). Source: Reuters (2021), Millions of websites offline after fire at French cloud services firm. Available at: https://www.reuters.com/article/us-france-ovh-fire-idUSKBN2B20NU.
[56] General Data Protection Regulation (GDPR). Legal text available at: https://gdpr-info.eu/.

113. According to research, ransomware coverage in insurance policies is not only encouraging threat actors, but the practice may be fueling the entire ransomware economy, so cyber underwriting is a key factor in this scenario and may have serious consequences for the insurance company.[57]

114. In order to mitigate the costs of ransomware attack on the insured, it is a common practice for insures to call for the services of cyber loss mitigation specialists. These specialists are commonly subcontractors of the insurers or referenced companies. They are essential for helping the insured to take emergency measures, track the malware used, and allow the return to normal situation. In the context of a widespread event, where a significant percentage of companies are impacted in a short lapse of time, it seems more than likely that these specialist companies get overwhelmed, entering in a saturation of their capacity. This can end in a slower reaction of the insured and an increase in the mean cost of the cyber incidents.

115. Table 6 discusses the likeliness/plausibility and possible impact of this scenario.

Table 6 – Ransomware / Data Theft scenario

Likeliness/ plausibility as a cyber resilience scenario	Multiple high-profile-attacks against insurance companies have become publicly known[58, 59, 60, 61]. In addition, attackers are known to specialize themselves by industries, so that this kind of event can be seen quite likely to become widespread and concern several insurers in a small lapse of time.
Likeliness/ plausibility as a cyber underwriting scenario	Losses coming from this category of cyber incident increased in the latest years. A significant increase in losses would be driven by the ability of attackers to use new hacking technics and/or to industrialize their actions a step further.
Possible impact of the scenario on the insurer (cyber resilience)	Depending on scope and sophistication of the attack, redundant sites and backups can be affected. Interruption of critical business processes is an immediate consequence and, if data is lost, recovery can be lengthy and difficult. In so-called 'double extortion attacks', sensitive data is also stolen, adding all potential impacts of the 'Data Breach' scenario to this direct impact on business operations.

[57] Although the largest insurance organisation in the United States defends ransom payment reimbursements, one of Europe's top five insurers announced in May 2021 it would suspend ransomware crime reimbursement.

[58] For example, a publicly known case is the French health insurance company MNH that was hit by a ransomware attack. Further details can be consulted on: Healthcare IT News (2021), French health insurance company MNH hit with ransomware attack. Available at: https://www.healthcareitnews.com/news/french-health-insurance-company-mnh-hit-ransomware-attack.

[59] Bloomberg (2021), CNA Financial Paid Hackers $40 Million in Ransom After March Cyberattack. Available at: https://www.bloomberg.com/news/articles/2021-05-20/cna-financial-paid-40-million-in-ransom-after-march-cyberattack.

[60] SC Media (2022), Insurance companies increasingly fall prey to cyberattacks. Available at: https://www.scmagazine.com/analysis/ransomware/insurance-companies-increasingly-fall-prey-to-cyberattacks.

[61] Bleeping Computer (2021), Insurer AXA hit by ransomware after dropping support for ransom payments. Available at: https://www.bleepingcomputer.com/news/security/insurer-axa-hit-by-ransomware-after-dropping-support-for-ransom-payments/.

Possible impact of the scenario on the insurance portfolio	This event will trigger the coverage of business interruption, data reconstruction costs, ransom payment, and data liability, in contracts where the losses coming from ransomware are not excluded.

5.2.3 DENIAL OF SERVICE (DOS)

116. A coordinated attack is launched against the main players in the financial sector, resulting in unavailability of entire customer databases, and also a certain number of hour system downtime for the banks or insurers' client-facing (including mobile and web-based) operational systems[62]. Or, if preferred, a malware program exploits a vulnerability in the networking equipment provided by one or several of the largest manufactures (Cisco, Juniper…) with a market share nearing 50%.[63]

117. The attack may or may not affect the insurance company itself. If it does, then it is a case similar to the ransomware attack, as most IT services could be down if the attack affects the core of the IT structure. On the other hand, it could be as mild as some downtime in the company's website or its employees' access to Internet, so the severity of the attack should be the main factor to decide prior to defining the scenario.

118. In this scenario, it is not considered that a denial of service attack will target directly the policyholders, but rather affect them through the outage of a main service provider that a significant number of policyholders need for business continuity. The potential impact could extend also to retail policyholders, though this should be more limited.

119. At any rate, this scenario is specifically oriented towards stressing cyber underwriting, as the number of policyholders affected (companies and individuals) could be very large and the losses substantial due to the affirmative and silent cyber insurance coverages.

120. Also, if the affected equipment cannot be repaired via software (i.e. downloading a patch) and requires substitution or a visit to the repair shop, then the amount of time needed to get back to normal could be measured in months, even without taking into account the current state of the world's logistics chain.

121. Table 7 discusses the likeliness/plausibility and possible impact of this scenario.

Table 7 – Denial of Service (DoS) scenario

Likeliness/ plausibility as a cyber resilience scenario	DoS attack harms undertakings connected to internet and can be impactful if their critical business process are online (for instance: underwriting

[62] The MAS (Monetary Authority of Singapore) previously conducted a cyber stress test in 2016 based on a scenario involving simultaneous hacking attacks on financial institutions. Source: IMF (2020), Cyber Risk Surveillance: A Case Study of Singapore. Available at: https://www.imf.org/en/Publications/WP/Issues/2020/02/10/Cyber-Risk-Surveillance-A-Case-Study-of-Singapore-48947.

[63] Networking devices are provided by a few big companies (Cisco, Juniper…) that make up for most of the market. If any of their models is compromised, a lot of networking infrastructure can suffer outages. For example, Cisco market penetration nears 20%. A Swiss report on cyber scenarios elaborated on this threat: SCOR (2017), Economic impact of cyber accumulation scenarios. Available at: https://www.imia.com/wp-content/uploads/2021/07/Economic_impact_Cyber_loss_accumulation_scenarios_SVV.pdf.

	online claims …). Today, with increased digitalization, the majority of the undertaking are in the scope of this scenario.[64]
Likeliness/ plausibility as a cyber underwriting scenario	Such an event having a significant impact on a cyber insurance portfolio never happened yet. In order to be of significance, it has to be assumed that a widely used cloud service or infrastructure provider suffers a significant outage. The impact of the outage depends on the type of service providers and the duration of the outage. Policyholders will usually be affected by short-term business interruptions, which can especially harm organizations with time-critical business processes. Liability insurance may be affected if the insured undertakings fail to deliver their services due to the attack. That seems however mitigated by the fact that the policyholder may transfer his liability to the service provider initially targeted. The claims cost in this scenario is however expected to be lower than for the cloud outage scenario due to the expected shorter-term business interruption.
Possible impact of the scenario on the insurer (cyber resilience)	Business Interruption (including Claims and underwriting operations may be unavailable, relationships with partners may be hampered) causing financial losses due to unavailability and own liability coverage.
Possible impact of the scenario on the insurance portfolio	This event will trigger the coverage of business interruption and data reconstruction costs in contracts where the losses coming from data center damage (or cloud outage) are not excluded. Also, DoS exclusion may have to be considered, but not all exclusions may work as the DoS attack is not considered to be targeting directly the policyholder. As a secondary effect, if a significant portion of businesses are impacted, a moderate shock on equity market can happen.

5.2.4 DATA BREACH

122. Malicious actors have infiltrated an organization's network, or that of a critical IT-service provider and have managed to extract sensitive data. This data can then be sold, made public, or used as a lever for extortion against the organization and potentially affected third parties such as customers that are affected by the breach. Insurers are potentially attractive targets for this attack. Stolen customer data such as social security numbers or debit card data can be used for impersonation and fraud. In addition, health insurers store especially sensitive personal data. This type of attack can be combined with deployment of ransomware.

123. Table 8 discusses the likeliness/plausibility and possible impact of this scenario.

[64] Example of DoS attack: AXA Faces DDoS After Ransomware Attack. Available at: https://www.infosecurity-magazine.com/news/axa-faces-ddos-after-ransomware/.

Table 8 – Data Breach scenario

Likeliness/ plausibility as a cyber resilience scenario	Insurers are potentially attractive targets for this attack. Stolen customer data such as social security numbers or debit card data can be used for impersonation and fraud. In addition, health insurers store especially sensitive personal data.
Likeliness/ plausibility as a cyber underwriting scenario	A massive data breach event or series of events, having a significant impact on the solvability of insurers appears quite unlikely, considering that such incidents actually constitute a small minority of the cyber claims, and that the corresponding losses amount to a small portion of the total cyber losses, as witnessed for example on the French market.[65]
Possible impact of the scenario on the insurer (cyber resilience)	Direct financial loss is unlikely to be a major factor, as the target will probably not even notice a successful attack. Financial impact through loss of availability is also unlikely with this threat. Financial impact through recovery efforts can arise through forensic investigation and communication efforts after a breach becomes known. **Financial loss through legal consequences** is a major concern with this threat, as GDPR fines and civil lawsuits[66] are likely in case of a serious breach of personal data. **Loss of reputation** and customer trust would perhaps be the strongest consideration in this scenario and could be more severe than with any other form of cyber attack, especially if customer health data is affected.
Possible impact of the scenario on the insurance portfolio	Policyholders will usually face legal consequences, which could be covered by liability insurance. The reputational damage will not be covered by usual policies. This event will trigger the coverage of the cost of reconstituting data or software that have been corrupted, but also the regulatory and defense costs that policyholders have to face in the event of a violation of the data privacy law. The impact is expected to be less material than for other scenarios due to a small accumulation of claims.

