Session 1: G7 CEG Fundamental Elements on Third-Party Cyber Risk Management

Tokyo, May 9th 2023

Who we are.

Tim Paulowitz (Deutsche Bundesbank)

- Co-Chair of G7 CEG Work Stream
- Senior Payments Expert

Matthias Rest (Deutsche Bundesbank)

- Co-Chair of G7 CEG Work Stream
- Senior Supervisor

Report from

G7 Cyber Expert Group Subgroup on Financial Sector Third-Party and Supply Chain Risk Assessment Strategy and review of the Fundamental Elements on Third-Party Cyber Risk Management

Introduction

Use of third parties in the financial sector is still increasing:

- The scale, complexity and interconnectedness of supply chains continue to grow.
- Maintaining an overview of third-party dependencies and associated cyber risks becomes increasingly challenging, for both individual entities and the financial system as a whole.

The G7 Cyber Expert Group (CEG) emphasized the growing importance of third-party cyber risk management in 2018 by publishing corresponding Fundamental Elements.

Update of G7 Fundamental Elements

2018: Release of the G7Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector

2022: **Why Update of the G7 Fundamental Elements?**

Update of G7 Fundamental Elements

Key adjustments to Fundamental Elements address:

- growing importance of third-party providers to the financial sector
- growing importance of supply chain (e.g. software bill of materials)
- emphasis on ICT providers for the cyber risk of entities
- importance of exit strategies for entities
- growing importance of transparency and information sharing

G7 FUNDAMENTAL ELEMENTS FOR THIRD PARTY CYBER RISK MANAGEMENT IN THE FINANCIAL SECTOR

Released October 2022

G-7 Fundamental Elements of Ransomware and Third Party Risk : 日本銀行 Bank of Japan (boj.or.jp)

Objective of the Fundamental Elements

The Fundamental Elements …

- …aim to further support the development of third party cyber risk management in the financial sector.
- …aim to help entities to tailor their specific risk profiles, operational and threat landscape, role in the sector, and legal and regulatory frameworks.
- …are non-binding and do not invalidate existing frameworks or prevent their continuous adaptation.
- …can be part of entities' cyber risk management toolkit.
- …can be used by authorities within and across jurisdictions to inform their public policy, regulatory and supervisory efforts to address third party cyber risks.

Element 1

Governance

Entities' governing bodies are responsible and accountable for effective oversight and implementation of third-party cyber risk management.

Element 2

Risk Management Process for Third-Party Cyber Risk

Entities have an effective process for managing third-party cyber risks through the entire third party risk management life cycle.

- Identification of Third Parties and Criticality
- Cyber Risk Assessment and Due Diligence
- Contract Structuring
- Ongoing Monitoring

Element 3

Incident Response

Entities establish and exercise incident response plans that include critical third parties.

Element 4

Contingency Planning and Exit Strategies

Entities have appropriate contingency plans and exit strategies in place to address situations where third parties fail to meet cyber-related performance expectations or pose cyber risks outside the entity's risk appetite.

Element 5

Monitoring for Potential Systemic Risks

Third-party relationships across the financial sector are monitored and sources of third-party cyber risk with potential systemic implications are assessed.

Element 6

Cross-sector Coordination

Cyber risks associated with third-party dependencies across sectors are identified and managed across those sectors.

Element 7

New Element

Third Parties to the Financial Sector

Third parties that enter into contractual relationships with an entity should be aware that risk management requirements of these entities might have implications for their provision of services and goods.

Key Takeaways from the Work Stream

- G7 jurisdictions already have a lot of best practices and tools in place to address third party risk management in the financial sector.
- Approaches regarding the **tools** in G7 jurisdictions are quite similar.
- **Best practices** are also mostly aligned.
- Still need for further improvement and cooperation.

What can be done to further improve?

Recommendations from the Work Stream Chairs

- Enhance cooperation, coordination and collaboration globally between entities, relevant authorities and jurisdictions.
- Coordination at G7-level would ease the development of cross-jurisdictional recognition of assurance schemes.
- Support the ongoing work of the Financial Stability Board (e.g. FSB Cyber Lexicon).

Thank you very much for your attention!