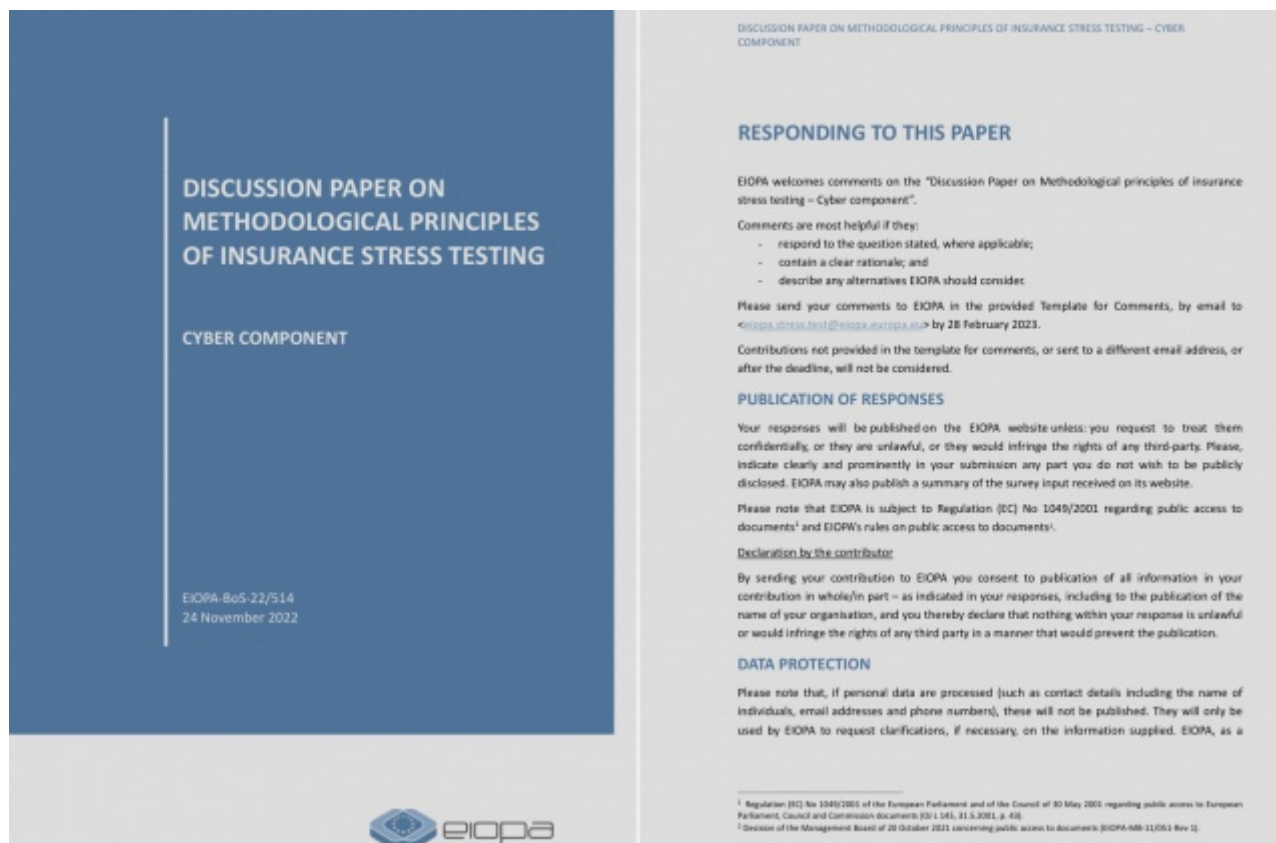


EIOPA e il Cyber Risk: quali rischi e quali stress test



di Spataro

Attenzione ai rischi assicurati e alle condizioni. Un tema già affrontato su [Assicurativo.it](https://www.assicurativo.it) Vediamo cosa dice EIOPA. Il paper è di 91 pagine

del 2023-06-19 su [Assicurativo.it](https://www.assicurativo.it), oggi è il 15.05.2024

The European Insurance and Occupational Pensions Authority (EIOPA) published today a [Discussion Paper on Methodological Principles of Insurance Stress Testing with focus on Cyber Risk](#).

This discussion paper contains a set of theoretical and practical approaches to support the design phase of potential future insurance stress tests with a focus on cyber risk. This should further enrich the bottom-up stress test toolbox with additional elements to be potentially applied in future exercises.

EIOPA aims at laying the groundwork for an assessment of insurers' financial resilience under severe but plausible cyber incident scenarios. The paper elaborates on two main aspects:

- cyber resilience, understood as the capability of an insurance undertaking to sustain the financial impact of an adverse cyber event;
- cyber underwriting risk, understood as the capability of an insurance undertaking to sustain "from a capital and solvency perspective" the financial impact of an extreme but plausible adverse cyber scenario affecting underwritten business.