5.2.5 POWER OUTAGE

124. A power outage might be caused by a threat actor making use of vulnerabilities in the regional/national electricity sector and grid systems or a failure in the grid. This could impact businesses, suppliers, critical vendors and families, triggering (Contingent) Business Interruption policies as well as property damage and general liability coverages. In order to

[65] Data breach represents less than 4.5% of the claims and data liability 3.8% of the losses in the "Lucy" study by AMRAE (the French professional association of risk managers), for the year 2021.
[66] For the purpose of this discussion paper, financial loss through legal consequences are excluded from the cyber resilience component as explained in section 3.

represent a widespread risk, the regional/national electricity sector and grid systems have to be damaged as well as their backup.

125. Table 9 discusses the likeliness/plausibility and possible impact of this scenario.

Table 9 – Power outage scenario

Likeliness/ plausibility as a cyber resilience scenario	At least two cases of power outage scenario are publicly known, one case was due to a malicious attack[67] and another case was caused by extreme weather events.[68] Like any other businesses in the jurisdictions impacted by the power outage, insurers would suffer in their operational activities.
Likeliness/ plausibility as a cyber underwriting scenario	As mentioned in the cyber resilience part above, cases of power outage already happened. It can be considered that all businesses and individuals in this jurisdiction suffer from the power outage as well as all suppliers and critical vendors covered by coverages for Contingent Business Interruption.
Possible impact of the scenario on the insurer (cyber resilience)	An insurance undertaking directly hit by a power outage would suffer major business interruptions for its duration. In contrast to other scenarios, where only a part of the ICT infrastructure might be impacted, most business processes would come to a standstill. However, when power is restored, recovery should be rather quick and little permanent damage to ICT infrastructure and systems is expected.
Possible impact of the scenario on the insurance portfolio	This event will trigger the coverage of business interruption and data reconstruction costs. The businesses observe, on average, crisis service costs of a certain EUR amount and recovery expense costs of a certain EUR amount per infected policyholder. The crisis service costs include elements such as IT forensics, notification etc.

[67] It has been reported in the press that cases of power outage due to cyber-attacks have occurred in Ukraine. ZDNET (2016), US report confirms Ukraine power outage caused by cyberattack. Available at:https://www.zdnet.com/article/us-report-confirms-ukraine-power-outage-caused-by-cyberattack/. Reuters (2022), Ukraine says it thwarted Russian cyberattack on electricity grid. Available at: https://www.reuters.com/world/europe/russian-hackers-tried-sabotage-ukrainian-power-grid-officials-researchers-2022-04-12/.

[68] In February 2021, a case of power outage due to an unusual ice storm was reported in USA (Texas). This event had an impact on critical infrastructures including some data centres. Source: Network Computing (2021), A Near Miss and a Total Loss: Lessons from 2021 in Data Centre Resiliency. Available at: https://www.networkcomputing.com/data-centers/near-miss-and-total-loss-lessons-2021-data-center-resiliency.

5.3 SCENARIOS NOT RETAINED FOR THE PURPOSE OF THIS PAPER

126. The five cyber risk scenarios selected above were retained based on their perceived relevance to the EU insurance sector and their feasibility. Three other scenarios were also considered, but were not pursued further. These might be developed at a later stage.

i. Unauthorized transaction, including "CEO" Fraud, execution of unwanted money transfer (for example, the Bangladesh bank robbery[69]), identity theft of numbers of insured allowing an attacker to empty their life insurance assets: this type of scenarios is not retained because the impact is expected to be insignificant compared to other scenarios.

ii. Payment infrastructure outage: such a scenario could be a separated dedicated stress test in itself as it would be close to a liquidity stress test. Other reasons not to retain this scenario are specific to the infrastructure that would be targeted:
   - Payment system outage ("Visa", "Mastercard"…): that scenario would have consequences on cyber underwriting (similarly to a cloud outage). Business interruption guarantees could be triggered. Indirect consequences could also occur (e.g. on the equity market). This scenario seems less likely and its consequences would likely be difficult to assess by insurance companies, which would have to go through a deep legal analysis of all contracts in order to assess if the exclusions would be triggered or not.
   - "SWIFT" outage, or a central counterparty (CCP) outage: such a scenario would first hurt the banks, the damages on the insurance market being secondary and deriving from the lack of resilience of banks. Insurance undertakings would have difficulties in identifying the real consequences.

iii. "Cryptojacking": this form of attack where compromised computing resources are used to mine cryptocurrencies, is getting more common as prices on the crypto-market are rising. However, it is not retained in this paper because the impact on individual victims is expected to be insignificant compared to the other scenarios.

Questions:

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

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

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

[69] Source: https://en.wikipedia.org/wiki/Bangladesh_Bank_robbery.

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

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

6 CYBER UNDERWRITING: SHOCKS, SPECIFICATIONS AND METRICS

6.1 GENERAL GUIDANCE

127. In terms of application of the shocks, cyber underwriting risks should be in general treated as any other insurance specific shock, e.g. shocks to lapses or shocks to claims. As such, the consequences of a cyber event can be traced back to an increase in claims deriving by higher frequency and, or higher costs. The application of the shocks and the calculation of the impacts should rely as much as possible to the standard EIOPA framework for stress testing with respect to: nature of the shocks (instantaneous), estimation of the impacts (fixed balance sheet), evaluation of the impacts (Solvency II balance sheet) and to the Solvency II framework.

128. On the time dimension, while shocks related to cyber event might be perpetuated over time, in the context of a cyber underwriting stress test they should be applied as instantaneous one-off shocks to the liability portfolios and related risk exposures registered at the reference date.

129. Consistently with the instantaneous nature of the shocks, the post stress balance sheet position should be recalculated without the application of any reactive management action, namely, no de-risking strategy should be taken into account, including:

- Adjustment to the underwriting strategy in place at the reference date
- Adjustment to the in-force reinsurance treaties in place at the reference date

130. The metrics used to measure the impact to an insurance undertaking should be consistent with the Solvency II framework and specifically with the balance sheet provisions therein. As already stated the valuation of the impacts will be initially limited to the impact on the assets, liabilities and eventually to the excess of assets over liabilities. No evaluation of the impacts on the solvency position (i.e. Own Funds and Solvency Capital Requirement) is expected at this stage if not explicitly requested and after careful cost/benefits considerations.

131. Being the shocks related to cyber events targeting the in-force portfolios of non-life business lines, they can be reflected to the insurance balance sheet in two ways:

- Via a full provisioning of the claims triggered by the prescribed shocks.
- Via a full payment of the claims triggered by the prescribed shocks.

132. Conscious of the fact that the in reality the approach taken by insurers lays in between the two extremes listed above, the proposed approximations allow for a controlled and homogeneous assessment of the impacts to the balance sheet of the companies.

133. In case of full provisioning, the prescribed increase in claims should mainly result:

- On the liability side of the BS in an increase of the non-life technical provisions, and
- On the asset side of the BS in a potential increase of the insurance recoverables (in line with the in-force reinsurance treaties. No change in the investments is expected.

134. In case of full payout of the claims the major impacts should be registered:
- On the liability side no change expected;[70]
- On the asset side in an increase of reinsurance receivables, a reduction in cash and equivalent, and a potential reduction in the investment portfolios in case the amount of cash and equivalent held at the reference date is not sufficient to cover the cash outflows deriving from the settlement of the claims.

135. Impacts are expected on other balance sheet items, e.g. deferred tax assets and liabilities. For this, simplifications and approximations might be defined and agreed in line with EIOPA stress test standards.

136. For cyber coverages that are not always clearly identifiable (e.g. silent-cyber), exclusion clause and risk-transfer mechanisms might fail or be challenged. Against this the impact of the prescribed shocks should be calculated:
- With and without the exclusion clauses;
- With and without the effect of the reinsurance coverages.

137. The use of reactive management actions, e.g. de-risking through reinsurance agreements, adjustment of pricing / reserving strategies, is not envisaged at this stage. Any relaxation of the fixed balance sheet assumptions should anyhow be part of the governance framework adopted by the group (e.g. risk management plans, investment strategies, recovery plans). Identified management actions should be plausible under the prescribed adverse scenario.

138. Section 6.2 elaborates on the shocks for each of the relevant scenarios identified for the underwriting component.

6.2 SHOCKS

139. Based on the considerations in section 5, shocks and specification are presented for the following three scenarios:
- Power outage
- Ransomware / data theft
- Datacenter infrastructure damage (cloud outage).

140. The Denial of Service (DoS) and Data Breach scenarios are not discussed due to a lower expected impact in terms of claims.

