Financial Industry-wide Cybersecurity Exercise (Delta Wall V)

Situation Surrounding Cybersecurity in the Financial Industry

- Fraudulent payments have occurred at multiple banks connecting cashless payment services provided by funds transfer service providers.
- Additionally, there have been cyberattacks taking advantage of the COVID-19 pandemic and targeting teleworking environments.
- As the threat of these cyberattacks might pose significant risks undermining the financial stability, it is crucial to improve incident response capability in the financial industry.

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
- ✓ 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.

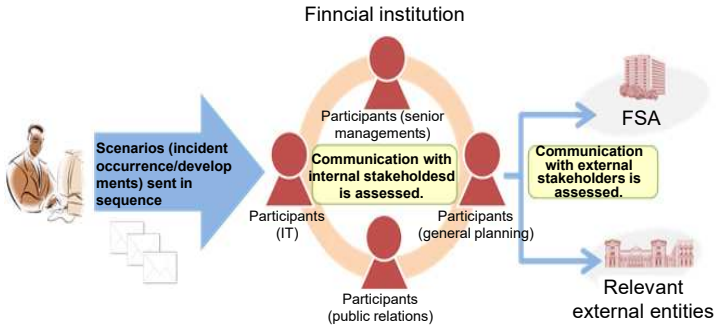
Financial Industry-wide Cybersecurity Exercise (Delta Wall V)

- In mid-October 2020, **JFSA conducted the fifth Industry-wide Cybersecurity Exercise (Delta Wall V*) and about 110 FIs participated.** Delta Wall V aims to improve incident response capability in the financial industry by assessing the **effectiveness of communication with internal and external stakeholders, including customers, upon cyber incident**, since the significance of such communication was more pronounced in the recent cyber heists. (*) Delta Wall means a key element in cybersecurity: the triad (Delta) of "self-help," "mutual assistance," and "public assistance."
- Based on the lessons of the last exercise, the exercise for banks focused on **the escalation process and the top management's decision making** through internal discussions, in order to **improve incident response capability**.
- **Some FIs participated under their actual teleworking environments** to improve their response capabilities under such circumstances.

Features of This Exercise

- ✓ This is an exercise to improve incident response capability by assessing the effectiveness of information sharing with internal and external stakeholders upon cyber incident.
- ✓ **The participants joined the Delta Wall V from their workplace** to facilitate participation of colleagues from relevant divisions, including IT, public relations and general planning, as well as senior managements.
- ✓ When designing a scenario, **using risk assessments and input from threat intelligence analysis** allow participants to recognize their potential weaknesses / vulnerability as well as to raise their awareness.
- ✓ 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

- ✓ A corporate website defacement causing influence on customers
- ✓ Malware infection of corporate PC and proliferation

For securities companies, FX service providers, insurance companies, funds transfer service providers and audit firms

- ✓ Customer information leakage
- ✓ Infection of intranet with malware that had exploited

Crypto-asset exchange service providers

- ✓Leakage of customer assets
- ✓Hacking of intranet and establishing unauthorized communications with external malicious server.