EIOPA invites stakeholders to share their feedback using the provided template **no later than 28 February 2023**. Contributions should be sent to the following email address: eiopa.stress.test@eiopa.europa.eu.

The feedback received will be considered in the preparation of a final methodological paper to be published on EIOPA's website.

[Go to the discussion paper](#)

Background

This discussion paper is part of a broader effort to enhance EIOPA's stress testing framework. In 2019, EIOPA initiated the enhancement of its methodology for bottom-up stress testing with its first paper on [Methodological Principles of Insurance Stress Testing](#). This was followed by work on specific stress testing related topics such as the assessment of liquidity positions under adverse scenarios and of vulnerabilities towards climate-related risks, leading to the publication of the second paper on [Methodological Principles of Insurance Stress Testing with a focus on Liquidity](#) and the third paper on [Methodological Principles of Insurance Stress Testing with a focus on Climate Risks](#).

Ecco l'indice del testo disponibile qui 31 JANUARY 2023 Discussion paper on methodological principles in insurance stress testing - Cyber component.pdf English(1.3 MB - PDF) [Download](#)

Ci scusiamo per l'impaginazione

CONTENTS

1 Introduction

2 Cyber risk for insurers

2.1 Cyber risk: main concepts

2.2 Cyber resilience: insurers as direct targets of cyber attacks

2.2.1 Motivation of cyber attacks against insurers

2.2.2 Perpetrators of cyber attacks against insurers

2.2.3 Types of cyber attacks against insurers

2.2.4 Impact of cyber attacks against insurers

2.3 Cyber underwriting: insurers exposed through underwritten products

2.3.1 Cyber insurance market

2.3.2 Affirmative cyber

2.3.3 Silent cyber

2.3.4 Accumulation risk

3 Key assumptions

4 Scope

4.1 Criteria

5 Scenarios

5.1 Scenario selection

5.2 Scenario narratives and specifications

5.2.1 Data Center/Infrastructure Damage (cloud outage)

5.2.2 Ransomware / Data Theft

5.2.3 Denial of Service (DoS)

5.2.4 Data Breach

5.2.5 Power outage

5.3 Scenarios not retained for the purpose of this paper

6 Cyber underwriting: shocks, specifications and metrics

6.1 General guidance

6.2 Shocks

6.3 Metrics

6.4 Examples of applications

6.4.1 Ransomware

6.4.2 Cloud outage	
6.4.3 Power Outage	
6.5 Silent cyber: additional guidance	
6.6 Data elements	

7 Cyber resilience: shocks, specifications and metrics	
7.1 General guidance	
7.2 Shocks	
7.3 Metrics	
7.4 Examples of applications	
7.4.1 Cloud outage	
7.4.2 Ransomware	
7.4.3 Denial of Service (DoS)	
7.4.4 Data breach	
7.4.5 Power outage	
7.5 Data elements	

8 Communication of results

9 Annexes

9.1 ANNEX: Glossary of cyber risk terms	
9.2 ANNEX: MITRE ATT&CK	
9.3 ANNEX: Cyber insurance coverages	
9.4 ANNEX: Example of data templates for cyber underwriting	
9.4.1 Example template for impact of cyber scenarios per product	
9.4.2 Example template for impact of cyber scenarios per economic sector	
9.4.3 Example template for accumulation exposure cyber insurance per IT service provider	

Table 1 – Impact of various cyber resilience scenarios	21
Table 2 - Advantages and disadvantages of targeting solo or group undertakings for the purposes of stress testing cyber risk	32
Table 3 - Reference metrics for inclusion of undertakings in the scope of a stress test with focus on cyber risk	34
Table 4 – Categories of cyber incidents and associated risk factors	37
Table 5 – Cloud outage scenario	40
Table 6 – Ransomware / Data Theft scenario	41
Table 7 – Denial of Service (DoS) scenario.....	42
Table 8 – Data Breach scenario	44
Table 9 – Power outage scenario	45
Table 10 – Cyber underwriting scenarios and their shocks	50
Table 11 – Cyber underwriting metrics.....	53
Table 12 – Ancillary indicators	54
Table 13 – Ransomware shocks	57
Table 14 – Cloud outage shocks	58
Table 15 – Power outage shocks	59
Table 16 – Cyber resilience scenarios and their shocks	64
Table 17 – Cyber resilience metrics	65
Table 18 – Cloud outage shocks	67
Table 19 – Ransomware shocks	69
Table 20 – DoS shocks	70
Table 21 – Data breach shocks.....	71
Table 22 – Power outage shocks	72

Hai letto: EIOPA e il Cyber Risk: quali rischi e quali stress test

Approfondimenti: [Cyberrisk](#) > [Fintech](#) > [Assicurativo](#) > [Privacy](#) > [Rischi](#) > [Civile.it](#) >

[Commenti](#) - [Segnalazioni](#) - [Home Assicurativo.it](#)