[70] Premium provision based on loss ratio assumptions may be modified resulting in an increase of the technical provisions. However, the cyber events specified in the scenario might be considered as a one-off event, therefore, as a simplification, no adjustment to the technical provisions is expected in the full pay-out approach.

141. Cyber underwriting scenarios are expected to be applied at a granular level for individual insurance products and policyholders. In the following, the impact of cyber underwriting stresses is further explained and the stress on insurance products and guarantees is detailed. For most products, the different shocks will impact frequency and/ or severity of the total insurance claims.

142. A general distinction can be made between affirmative cyber and silent cyber. For affirmative cyber, the insurance undertaking offers an explicit (stand-alone or add-on) cyber coverage to its policy holder. For silent cyber, the coverage of cyber is implicit due to imprecise policy wording or by not explicitly including or excluding cyber as a covered risk.

143. For both covers, it is expected that the undertaking will assess at policy level whether the cyber incident leads to an insurance claim and quantifies the claims cost. The undertaking can make use of an absolute amount based e.g. on an average observed claims cost or on a relative amount based on the typical damage caused by a specific cyber incident. Such values can of course differ between the different types of policyholders and a specific granularity might need to be considered.

144. Hereafter an overview of the different product lines or guarantees impacted are presented as well as an overview of the potential shocks for each scenario.[71] These shocks have been observed in the cyber underwriting stress tests that undertakings developed e.g. within their ORSA. Some insurers have more simplified approaches, while some other undertakings have more sophisticated set-ups. However, the shocks mentioned below maintain a balance between the different approaches observed.

Table 10 – Cyber underwriting scenarios and their shocks

	SCENARIO		
PRODUCT LINE OR GUARANTEE	**Ransomware**	**Power Outage**	**Cloud Outage**
All products (non-life)	Infection rate	Geographical location risks Duration of the power outage	Market share impacted cloud Duration of the outage of the cloud infrastructure
(Contingent) Business Interruption	Average duration interruption Loss in profit per day	Average duration interruption Loss in profit per day	Average duration interruption Loss in profit per day

[71] The selection of the shocks in future exercises will depend on the narrative of the scenario and on the information available for their calibration.

Crisis service costs	Average cost IT forensics Average cost Notification	Average cost IT forensics Average cost Notification	Average cost IT forensics Average cost Notification
Recovery expenses	Recovery expenses	Recovery expenses	Recovery expenses
Professional Indemnity	Average cost per claim	Average cost per claim	Average cost per claim
Director's and Officer's	Average cost per claim Stock price depreciation Probability for a negative outcome of a court case	Average cost per claim Stock price depreciation Probability for a negative outcome of a court case	Average cost per claim Stock price depreciation Probability for a negative outcome of a court case
Other product lines or guarantees (silent or affirmative cyber)	Average cost per claim	Average cost per claim	Average cost per claim
Cyber Extortion	Average ransom amount Propensity to pay ransom		
Data exfiltration	Average cost per client per infected policyholder		
Property Damage		Average claim during power outage	
Regulatory fine / damages	National legislation (per claim)		

145. Some of the shocks mentioned in Table 10 may be portfolio specific. Next to the average duration of business interruption, this may e.g. hold for the total lost profit per day of interruption as it would depend on the turnover of the individual policyholder and the relative reduction in gross profit margin which can be specific to the economic sector in which the policyholder operates.

146. The scenarios can also trigger crisis management service costs such as IT forensics and notification of victims, but also recovery expenses. For this element, an average cost per infected policyholder can be determined to calculate the total insurance claims.

147. Moreover, the design of the shock and the calibration should take into account the practical implications of a sudden increase in the frequency of the cyber incidents. For resolving these incidents, insurers tend to rely on expert suppliers, typically called "Incident response managers" or more precisely "IT forensic experts". The first task of these IT forensic experts is

to identify the root cause of the cyber infiltration in order to be able to detect and respond and then to decide whether the ransom is worth paying. The resources of these suppliers in terms of available experts are not infinite. So, a major increase in the frequency of cyber events could end up in the shortage of resources and ultimately have the following consequences:

- Insured would be more inclined to pay the ransom, and possibly paying it uselessly (paying the ransom gives no warranty that all the issues are solved).
- Insured would take more time to restore their IT services and the average duration of business interruption would increase.

148. For the calibration of the shocks EIOPA could also consider a collaboration with other European agencies or platforms (e.g. ESRB, ENISA, Joint Cyber Unit), practitioners, academia and model vendors.

6.3 METRICS

149. The aim of these metrics is to provide a comprehensive overview of the major drivers behind the impact of the prescribed scenarios on the Solvency II Balance Sheet and on the Profit and Loss of the participants. Given the doubts of appreciation of the silent cyber exposures, evaluation metrics should focus both on quantitative and qualitative aspects, in order to be able to build severe but plausible scenario(s), with the scope set on claims, premiums and risk retention.

150. Scenarios will have the common goal of the assessment of the change in Balance Sheet, Own Funds, SCR, SCR Ratio as consequences of shocks that were applied. EIOPA will follow, as for the other risks, a staggered approach starting from balance sheet metrics and moving to solvency metrics at a later stage if not explicitly requested.

151. The clear identification of the exposures to affirmative cyber coverages (both on a standalone basis and with cyber as an add-on coverage) allows a clear estimation of the impacts stemming from a potential increase in frequency and severity of the claims against the prescribed scenarios.

152. The potential for silent coverages increases the complexity of the estimation of the exposure, which might be approximated by the overall exposure towards specifically identified business lines. Additional complication comes from the potential litigations stemming from denial of reimbursement upon claims related to silent exposures where the cyber coverages are not explicitly excluded.[72]

[72] Supervisory experience shows that the estimation of exposures may also be complex for the contracts that are initially not intended to cover cyber risk, but still are affirmatively including that risk, though this is not the main part of the insured risk (typically, contracts formerly including a silent exposure, whose wording has been reviewed to affirmatively include that risk).

153. The proposed metrics should therefore account for both silent and affirmative coverages in terms of baseline and stressed exposures. Metrics for those coverages take into account all the business lines that are potentially exposed to non-affirmative or affirmative cyber risk (total GWP, claims, TP).

Table 11 – Cyber underwriting metrics

METRIC	Description
TP for Affirmative cyber products (change of) gross and net	Baseline Vs Adverse Assuming a full reserving of the claims To be reported separately for: • cyber standalone coverages; • products with cyber as add-on coverage but main risk being covered; • products with cyber as add-on coverage and not as main risk being covered.
Claims Paid for Affirmative cyber products (change of) gross and net	Baseline Vs Adverse Assuming a full payout of the claims To be reported separately for: • cyber standalone coverages; • products with cyber as add-on coverage but main risk being covered; • products with cyber as add-on coverage and not as main risk being covered.
TP Claims for non-Affirmative cyber products (change of) gross and net	Calculation by participant or estimation Baseline Vs Adverse Assuming a full reserving of the claims
Claims paid for non-Affirmative cyber products (change of) gross and net	Baseline Vs Adverse Assuming a full payout of the claims
Loss ratio for affirmative cyber products	Baseline Vs Adverse To be reported separately for: • cyber standalone coverages; • products with cyber as add-on coverage but main risk being covered;

	• products with cyber as add-on coverage and not as main risk being covered.
Loss ratio for non-affirmative cyber products	Baseline Vs Adverse Based on provided parameters in absence of explicit exclusions
Liabilities (change of)	Baseline Vs Adverse It can be limited at an initial stage to the change of TP
Assets (change of)	Baseline Vs Adverse To be considered in case of full payout of claims
Excess of Asset over Liabilities (change of)	Baseline Vs Adverse
Assets over Liabilities (change of)	Baseline Vs Adverse
Eligible Own funds (change of)*	Baseline Vs Adverse
SCR, SCR underwriting (non-life)*	Baseline Vs Adverse
SCR ratio*	Baseline Vs Adverse
Expected losses if key exclusions are not applicable under stress	Adverse

* to be considered at a later stage.

154. The metrics can be complemented by a set of information on the baseline exposures towards affirmative and non-affirmative cyber risk. Such information, included without aim of completeness in Table 12, serves to build a better picture of the risk profile of the undertakings and potentially for validation purposes.

Table 12 – Ancillary indicators

INDICATORS	Comments
GWP for Affirmative cyber products gross and net	Baseline To be reported separately for: • cyber standalone coverages; • products with cyber as add-on coverage but main risk being covered; • products with cyber as add-on coverage and not as main risk being covered.
GWP for non-Affirmative cyber products gross and net	Baseline (estimation)
Reinsurance retention	Baseline

	For whole portfolio and each cyber product It can be calculated from net and gross claims and WP
Top X exposures (number of policies and/or sum insured) of policyholders to Third Parties	This metrics has the scope of estimating the accumulation of exposures for cyber insurance per IT service provider whose services are used by policyholders.
How many unique insurance products allocated to LoBs?	Baseline
How many of these unique insurance products are potentially affected by silent cyber?	Baseline
How many of these unique insurance products have a cyber exclusion?	Baseline
How many of those (cyber exclusions) have occurred due to active contract adjustment in the recent past?	Baseline
Products weights as TP Claims & GWP in LoB	Baseline

155. The quantitative metrics described in the table can be complemented by qualitative information, such as information on the existence of reinsurance agreements for affirmative cyber. Such information might allow for an accurate quantification of the impact of the shocks. Usually, due to big amounts of sum insured, undertakings have both: Excess of loss and proportional treaties.

