Financial Industry-Wide Cybersecurity Exercise (Delta Wall VIII)

Landscape of Cyber Risk Faced by the Financial Sector

- Large-scale cyberattacks are increasingly observed across the world. Techniques used by attackers become further sophisticated and complicated.
- Similarly, in Japan, cyberattacks increasingly cause disruption of business operations, compromise of confidential information and financial losses.
- Threats of cyberattacks potentially pose significant risks that could undermine financial stability.

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,
- Approx. 2,700 individuals from 150 FIs at DW VI in 2021, and
- Approx. 3,500 individuals from 160 FIs at DW VII in 2022.

✓ Feedback from the participants indicates that DW has 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 VIII (2023)

- In October 2023, **Financial Services Agency (JFSA) conducted Delta Wall* VIII.**
  * The name "Delta Wall" represents the triad (delta) of "self-help," "mutual assistance," and "public assistance," which are key elements of cybersecurity
- The coverage was expanded from the previous fiscal year to include insurance companies. From the perspective of increasing the participation rate of critical infrastructure operators, **165 FIs participated** (an increase of 5 FIs from the previous fiscal year).
- For banks, by using severer scenarios that would exert an influence on their important business operations, in consideration of the maturity assessment of past exercises, the content and sufficiency of their discussions with the involvement of top management, such as priorities in business operations in the event of an incident, are to be verified. For other scenarios as well, the content of the exercise will be enhanced by raising levels of difficulty, such as including halts in infrastructure systems.
- As in the previous fiscal year, **FIs are free to choose to participate in their workplaces or under their actual teleworking environments** to improve their response capabilities, including those under teleworking environments.

Features of the Exercise

✓ One of the aims is to check financial institutions' **initial responses upon an incident, how they investigate and analyze the attack, including technical responses, how they contain and eliminate the impact of the attack, and how they respond to customers and business continuity, including the recovery of services**.

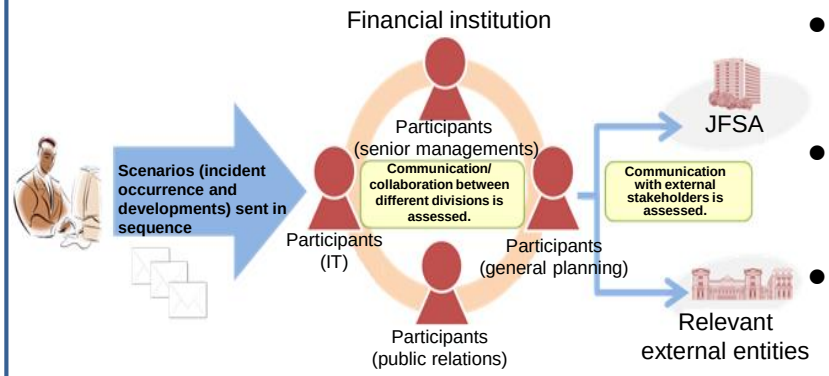
✓ **The participants join the Delta Wall VII from their workplace**, which encourages participation not only from IT divisions, but also from other relevant divisions, such as public relations, various business lines, and senior management.

✓ 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.

✓ The DW **emphasizes ex-post evaluation** by presenting concrete remedial measures and best practices so that participating FIs can improve their response capabilities while following the plan-do-check-act (PDCA) cycle.

✓ **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 and Credit Associations**
  - ✓ Halts in operation systems and terminals occurred (including halts in their common infrastructure systems).
- **Securities Companies**
  - ✓ Halts in operation systems, etc. occurred (including halts in part of the securities infrastructure systems).
- **Life Insurance Companies, Non-Life Insurance Companies, Funds Transfer Service Providers, Issuers of Prepaid Payment Instruments, and Crypto-asset Exchange Service Providers**
  - ✓ Halts in operation systems were triggered by the vulnerability of network equipment.