Cyber Risks as a Challenge for Corporations and Their Executives in Japan

March 23, 2023＠Frankfurt aM

Gen Goto (University of Tokyo)

Cyber security incidents and damages caused

- Personal data breaches
  - E.g. Benesse (2014), Morinaga (2022)
- Unauthorized access to FinTech services
  - E.g. Coincheck (2018), Seven Pay (2019)
- Distributed denial of service (DDoS) attacks
- Targeted ransomware attacks
  - Rapid increase since 2020
  - E.g. Handa Hospital (2021), Toyota's supplier (2022)
- Damages
  - Compensation to customers (ca. ¥1000~5000/person in case of personal data breach)
    - US-style class action unavailable
  - Disclosure of business secrets
  - Loss of reputation
  - Interruption of business activities (may extend to trade partners)
  - Payment of ransom

Responding to cyber security risks

- Ex ante
  - Install a system to prevent/detect cyber security incidents
  - Business continuity planning re cyber security incidents
  - Cyber security insurance

- Ex post
  - Digital forensics to identify the source
  - Restoration of systems (if possible)
  - Decide whether to pay ransom or not
  - Notification to affected trade partners and individuals
  - Decide whether to disclose publicly about the incident or not

Duties and liabilities of directors and executive officers in Japan

- Liability of directors and executive officers toward the corporation for damages caused by a breach of his/her duties (Art.423 JCA)
  - Fault-based liability, but burden of proof for a breach on plaintiffs
  - Derivative suit: no standing requirement, no dismissal by special litigation committee, no discovery

- Duty of care (Art.330 JCA, Art.644 Civil Code)
  - Duty of oversight
    - As a board member and as an executive officer
  - Duty to establish an internal control system to manage various kinds of risks, as a part of duty of care
    - Osaka District Court, Sept 20, 2000 (Daiwa Bank)
    - JCA requires internal control system to be decided by the board of directors

Ex ante: internal control system

- System for preventing/detecting cyber security incidents and BCP constitute a part of internal control system
  - “Internal control system to manage risks of losses for the company and its subsidiaries” (Art.100, para.2, (ii)(v)(b), Ministerial Ordinance for Enforcement of JCA)
  - Cybersecurity at trade partners in the supply chain also relevant (e.g. Toyota)
- Possible liability of directors/executive officers for failing to implement an effective internal control system
- It is generally accepted that business judgement rule (Japanese version) is applicable for decisions re the content of internal control system
  - However, how BJR is applied is not so clear

How is the adequacy of internal control system judged?

- Supreme Court, July 9, 2009 (Japan System Technology)
  - Whether the company's internal control system can prevent wrongful acts that can be normally expected
  - For wrongful acts committed in a way that cannot be normally expected, whether there were special circumstances that would enable prediction of such acts
  - Inflation of sales by employees, the method used could not be expected, no red flag

- Obtaining information on possible wrongful acts
  - Other companies in the industry, guidelines by government agencies, reports by other companies that experienced scandals, whistle blowing, etc.

Internal control system re cybersecurity risks

- Basic framework by the Supreme Court decision would apply

- Characteristics of cybersecurity risks
  - Malicious attack from outside
  - Rapid evolution of attack methods

- Some modification might be necessary
  - Periodical and ad hoc updates to adjust to new types of attacks
  - Importance of BCP

Hiroshima High Court, Okayama Branch Oct 18 2019 (In re Benesse)

- In 2014, an employee of an independent contractor sold private info of Benesse's customers to third party
- No problem re internal control system had been reported to Benesse's board
- The system was not updated to prevent transmission of information to the new model of smartphone used
- The content of internal control system shall be decided by directors exercising its discretion
- Liability of directors was denied as plaintiffs failed to prove that the internal control system and its implementation did not meet the standard required for listed companies at that time

- Cf. Tokyo High Court, March 25, 2020 held Benesse liable to the customers affected, noting that Benesse should have recognized the risk of breach using the new model and should have ordered the IC to update the security software

Ex post: payment of ransom

- Does paying ransom to attackers violate laws or regulations?
  - US Foreign Assets Control Regulation: prohibition of ransom payment to those on SDN list, exemptions might be available by reporting to relevant authorities
  - No law or regulation in Japan prohibits payment
    - However, METI advices companies to refrain from paying as it would encourage attackers while restoration of encrypted data is not guaranteed at all
- Does paying ransom constitute a breach of director's duty of care?
  - Business judgment rule applicable
    - METI has no regulatory power and its advice is not binding
    - Cf. Tokyo District Court's decision on TEPCO Fukushima 1st incident derivative suit
  - Decision to pay after assessing factors such as effect of not paying, effect of paying, and availability of other restoration measures would be protected

Disclosure

- Cf. US: SEC proposed rule on cybersecurity risk management (Fed. Reg. 87(2022) 16590)
  - Disclosure of material cybersecurity incidents within 4 business days
  - Periodic disclosures of cybersecurity risk management policy and procedures, management's role and BOD's oversight, and BOD's cybersecurity expertise
- Disclosure of cybersecurity incidents
  - No specific disclosure requirement on cybersecurity incidents
  - Timely disclosure by TSE listing rules applicable if the amount of damage by the incident would exceed 3% of net asset or 30% of ordinary profit
  - Since 2022, notification of personal info breach to those affected and reporting to the authority are mandatory under Personal Information Protection Act
- Disclosure of internal control system
  - Disclosure of the outline of BOD's decision on internal control system and how it is implemented in the annual report under JCA (Art.118(ii) Ministerial Ordinance for Enforcement of JCA)
    - Audited by statutory auditors or audit committee (Art.129(1)(v) Ministerial Ordinance)
  - Not covered by special civil liability rules for misrepresentation of disclosure documents under Financial Instruments and Exchange Act