156. The above presented metrics have the aim of reflecting a quasi-complete overview of the financial statements of undertakings. Their role is to be used in order to estimate the net financial impact.

157. The next sections provide further information on possible shocks that can be taken into account against the background of the different scenarios and the silent cyber risk.

6.4 EXAMPLES OF APPLICATIONS

6.4.1 RANSOMWARE

158. Under a systemic ransomware scenario, a threat actor delivers a ransomware amongst a large number of economic actors and a multitude of policyholders are impacted. Typically, the ransomware encrypts the data and therefore it results in a loss or in an exfiltration of information which can even lead to the private data becoming public. However, the threat actor asks a ransom from the policyholder in exchange for the key to decrypt the ransomware.

159. The ransomware will be spread and infect a multitude of policyholders. The infection rate of policyholders impacted will be the main driver of claims frequency. The historical data

observed during larger ransomware events can be used to calibrate the infection rate. However, given that historically no fully systemic ransomware event has yet been observed, expert judgement should be used to supplement the existing data and to assure that the scenario is sufficiently representative of tail risk. A distinction could be made between the direct exposure in terms of infected policyholders and the indirect exposure in terms of critical vendors and suppliers which trigger Contingent Business Interruption coverages.

160. It is observed that not all infected policyholders pay the ransom. This would typically depend on the existence of a back-up and incident response plan. If the policyholder has a recent back-up, the data can more easily be restored and the ransom does not need to be paid. However, policyholders which do not have a back-up or incident response plan do not have this option and might therefore be more inclined to pay the ransom.

161. However, until the data is restored or decrypted, (part of) the business of the policyholder is interrupted. The lost gross revenue during this period can be insured in some cases by a business interruption policy or coverage within a cyber policy. This would depend on the individual data of the infected policyholder, but also on the average duration of the interruption caused by the ransomware.

162. Also, in the case of Contingent Business Interruption policies, the average duration of the interruption of the critical vendor or supplier will be a determining factor. Claims data can be used to determine this average duration. Otherwise, in some cases recovery curves can be constructed where the propensity to recover per time step is determined. This last approach allows a more granular consideration of contractual deductibles and limits. It can also be considered for the determination of the recovery time whether the policyholder has a back-up or incident response plan which could shorten business interruption. It is observed that the size of the undertaking can be a determining factor in the recovery process. Larger undertakings might have a better cyber hygiene leading to a faster recovery. Therefore, size could be a determining factor in the calibration of the average duration of the interruption.

163. Furthermore, the ransom amount can be calibrated as an average amount based on the claims history of the undertaking or external data from public providers. This amount can be very different amongst undertakings. It is therefore useful to consider whether aspects such as the size or the economic sector wherein the policyholder operates have an influence. The propensity to pay the ransom can be determined in a similar manner. For this shock, it should be noted that local mitigation measures or legal environment might restrain the propensity to pay the ransom in certain countries.

164. Moreover, if data exfiltration occurs, it is also expected that this would generate a cost. Typically, it is observed that this costs increases with the number of records exfiltrated. It would for instance be possible to determine an average cost per record. This cost would also be different according to the type of information. Indeed, financial and health information might be more sensitive and therefore lead to higher costs. The type of data exfiltrated would of

course be different between economic sectors where some might have more access to such sensitive information. This would then imply that different economic sectors have different average costs.

165. An illustrative and not exaustive set of shocks , excerpted from Table 10, is presented in Table 13.

Table 13 – Ransomware shocks

Shock	Description
Share of policyholders affected	Infection rate (% of total policyholder per affected business-line).
Share of policyholders that opt to pay ransom	% of affected policyholders that have ransom coverage that opt to pay the ransom
Ransom amount	EUR
Average duration interruption	days
Loss in profit per day	Revenue loss per day (EUR). It can be specified per sector (NACE code)
Recovery expenses	One off expenses (EUR) per affected policyholder

166. The impact should be measured based on the standard Solvency II metrics described in section 6.3.

6.4.2 CLOUD OUTAGE

167. Under a cloud outage scenario, a cyber incident at a cloud service provider (such as misconfiguration or a cyber attack) leads to an interruption of infrastructure, platform and software services provided leading to an interruption in the activities of the business who make use of the cloud. After the outage is restored, the business operations also recover after some time.

168. The outage of the cloud service provider will lead to interruption of the infrastructure, the platform and software services and the business operations making use of the services. The claims frequency resulting from this outage would be based on the market share of the cloud service provider as it is present in the portfolio of the insurer. A distinction can be made between the direct exposure of the business operations impacted which make use of the cloud services and the indirect exposure resulting from critical vendors and suppliers of the policyholders which make use of the cloud services and which triggers Contingent Business Interruption coverages.

169. For these different undertakings, the average duration of the interruption should be defined. For the cloud itself, it is possible that the infrastructure is not recovered instantaneously and that activities build up gradually e.g. because not all data centers are restored at the same time. Similarly, for PaaS and SaaS service providers and business the recovery can be gradual. A possibility exists therefore to have a finer granularity than a simple average per type of undertaking and to define instead a recovery curve which defines a percentage of undertakings which has recovered after a number of time. Such a more granular approach allows to capture the deductible and limit for BI and CBI covers in a more precise manner. Similarly to the ransomware scenario, it can also be considered for the cloud outage event that for the determination of the recovery time whether the policyholder has a back-up or incident response plan which could shorten business interruption. It is observed that the size of the undertaking can be a determining factor in the recovery. Larger undertakings might have a better cyber hygiene leading to a faster recovery. Therefore, size could be a determining factor in the calibration of the average duration of the interruption.

170. An illustrative and not exaustive set of shocks, excerpted from Table 10, is presented in Table 14.

Table 14 – Cloud outage shocks

Shock	Description
Share of policyholders affected	% of total policyholder per affected business-line. Concentration rate can increase the number of affected policyholders.
Average duration interruption	days
Loss in profit per day	Revenue loss per day (EUR). It can be specified per sector (NACE code)
Recovery expenses	One off expenses (EUR) per affected policyholder

171. The impact should be measured based on the standard Solvency II metrics described in section 6.3.

6.4.3 POWER OUTAGE

172. During a business blackout scenario, a cyber incident at an energy company leads to a load shedding and ultimately to a full power outage in a specific region or country. This would of course lead to business operations being directly interrupted in this region and would trigger insurance claims. After some time, the cyber incident is resolved at the energy company, power is restored, and business operations start again. In general, it is observed that load shedding plans can be in place to avoid outage in critical parts of the economy. But if the cyber incident has a large impact, this could not be avoided.

173. It can be assumed that all businesses which reside in the affected region are fully impacted. The claims frequency of the event can therefore be based on the geographical location of the policyholder or of the critical vendors and suppliers in case of a Contingent Business Interruption policy.

174. Property damage can be expected in different actors of the economy. Firstly, the power outage might lead to material damage at the power provider when the incident occurs or when power is restored. Also, the sudden restoration of power can lead to damages and ultimately insurance claims. Secondly, it is observed that the risk of theft is increased when a power outage occurs. Lastly, refrigerated goods might be spoiled because of the power outage for businesses and families. Undertakings can use the average claim cost during power outages to calibrate the insurance losses. Here the specific geographical region can be considered as well as the duration of the power outage. Indeed, since it was triggered by a cyber incident, the outage might last longer than historically observed by the insurance undertaking.

175. The power outage itself is consider having a gradual recovery were not all power is restored at once and not all businesses are immediately operational again. During the downtime, it can however be assumed that the affected facilities are 100% impacted. Based on the average duration of the interruption the relevant claims cost can therefore be defined. It is possible to have also for the blackout scenario a finer granularity than a simple average per type of undertaking and to define instead a recovery curve which defines a percentage of undertakings which has recovered after a number of time. Such a more granular approach allows to capture the deductible and limit for BI and CBI covers in a more precise manner. Next to the average duration, the total lost profit per day of interruption is expected to be 100% for the affected facilities in the geographical region.

176. For the power generation companies, an additional cost would be expected to occur. It is possible that the cyber incident for the power generation company would result in regulatory fines and that damages would need to be paid to impacted businesses and families. This would of course be highly dependent on the national legislation applicable for the power outage.

177. An illustrative and not exaustive set of shocks, excerpted from Table 10, is presented in Table 15.

Table 15 – Power outage shocks

Shock	Description
Share of policyholders affected	% of total policyholder per affected business-line. Concentration rate, based on the geographical location of the power outage, can increase the number of affected policyholders.
Average duration interruption	Hours
Recovery expenses	One off expenses (EUR) per affected policyholder

178. The impact should be measured based on the standard Solvency II metrics described in section 6.3.

6.5 SILENT CYBER: ADDITIONAL GUIDANCE

179. Next to the elements mentioned in the scenario-specific paragraphs, which relate more to affirmative cyber, it is also expected that silent cyber cover might be triggered if no appropriate exclusions are put in place. For instance, it can be expected that in General Third Party Liability certain products would lead to insurance claims.

