Financial Industry-Wide Cybersecurity Exercise (Delta Wall VI)

Situation Surrounding Cybersecurity in the Financial Industry

- Large-scale cyberattacks have occurred in various countries worldwide, and the employed techniques are becoming further sophisticated and complicated.
- Also in Japan, there have been cyberattacks due to which business operations were hindered, critical information was stolen, and financial damage was 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 were annually conducted since 2016. Participants were as follows :

- Delta Wall I in 2016, about 900 individuals at 77 financial institutions (hereinafter FIs)
- Delta Wall II in 2017, about 1,400 individuals at 101 FIs
- Delta Wall III in 2018, about 1,400 individuals at 105 FIs
- Delta Wall IV in 2019, about 2,000 individuals at 121 FIs
- Delta Wall Ⅴ in 2020, about 1,700 individuals at 114 FIs

✓ Many of the participating FIs have reviewed or plan to review their existing rules, and have strengthened or plan to strengthen information sharing procedures internally and externally. Delta Wall has thus encouraged FIs to improve their incident response capability.

Financial Industry-Wide Cybersecurity Exercise (Delta Wall VI)

- In October 2021, **Financial Services Agency（hereinafter JFSA）conducted the sixth Industry-Wide Cybersecurity Exercise (Delta Wall* VI).**

(*) Delta Wall means a key element in cybersecurity: the triad (Delta) of "self-help," "mutual assistance," and "public assistance."

- **150 FIs and other organizations participated.** The number of small-and medium-sized financial institutions increased particularly from Shinkin banks and credit associations in addition to funds transfer businesses providers where cyber incidents happened to dome of these providers.
- Participants are requested to submit the results of their self-analyses concerning items that they failed to achieve (whether it was a problem regarding a contingency plan (Plan) or a problem in taking measures (Do), etc.) to **clarify factors for their evaluation results**, thereby enhancing the effect of the exercise.
- As in the previous fiscal year, **some FIs participated under their actual teleworking environments** to improve their response capabilities under such circumstances.

Features of the Exercise

✓ One of the aspects is to check financial institutions' **initial responses** upon a cyber incident, **investigations of the details of the attack and other technical responses, information sharing and continuation of services**, etc.

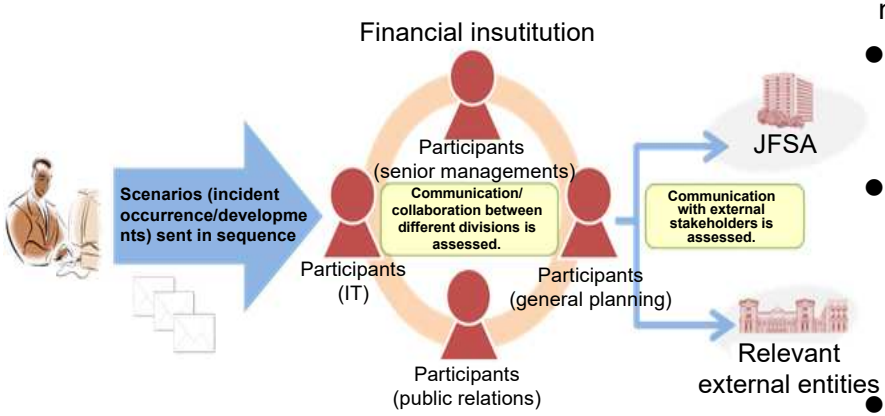
✓ For banks, the exercise verified **the details of their discussions and decision making processes** when responding to an incident.

✓ **The participants joined the Delta Wall Ⅵ from their workplace** to facilitate participation of colleagues from relevant divisions, including IT, public relations and general planning, as well as senior managements.

✓ The exercise **emphasized on assessing the participants' actions and decision making during the exercise,** recommending concrete improvement measures and sharing best practices after the exercise.

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

Exercise Scheme



[Scenario Example]

- **For banks**

(The exercise was conducted by a blind method.)

- **For Shinkin banks and credit associations**
  - ✓ Abnormality in a critical system that causes an impact on customers
- **For securities companies, FX service providers, funds transfer service providers, and crypto-asset exchange service providers**
  - ✓ Unauthorized access to a transaction system that causes leakage of customer assets
- **For insurance companies, insurance representatives, and audit firms**
  - ✓ Customer information leakage