Financial Industry-Wide Cybersecurity Exercise (Delta Wall Ⅶ)

Landscape of Cyber Risk Faced by the Financial Sector

- Large-scale cyberattacks happened across the world. The techniques employed in these attacks became increasingly sophisticated and complicated.
- In Japan, there were cyber incidents where operations of companies and entities were disrupted, confidential information leaked, and financial losses were caused.
- The threat of these cyberattacks poses significant risks with the possibility of undermining the stability of the financial system as a whole. It is crucial to improve the overall ability of financial institutions to respond to incidents.

Overview of Previous Exercises

✓ Delta Wall (DW) has annually been conducted since 2016. The number of participants were:
- Approx. 900 individuals from 77 financial institutions (FIs) at DW I in 2016
- Approx. 1,400 individuals from 101 FIs at DW II in 2017,
- Approx. 1,400 individuals from 105 FIs at DW III in 2018,
- Approx. 2,000 individuals from 121 FIs at DW IV in 2019,
- Approx. 1,700 individuals from 114 FIs at DW V in 2020, and
- Approx. 2,700 individuals from 150 FIs at DW VI in 2021.

✓ Feedback from the participants indicates that DW contributed to improving FIs' capabilities to respond to incidents. For example, many of the participating FIs indicated that they reviewed their policies and procedures, or would do so, and that they strengthened information sharing (incl. internal and external information sharing) or would do so.

Delta Wall VII (2022)

- In October 2022, **Financial Services Agency (FSA) conducted Delta Wall* VII.**
  * Delta Wall stands for the triad (delta) of "self-help," "mutual assistance," and "public assistance," which are key elements of cybersecurity.
- To improve the participation rate, the number of participating securities companies and funds transfer service providers was increased. **As a result, 160 financial institutions and firms participated.**
- As in the previous fiscal year, **FIs are free to choose to participate under their actual teleworking environments** to improve their response capabilities under such circumstances.
- Participants are required to submit a self-analysis report regarding items to which they could not properly respond. It is intended to enhance the outcomes of the exercise **by clarifying lessons learned through the analysis**.

Features of the Exercise

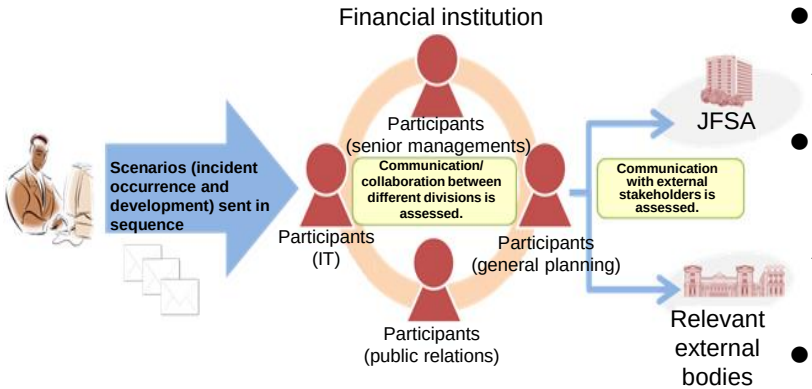
✓ One of the aims is to check how financial institutions **investigated the attack, how they responded, including technical responses, responses from the perspective of customer relations, efforts to continue services and responses for restoration.**

✓ **The participants join the Delta Wall VII from their workplace**, which encourages participation not only from IT division, but also from other relevant divisions, such as public relations, various business lines, and senior management.

✓ The DW **emphasizes ex-post evaluation of actions taken and decisions made by participants during the exercise.** FSA's feedback aims to provide recommended actions and share best practices observed in the exercise.

✓ **The lessons learned will be shared with the entire industry**, not just with the participants.

Illustration of the Exercise



Examples of the scenarios:

- **Banks**
  ✓ The exercise was conducted by a blind method.
- **Shinkin Banks, Credit Associations and Labor Banks**
  ✓ Customer information was leaked. Malfunctions of FI's websites occurred.
- **Securities Companies, FX Service Providers, Funds Transfer Service Providers, and Issuers of Prepaid Payment Instruments**
  ✓ Halt of operation systems was triggered by malfunctions in network equipment.
- **Crypto-asset Exchange Service Providers**
  ✓ Outflow of crypto-assets was triggered by information leakage.