180. More concretely, for Professional Indemnity (PI) or Errors & Omissions (E&O), it is possible that for the following:

- Ransomware
  IT service providers or IT professionals are insured. The cyber threat actor would of course be directly responsible for the ransomware. However, the IT service provider might have made a professional error which would result in a liability and ultimately could lead to insurance claims. Moreover, for other companies, it is possible that when the data is exfiltrated that this is in part due to professional negligence. The lacking ICT risk management of the policyholder could have allowed the data to be exfiltrated which would trigger a liability towards its clients. For both the IT and non-IT companies, an average cost per claim could be used to determine the total insurance claim. To consider more directly the number of clients of the policyholder which are impacted, the average cost per claim could be differentiated according to the size of the policyholder. A further possibility would be to immediately make use of an average cost per client of the policyholder.
- Cloud outage
  IT service providers or IT professionals are insured. The cloud service providers (IAAS,PaaS & SaaS) are liable for the interruption of activities. An average cost per claim can be used which should consider the length of the duration and the type of company which might lead to higher claims.
- Power outage
  Energy companies are liable for the power outage. Also the impacted businesses might be liable if this would result in delayed projects and if these consequences could have been avoided in a reasonable manner. Furthermore, it the energy companies made use of specific IT solutions to defend themselves from cyber incidents, it is expected that also the IT service providers have a Product Liability if these solutions did not provide the required result. An average cost per claim can be used which should consider the length of the duration and the type of company which might lead to higher claims.

181. For Director's and Officer's (D&O) liability, the rationale can be similar as for PI or E&O. The professional negligence of directors and officers (of IT and non-IT companies or cloud PaaS and SaaS service providers, depending on the scenario) could result in a liability towards for instance its shareholders. Also in this could an average cost per claim be used to calculate the total insurance loss for unlisted undertakings. For listed undertakings, a cost per claim could be determined at the level of the policyholder based on its market capitalisation and the expected depreciation of the stock price due to a systemic ransomware. Of course would not all ransomware attacks result in an insurance claim since this would indeed typically depend on the outcome of the court cases. A probability for a negative outcome of the court case can therefore be used.

182. Silent cyber is also observed in other Property and Casualty product lines. Undertakings could calculate the insurance claims from these other lines based on an average cost per claim. Products offering cyber asan add-on coverage and not as the main coverage should be treated as explicit cyber in case undertakings have a sufficient granular view of the exposures. Otherwise, they can be treated as silent cyber.[73]

183. More specific methodologies in line with the characteristics of the product line can also be envisaged.

6.6 DATA ELEMENTS

184. The information collected in the context of a cyber stress test exercise should cover, as for other tress test exercises, the exposures under baseline and adverse scenario. As a principle the data collection should be limited only to the quantitative and qualitative information needed to analyse the impact of the prescribed scenario and for validation purposes.

185. While the metrics for the cyber underwriting are inspired by the Solvency II framework, the specificity of the risks and the current lack of granular reporting under the regular Solvency II reporting does not allow to fully rely on standard templates. In the future, EIOPA could rely on the information to be reported in template S.14.03 on cyber underwriting risk (which is part of the 2020 review of Solvency II).[74]

186. The information collected should allow for a proper assessment of the impacts of the shocks to the Solvency II balance sheet (e.g. S02.01) and a breakdown of the impacts on the liability side in terms of:

- Technical provisions for line of business (ref. S.17.01);[75]

[73] Please refer to footnote 72.

[74] Draft Amended Implementing Technical Standards (ITS) on supervisory reporting and disclosure – ITS on supervisory reporting. Available here: https://www.eiopa.europa.eu/document-library/technical-standard/draft-amended-implementing-technical-standards-its-supervisory_en.

[75] Reference to QRT templates serves as a simple indication to the type of information to be collected.

- Evolution of the claims by line of business (ref. S.05.01);
- Evolution of the technical provisions by line of business (ref. S.17.01);
- Ceded part of the risk (ref. S.30.03).

187. The information shall be collected separately for the affirmative and non-affirmative exposures. Additionally, specific information on the potential accumulation of risk due to common exposures to specific IT service providers might also be collected.

188. Annex 9.4 provides some examples of templates for the cyber underwriting component. It is important to note that these templates are for illustrative purpose only. EIOPA could adjust the information requested and granularity of the templates depending on the specificity of a future stress test exercise with focus on cyber risk.

Questions:

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

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.

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.

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

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

7 CYBER RESILIENCE: SHOCKS, SPECIFICATIONS AND METRICS

7.1 GENERAL GUIDANCE

189. As for cyber underwriting, the application of cyber resilience shocks and the calculation of the impacts should rely as much as possible on the standard EIOPA framework for stress testing with respect to: estimation of the impacts (fixed balance sheet), evaluation of the impacts (Solvency II balance sheet) and to the Solvency II framework. It is worth noting that for the assessment of the cyber resilience the prescribed shocks materialize over a defined period of time (e.g. hours, days). While undertakings should estimate the deriving costs over such elapsed time, the impacts should be reflected in the P&L and/or Solvency II balance sheet at the reference date.

190. The metrics used to measure the impact to an insurance undertaking should be consistent with the Solvency II framework and specifically with the balance sheet provisions therein. The valuation of the impacts will be initially limited to the impact on the assets, liabilities and eventually to the excess of assets over liabilities. No evaluation of the impacts on the solvency position (i.e. Own Funds and Solvency Capital Requirement) will be expected at a first stage unless explicitly requested and after careful cost/benefits considerations.

191. As discussed in section 2, the consequences of a cyber event can be traced back to an increase in operational and other costs associated to business interruption (including loss of revenue corresponding to lost business during the duration of the cyber event) and to detection and recovery costs. These costs impact the profit and loss and balance sheet of the stressed undertakings.

192. Given that shocks related to cyber events are expected to lead to an increase in operational and other costs, they can be reflected on the insurance balance sheet in two ways:

- Via a full provisioning of the costs triggered by the prescribed shocks.
- Via a full payout of the costs triggered by the prescribed shocks.

193. Conscious of the fact that the in reality the approach taken by insurers lays in between the two extremes listed above, the proposed approximations allow for a controlled and homogeneous assessment of the impacts to the balance sheet of the companies.

194. In case of full provisioning, the prescribed increase in costs should mainly result in an increase of the provisions other than technical provisions.[76]

[76] Depending on the nature of the costs they might be split between provisions other than technical provisions and contingent liabilities.

195. In case of full payout of the costs, the major impacts should be registered as a reduction in cash and equivalent, and a potential reduction in the investment portfolios in case the amount of cash and equivalent held at the reference date is not sufficient to cover the cash outflows deriving from cost of recovery.

196. Impacts are expected on other balance sheet items, e.g. deferred tax assets and liabilities. For this, simplifications and approximations might be defined and agreed in line with EIOPA stress test standards.

197. Section 7.2 elaborates on the shocks for each of the relevant scenarios identified for the cyber resilience component.

7.2 SHOCKS

198. Based on the considerations in section 5, cyber resilience shocks and their specification are presented for all the five scenarios in the scope of this paper.

199. Table 16 lists the possible shocks for all the scenarios considered in the cyber resilience component. Shocks are in general linked to the downtime of the relevant infrastructures or systems affected by the cyber event (outage time) and the type of business processes affected (e.g. distribution activities, claims handling, etc.). These shocks should allow the participating undertakings to properly estimate the time to recover from the cyber event and the financial costs associated both to interruption of business and recovery.

Table 16 – Cyber resilience scenarios and their shocks

	Scenarios				
	Cloud Outage	**Ransomware**	**Data Breach**	**Power outage**	**DoS**
Shocks	Outage time	Business processes affected Penalty factor on recovery times	Percentage of data breached Percentage of sensitive data breached	Outage time	Business processes affected Outage time

7.3 METRICS

200. Cyber resilience is the capability of an insurance undertaking to sustain the operational and financial effect of an adverse cyber-event. As discussed in section 2, cyber attacks can cause to the insurer direct financial losses or indirect financial losses due to unavailable systems, restoration and loss of reputation.

201. To assess and measure the degree of cyber resilience, operational and financial metrics should be used. The purpose of the operational metrics is to measure the impact of an adverse cyber scenario on the continuity of critical business services. Thus, they should inform on the level of operational resilience of participating undertakings. On the other hand, financial metrics assess the impact on the insurer profit and loss and balance sheet. The latter should inform on the undertakings' financial resilience following a cyber event. The financial impact of an adverse cyber scenario is in most instances strictly related to the operational resilience of an undertaking, i.e. the longer it takes to restore the affected systems or business processes or the more critical they are, the higher the expected costs associated to business interruption and to restoration.

202. Contrary to the cyber underwriting component of this paper, for which standard financial metrics can be used and some work has already been developed by other supervisors, work to assess the impact of cyber resilience scenarios is still incipient and more initiatives are needed to develop common cyber resilience metrics. Against this background, this section aims to propose an indicative list of potential metrics relevant for the proposed scenarios. Given the exploratory nature of this work, this list shall not, in any case, be seen as exhaustive.

203. Table 17 describes the operational and financial metrics proposed to assess the impact of the cyber resilience scenarios considered in this paper.

Table 17 – Cyber resilience metrics

	Metric	Description
Operational	**Time elapsed until return to business as usual (time to BAU)**	Adverse Average time to restore operations after the shock, i.e. mean time elapsed between initial notification and resuming normal level of operations.
	Business processes affected *	Adverse List of business processes that are affected by the attack.
Financial	**Operational and other costs (change of)**	Baseline Vs Adverse Operational and other costs should comprise business interruption costs, including loss of revenue corresponding to lost business during the downtime, and detection and recovery costs.
	Total Assets (change of)	Baseline Vs Adverse (in case of payout)
	Total Liabilities (change of)	Baseline Vs Adverse (in case of provisioning)
	Excess of Asset over Liabilities (change of)	Baseline Vs Adverse

	Provision other than technical provisions (change of)	Baseline Vs Adverse
	Contingent liabilities (change of) **	Baseline Vs Adverse
	Impact on Own Funds (change of) ***	Baseline Vs Adverse
	SCR***	Baseline Vs Adverse
	Solvency Ratio ***	Baseline Vs Adverse

* In some scenarios, this can be defined as a shock.
** As explained in section 7.1, depending on the nature of the costs they might be split between provisions other than technical provisions and contingent liabilities.
*** To be considered at a later stage. Specific considerations shall be devoted to the SCR_{op} component and its constituents which are not suitable for event-based assessment.

204. To measure the operational impact of a cyber resilience scenario, insurers must estimate the average time to fully restore operations after a cyber incident. Moreover, they should assess the business processes that would be affected by the scenario (e.g. pricing, distribution activities, claims handling, etc.). As explained above, damage done on the infrastructure of the insurer, time and cost to restore the system and loss of business will all create exceptional losses.[77] These exceptional losses will impact the balance sheet of the insurer either through a reduction on the asset side in case the costs for recovery are instantly paid or through an increase of the liabilities in case the costs are provisioned. The cost of the incident should depend heavily on the time to BAU.

205. The metrics presented in Table 17 could be complemented by other qualitative information with the aim of better assessing the cyber security practices of the participating undertakings and e.g. availability of backup systems. This information will be considered in section 7.5.

206. Section 7.4 provides further information on possible shocks for each of the cyber resilience scenarios.

7.4 EXAMPLES OF APPLICATIONS

7.4.1 CLOUD OUTAGE

207. This scenario deals with the possibility of losing access to the data centers of the company where its core applications and databases supporting business operations are located. This will affect the ability of the employees to carry out their daily work and, also, the clients and partners will not be able to access the company's websites and associated services. This

[77] Regulatory fines and compensation against legal actions might be expected in some scenarios, but are not included in the scope of this paper.

scenario can be caused by misconfiguration or accident in the IT infrastructure or by deliberate attack, most probably a ransomware.

208. As part of the stress scenario, companies should be provided with the infrastructure outage time (in hours) as a shock. The outage time should be dependent on the in-/out-sourcing model of the company, i.e. on whether the data center is an internal infrastructure operated by the company itself or an infrastructure provided by a specialized vendor (e.g. Microsoft, Amazon, Google...).

209. In the case of companies that own and operate their own data centers, the difficulty to restore services could be higher due to the time needed to procure specialized technicians/materials to tackle an abnormal situation. Even the first steps to determine the root cause of the problem could require technical know-how beyond the usual expertise of in-house personnel.

210. On the other hand, data centers operated by big cloud providers will not suffer this shortcomings or, at least, not to a comparable degree, as this type of problems fall squarely within their area of expertise and because their own business depends on having extremely quick recovery times.

211. The outage time could be calibrated based on historical data, when available. Examples of potential relevant sources in this regard include the following:

- Annual outage analysis 2021 - The causes and impacts of data center outages
- Understanding the Cost of Data Center Downtime - An Analysis of the Financial Impact

212. A typical set of shocks, excerpted from Table 17 , is presented in Table 18.

Table 18 – Cloud outage shocks

Shock	Description
Outage time	Outage time (in hours) dependent on whether: i) the data center is an internal infrastructure operated by the company; or ii) an infrastructure provided by a specialized vendor (Microsoft, Amazon, Google...).

213. The impact of the shocks should be measured based on the operational and financial metrics described in section 7.3.

214. This scenario could affect every IT service that requires access to centralized applications and databases, rendering every IT service unavailable except for the general purpose programs that run exclusively in the employees' PCs (i.e. Excel, Word, Power Point). Internet access, e-mail and phone communications should not be affected as a general rule. Depending on the company IT architecture, certain business processes will be affected. The impact will be higher in companies with higher concentration of IT services and lower in those where these are delegated in their offices/branches.

215. Against this background, for this scenario, in addition to the estimated time to BAU and financial impact (via operational and other costs), it would be relevant to assess the impact on the continuity of business processes. As such, companies should provide the list of affected processes, which could include, without aim of completeness:
   i. Pricing
   ii. Distribution activities
   iii. Claims handling
   iv. Annuity payments processes
   v. Policy and documentation issuance
   vi. Additionally all the activity of administrative, investment and management departments.

216. To estimate the time to BAU, companies should assess how long it would take to restore their operations fully once the affected infrastructure is recovered (assuming recovery of the business processes might not take place coincidently with the recovery of the affected infrastructure).

7.4.2 RANSOMWARE

217. This scenario reflects the undertaking's network being infected with encryption malware. This will initiate a large scale encryption of databases, fileshares and possibly even system components, across the whole enterprise infrastructure. Once encrypted, data is functionally considered lost and needs to be restored from backups. Note that, in practice, this scenario can often occur together with a data breach scenario.

218. In this scenario, undertakings would be prescribed with the list of business processes compromised by the attack, which would become disabled and require restoration. In contrast to data center outages, Ransomware can affect the whole network of an undertaking even if multiple redundant sites are in operation. Basically, only an organisation's cyber defences and IT-security measures can limit the spread of such malware. Depending on how successful these are in mitigating the impact, a certain percentage of critical data will be affected by the attack.

219. When considering a severe Ransomware infection, the possibility of damage to vital infrastructure needed for recovery needs to be taken into consideration:
   - Backups can be directly affected if they are not stored offline (e.g. on tapes), or if the attackers have used *wipers* or malware that remained dormant for a longer period of time and has been copied into the backups themselves;
   - Vital configurations and system components can be lost, in the worst case an attacker can achieve domain administrator status and lock IT-personnel out of their systems;
   - Server and client devices that are completely locked or suspected to be infected with hidden backdoors might have to be physically replaced.

220. Any of these factors would be a hindrance to recovery efforts and these possibilities should be taken into account in a severe Ransomware scenario. Therefore, a penalty factor on recovery

times could be considered as an additional shock under this scenario. This factor would reflect the potential longer time of recovery due to encrypted backups and configurations and should be multiplied by the expected time to BAU (factor >1).

221. The potential payment of ransom is not included as a shock, but it could be considered at a later stage.

222. Historical data for Ransomware attacks is available. This is often spread across case studies or small-scale surveys. In the context of stress testing, both types of sources can be useful - the former especially for supporting a plausible worst-case scenario, the latter for correlating these with estimated average values. The following selection of sources has been made to support the calibration:

- Case Studies:
  - Health Service Ireland Conti Attack
  - NotPetya Attack effect on Maersk
  - NotPetya Attack effect on FedEx
- Statistics and Surveys:
  - IBM Report on cost of Data Breaches
  - Varonis Ransomware Statistics
  - Purplesec Ransomware Statistics

223. A typical set of shocks, excerpted fromTable 17, is presented in Table 19.

Table 19 – Ransomware shocks

Shock	Description
Business processes affected	List of business processes that are disabled and need to be restored.
Penalty factor on recovery times	Factor reflecting the potential longer time of recovery due to encrypted backups and configurations, to be multiplied by the expected time to BAU (factor >1).

224. The impact of the shocks prescribed under this scenario should be measured based on the operational and financial metrics described in section 7.3.

7.4.3 DENIAL OF SERVICE (DOS)

225. A DoS attack is launched against the participating undertaking or a service provider, resulting in unavailability of entire customer database and a short term IT systems outage. This scenario excludes permanent damage to IT system and ransom payments.

226. Under a DoS attack, the company's IT system faces a certain number of hours downtime including mobile and web-based operational systems, affecting most of undertaking's business processes for the duration of the interruption. Accordingly, under this scenario, as for the

Ransomware attack, participating undertakings would be prescribed with a list of business processes that would be disabled by the DoS attack as well as with the duration of the services interruption (outage time).

227. Shocks could be calibrated based on public data, if available. Examples of potential data sources include:

- 20+ DDoS attack statistics and facts for 2018-2022 (comparitech.com)
- Understanding the Cost of Data Center Downtime - An Analysis of the Financial Impact
- AXA Faces DDoS After Ransomware Attack - Infosecurity Magazine (infosecurity-magazine.com)

228. A typical set of shocks, excerpted from Table 16, is presented in Table 20.

Table 20 – DoS shocks

Shock	Description
Business processes affected	List of business processes that are disabled and need to be restored.
Outage time	The amount of time (in hours) until the affected services are available again.

229. The impact of the shocks prescribed under this scenario should be measured based on the operational and financial metrics described in section 7.3.

230. It should be noted that under a DoS attack, in contrast to a Ransomware attack, the financial impact through recovery efforts will usually be limited in duration, as no permanent damage to hardware and software is expected. In the short term, however, overtime and external support might be necessary.

7.4.4 DATA BREACH

231. This scenario reflects the infiltration of malicious actors into the organization's network that have managed to extract sensitive data and the consequences deriving from this infiltration. In practice, this scenario can often occur together with a Ransomware attack.

232. Possible shocks in a data breach scenario, even if in combination e.g. with a Ransomware scenario, would be the percentage of data and/or sensitive data that is breached.

233. As for other scenarios, shocks could be calibrated based on public data, if available. Examples of potential data sources include:

- IBM Report on cost of Data Breaches;
- Techjury – Data breach statistics
- Varonis – Data breach statistics

234. A typical set of shocks, excerpted from Table 17, is presented in Table 21.

Table 21 – Data breach shocks

Shock	Description
Percentage of data breached	Percentage of data that are breached after the attack (%).
Percentage of sensitive data breached	Percentage of sensitive data that are breached after the attack (%).

235. The impact of the shocks prescribed under this scenario should be measured based on the operational and financial metrics described in section 7.3 .

236. The time to recover from a data breach (time to BAU) should take into account the total time needed for the many components of data breach: detection and escalation; notification; ex-post response.

237. Estimates of direct costs from a data breach scenario should consider all the activities needed for the detection and mitigation of the impact of the event and to restore records breached (where feasible). In contrast to other scenarios, these costs are likely to be limited as the attack in some cases might even go unnoticed.

238. Indirect costs are predominant in this scenario and could include:

- the decrease of future premiums due to loss of reputation;
- the fees due to central authorities regulating data privacy;
- the legal actions from consumers / consumers associations.

239. The cost of a data breach incident would closely depend on the volume of data breached.

240. As discussed in sections 3 and 5, indirect costs as described above are out of the scope of this paper, making this scenario less relevant on a standalone basis.

7.4.5 POWER OUTAGE

241. This scenario reflects the impact on the operational activities of an undertaking stemming from the usage, by a threat actor, of vulnerabilities in the regional/national electricity sector and grid systems or from a failure in the grid that leads to a power outage. The shock should be applied in the regions where the main activities of the participants are located (head office, data storage, etc.).

242. This will affect most of undertaking's business processes for the duration of the power interruption and, as power is restored, undertakings would recover without a permanent damage to ICT infrastructure and systems.

243. In contrast to other scenarios, where only a part of the ICT infrastructure might be impacted, most business processes would come to a standstill during a power outage, affecting most operations of undertakings. These may include communications, administrative activities, management departments, and interrupt services such as pricing, claims handling and payment processes.

244. Accordingly, the shock in this scenario would be the outage time, i.e. the period during which the power is out, and the undertaking's operations are interrupted. The shock should be applied in the region(s) where the main activities of the participants are located (head office, data storage, etc.).

245. To calibrate the duration of a power outage, aspects such as location area of the incident might be considered, as well as immediate or gradual power restoration. Historical information on the duration of power downtimes may be used in order to calculate a realistic figure. Some statistics can be found in public reports or websites, which can be used for calibrating the duration and estimating the costs associated with a power outage scenario, such as:

- https://www.pnnl.gov/main/publications/external/technical_reports/pnnl-13797.pdf
- https://link.springer.com/content/pdf/bbm:978-1-4020-4364-2/1.pdf
- https://raeng.org.uk/media/2s2pgeeg/single-pages-counting-the-cost-report.pdf

246. A typical set of shocks, excerpted from Table 17, is presented in Table 22.

Table 22 – Power outage shocks

Shock	Description
Outage time	Period during which the power is out, and the undertaking's operations are interrupted (in hours).

247. The impact of the shocks prescribed under this scenario should be measured based on the operational and financial metrics described in section 7.3.

248. In contrast to the cloud outage scenario, it is considered that all business processes of the undertaking would be interrupted during the duration of the power outage. Moreover, the financial impact should materialize mostly in terms of business interruption, as recovery costs are expected to be limited in this scenario. As for the cloud outage scenario, companies will be asked to estimate the time to BAU assuming that recovery of the business processes might not take place coincidently with the recovery of the affected infrastructure.

7.5 DATA ELEMENTS

249. As a principle, the information collection in the context of a stress test exercise should be limited to the quantitative and qualitative data required to analyse the impact of the prescribed scenario and for validation purposes. Information can be collected both for the baseline and the adverse scenario, where applicable, and will be based on, but not limited to, the metrics presented in section 7.3.

250. As explained in section 7.3, the analysis of the impact of cyber resilience shocks relies on both operational and financial metrics. While financial metrics can be translated to the Solvency II framework, the same does not apply to the operational metrics.

251. To assess the operational impact of the shocks, the following quantitative and qualitative information could be collected:

- Time elapsed until return to business as usual (time to BAU);
- List of business processes affected by the cyber scenario;
- Availability of backups / alternative infrastructure;
- Cyber security practices / hygiene;
- Impact tolerances for specific business services.

252. For specific scenarios, such as the Cloud outage and Power outage scenarios, details on the largest exposures to cloud providers or location of critical IT infrastructures could be requested.

253. To assess the financial impact of the shocks, quantitative information on both the asset and liability sides of the Solvency II balance sheet (e.g. S.02.01) should be collected. Moreover, to assess the impact on the participating undertakings' profit and loss, information on operational and other costs could be collected, with the following breakdown:

- Business interruption costs;
- Detection and restoration costs.

254. Finally, a stock take of cyber resilience risk past events could also be considered in order to inform the scenario design and calibration of shocks going forward.

Questions:

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

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

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.

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

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.

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

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.

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

8 COMMUNICATION OF RESULTS

255. Disclosure of stress test results should follow the standard process defined in the general methodological principles of insurance stress testing.[78] Accordingly, the output of a stress test exercise with a focus on cyber risk should consist of a public report and a potential set of recommendations to NCAs where necessary. Recommendations, not public, can also target specific insurers based on their individual results.

256. In a standard financial stress test, the published report usually provides an overview of the exercise and discusses the results at country and/or EU aggregate level, whereas individual results, used in the dialogues between EIOPA and the NCAs, might be published upon consent of the participating undertakings.

257. Due to the intentional nature of cyber threats currently covered in this methodological paper, the results of a stress test with a focus on cyber risk are particularly sensitive to public disclosure as they inform on the potential vulnerabilities of the participating undertakings. Sensitivity could be higher with regards to the assessment of cyber resilience risk, as results would identify the potential weaknesses of the cyber defences and business processes of those undertakings. Against this background, the process for communicating and disclosing such results shall be considered with due care and might be adapted to ensure that identified vulnerabilities will not be explored by malicious actors.

[78] EIOPA (2020), Methodological principles of insurance stress testing. Available at: https://www.eiopa.europa.eu/document-library/methodology/methodological-principles-of-insurance-stress-testing_en?source=search.

9 ANNEXES

9.1 ANNEX: GLOSSARY OF CYBER RISK TERMS

Business interruption cost: income losses in the event that the business is halted due to a cyber risk event.

Cryptojacking: Abuse of a victim system's computing power to mine cryptocurrency and transfer it to the attacker.

Data Breach: Unauthorised disclosure of confidential data held by an organisation, often related to personal customer data.

Denial of Service (DoS): Maliciously flooding a target system with more data traffic than it can handle, in order to put it out of operation.

Disinformation campaigns: Orchestrated effort to spread false information, often using social media.

IaaS: Infrastructure as a Service, it is a cloud-based services for storage and networking based on a on-demand services model. In general, IaaS is used by network architects. Examples of IaaS : Amazon Web Service, Digital ocean, Google Compute Engine, Magneto, Cisco Metapod.

Malware: Generic term for malicious software designed to circumvent security protocols and posing a danger to information security.

Maximum Tolerable Period of Disruption: period following a cyber resilience risk events after which the participant's business sustainability will be vulnerable if the activity is not resume to business as usual.

PaaS: Plateform as Service, is a cloud platform solution for businesses composed of services managed by a third party. In general, PaaS is used by developers. Examples of PaaS : Windows Azure, AWS Elastic Beanstalk, Apache Stratos, OpenShift, Force.com, Heroku.

Ransomware: Malware that can cause the unauthorised encryption of data, allowing attackers to demand money in exchange for the decryption key.

SaaS: Software as Service, is a cloud application services that are made available online by a third party. In general, SaaS is used by end users. Examples of SaaS: Salesforce, Dropbox, BigCommerce, MailChimp, Hubspot, ZenDesk.

Supply-chain attack: attack that circumvents security protocols at a target organisation by compromising trusted business partners such as software suppliers.

Wiper: is a class of malware intended to erase (wipe, hence the name) the hard drive of the computer it infects, maliciously deleting data and programs.

Zero-day attack: attack that exploits a potentially serious software security weakness that the vendor or developer may be unaware of.

9.2 ANNEX: MITRE ATT&CK[79]

Using MITRE's corresponding online tools, it is possible to create a view on how many threat actors have been known to make use of each attack methodology. MITRE's data base contains 129 known group of malicious actors, with a short history of their activities and an estimation of their motivations. Based on this information, 20 threat groups were selected that fit the profile of acting for financial gain and are known to target the financial sector while not having a specific geographic focus outside Europe.

By scoring the attack techniques described in the framework according to their use amongst this group of 20 highly relevant threat actors, the following heat map presents itself (red representing techniques most commonly used, green less common usage and white no known usage within this circle of threat actors):

[79] MITRE ATT&CK®. Available at: https://attack.mitre.org/.

Threat actor groups selected in study of MITRE ATT&CK techniques: admin@338, Blue Mockingbird, Carbanak, DarkVishnya, Deep Panda, Evilnum, FIN10, FIN4, FIN6, GOLD SOUTHFIELD, Indrik Spider, menuPass, Poseidon Group, Rocke, Silence, TA505, TA551, TeamTNT, Turla, Wizard Spider.

9.3 ANNEX: CYBER INSURANCE COVERAGES[80]

Incident Type Group	**Coverage Scope**
Psychological support	Assistance and psychological support to the victim after a cyber-event leading to the circulation of prejudicial information on the policyholder without his/her consent.
Bodily injury and death	Compensation costs for bodily injury or consecutive death through the wrong-doing or negligence of the observed company or related third parties (e.g. sensible data leakage leading to suicide).
Breach of privacy compensation	Compensation costs after leakage of private and/or sensitive data, including credit-watch services, but excluding incident response costs.

[80] Based on CRO Forum (2016), Concept Paper on a proposed categorisation methodology for cyber risk (available at https://www.thecroforum.org/wp-content/uploads/2016/06/ZRH-16-09033-P1_CRO_Forum_Cyber-Risk_web-2.pdf) and OECD (2017), Supporting an effective cyber insurance market (available at: https://www.oecd.org/finance/supporting-an-effective-cyber-insurance-market.htm).

Business interruption (Interruption of operations)	Reimbursement of lost profits caused by a production interruption not originating from physical damage.
Communication and media	Compensation costs due to misuse of communication media at the observed company resulting in defamation, libel or slander of third parties including web-page defacement as well as Patent/Copyright infringement and Trade Secret Misappropriation.
Contingent business interruption (CBI) for non-physical damage	Reimbursement of the lost profits for the observed company caused by related third parties (supplier, partner, provider, customer) production interruption not originating from physical damage.
Cyber ransom and extortion	Costs of expert handling for a ransom and/or extortion incident combined with the amount of the ransom payment (e.g. access to data is locked until ransom is paid).
Data and software loss	Costs of reconstitution and/or replacement and/or restoration and/or reproduction of data and/or software which have been lost, corrupted, stolen, deleted or encrypted.
Directors' and officers' liability	Compensation costs in case of claims made by a third party against the observed company directors and officers, including breach of trust or breach of duty resulting from cyber event.
Environmental damage	Coverage scope: compensation costs after leakage of toxic and/or polluting products consecutive to a cyber-event.
Financial theft and/or fraud	Pure financial losses arising from cyber internal or external malicious activity designed to commit fraud, theft of money or theft of other financial assets (e.g. shares). It covers both pure financial losses suffered by the observed company or by related third parties as a result of proven wrong-doing by the observed company.
Fines and penalties	Compensation for fines and penalties imposed on the observed company. Insurance recoveries for these costs are provided only in jurisdictions where it is allowed.
Incident response costs	Compensation for crisis management/remediation actions requiring internal or external expert costs but excluding regulatory and legal defense costs. Coverage includes: (i) IT investigation and forensic analysis, excluding those directly related to regulatory and legal defenses costs; (ii) public relations and communications costs; (iii) remediation costs (e.g. costs to delete or cost to activate a "flooding: of the harmful contents published against an insured); (iv) notification costs.
Intellectual property theft	Loss of value of an Intellectual Property asset, resulting in pure financial loss.
Legal protection	Lawyer fees Costs of legal action brought by or against the policyholder including lawyer fees costs in case of trial. Example: identity theft, lawyer costs to prove the misuse of victim's identity.

Network security/Security failure	Compensation costs for damages caused to third parties (supplier, partner, provider, customer) through the policyholder/observed company's IT network but excluding incident response costs. The policyholder/observed company may not have any damage but has been used as a vector or channel to reach a third party.
Physical asset damage	Losses (including business interruption and contingent business interruption) related to the destruction of physical property of the observed company due to a cyber-event at this company.
Products liability	Compensation costs in case delivered products or operations by the observed company are defective or harmful resulting from a cyber-event, excluding technical products or operations (Tech E&O) and excluding Professional Services E&O.
Professional services E&O, Professional indemnity	Compensation costs related to the failure in providing adequate professional services or products resulting from a cyber-event, excluding technical services and products (Tech E&O).
Regulatory & legal defense costs (excluding fines and penalties)	A: Regulatory costs: compensation for costs incurred to the observed company is related third parties when responding to governmental or regulatory inquiries related to a cyber-attack (covers the legal, technical or IT forensic services directly related to regulatory inquiries but excludes Fines and Penalties). B: Legal defense costs: coverage for own defense costs incurred to the observed company or related third parties facing legal action in courts following a cyber-attack.
Reputational damage (excluding legal protection)	Compensation for loss of profits due to a reduction of trade/clients because they lost confidence in the impacted company.
Tech E&O	Compensation costs related to the failure in providing adequate technical service or technical products resulting from a cyber-event.

9.4 ANNEX: EXAMPLE OF DATA TEMPLATES FOR CYBER UNDERWRITING

9.4.1 EXAMPLE TEMPLATE FOR IMPACT OF CYBER SCENARIOS PER PRODUCT

Product (EN)	Guarantee	Gross claims Affirmative Cyber standalone coverages	Gross claims Affirmative Products with cyber as add-on coverage but main risk being covered	Gross claims Affirmative Products with cyber as add-on coverage and not as main risk being covered	Gross claims Non-affirmative	Gross claims Total	Ceded to reinsurer	Net claims
Cyber insurance	Crisis service costs							
	Cyber extortion							
	Recovery expense costs							
	Regulatory Fines							
	Data and Software Loss							
	Business Interruption							
	Contingent Business interruption							
	Other							
	Total							
Fire and other damage to property insurance	Physical Damage							
	Business Interruption							
	Contingent Business interruption							
	Total							
Directors' and Officers' Liability	Total							
Professional Indemnity	Total							
Public and Products Liability	Total							
Credit and suretyship	Total							
Other	Total							
Total								

9.4.2 EXAMPLE TEMPLATE FOR IMPACT OF CYBER SCENARIOS PER ECONOMIC SECTOR

Economic sector	Number of Policies	Exposure (Sum Insured)	Gross Written Premium	Number of Claims	Gross Claims
A - AGRICULTURE, FORESTRY AND FISHING					
B - MINING AND QUARRYING					
C - MANUFACTURING					
D - ELECTRICITY, GAS, STEAM AND AIR CONDITIONING SUPPLY					
E - WATER SUPPLY; SEWERAGE, WASTE MANAGEMENT AND REMEDIATION ACTIVITIES					
F - CONSTRUCTION					
G - WHOLESALE AND RETAIL TRADE; REPAIR OF MOTOR VEHICLES AND MOTORCYCLES					
H - TRANSPORTATION AND STORAGE					
I - ACCOMMODATION AND FOOD SERVICE ACTIVITIES					
J - INFORMATION AND COMMUNICATION					
K - FINANCIAL AND INSURANCE ACTIVITIES					
L - REAL ESTATE ACTIVITIES					
M - PROFESSIONAL, SCIENTIFIC AND TECHNICAL ACTIVITIES					
N - ADMINISTRATIVE AND SUPPORT SERVICE ACTIVITIES					
O - PUBLIC ADMINISTRATION AND DEFENCE; COMPULSORY SOCIAL SECURITY					
P - EDUCATION					
Q - HUMAN HEALTH AND SOCIAL WORK ACTIVITIES					
R - ARTS, ENTERTAINMENT AND RECREATION					
S - OTHER SERVICE ACTIVITIES					
T - ACTIVITIES OF HOUSEHOLDS AS EMPLOYERS					
U - ACTIVITIES OF EXTRATERRITORIAL ORGANISATIONS AND BODIES					
OTHER					
All sectors					

9.4.3 EXAMPLE TEMPLATE FOR ACCUMULATION EXPOSURE CYBER INSURANCE PER IT SERVICE PROVIDER

IT Service Provider	Name of IT service provider	Number of Policies	Exposure (Sum Insured)
IT service provider 1			
IT service provider 2			
IT service provider 3			
IT service provider 4			
IT service provider 5			
IT service provider 6			
IT service provider 7			
IT service provider 8			
IT service provider 9			
IT service provider 10			
Total (across all IT service providers)			

EIOPA

Westhafen Tower, Westhafenplatz 1
60327 Frankfurt – Germany
Tel. + 49 69-951119-20
info@eiopa.europa.eu
https://www.eiopa.europa.eu