Cyber Risks as a Challenge for Corporations and Their Executives: A Case of Korea

March 23, 2023

Seoul National University, School of Law

Kyung-Hoon Chun

Assigned Topic

"Cyber Risks as a Challenge for Corporations and Their Executives (Duties, Liability)"

- Key Words
  - Cyber Risks
  - Corporations and Executives
  - Challenge : Duties, Liability
  - (Each jurisdiction: Korea)

Research Questions

- What are cyber risks and why are they important to companies?
- What are the duties and liability of the directors and executives in relation to the cyber risks?
  - as a general legal theory
  - as a matter of Korean law
- What should the corporate law do to cope with the ever-increasing cyber risks?
  - rule-based approach (e.g., statutory security standards)?
  - standard-based approach (e.g., directors' oversight duty)?

Cyber risk refers to the potential harm or damage that can arise from the use of digital technology, including computers, networks, software, and the internet. Cyber risk can take many forms, including data breaches, cyber attacks, hacking, phishing, ransomware, and other types of cybercrime.

The consequences of cyber risk can be significant, ranging from financial loss and damage to reputation to legal liability and regulatory penalties. Cyber risk can also pose a threat to national security and public safety, as critical infrastructure such as power grids and transportation systems are increasingly connected to digital networks.

To manage cyber risk, individuals and organizations need to take proactive measures to protect themselves and their systems from cyber attacks. This includes implementing strong security measures such as firewalls, encryption, and multi-factor authentication, as well as training employees to be vigilant and aware of potential cyber threats. Regular security assessments and risk analyses can also help identify vulnerabilities and develop strategies to mitigate them.

By chatGPT

Cyber Risk and Its Significance

Definitions

- Cyber Risks
  - the exposure to the possibility of *loss* from a cyberattack or incident (Evans, 2019)
  - the potential *harm or damage* that can arise from the use of digital technology, including computers, networks, software, and the internet (chatGPT, 2023)
- Cybersecurity
  - measures taken to protect the IT system against cyberattacks
- Cyber Vulnerability
  - Weakness in an IT system that could be exploited or triggered by cyber attackers

Cyber Risk: Loss or Harm

- Direct financial loss: theft of funds, payment fraud, ransomware demands
- Data loss: theft, destruction, or alteration of sensitive data, including personal information
- Operational disruption: denial of service (DOS), system failures, or loss of productivity
- Reputational damage: which may lead to loss of trust, customers, and market share
- Physical harm: cyber attacks on critical infrastructure, such as energy grids and transportation systems
- National security threats

Growing Importance of Cyber Risks

- Growing reliance on technology and the internet, both by the company and by its consumers/customers
- Growing cyber security vulnerability due to increasingly complicated software/networks
- Consequences are severe: business interruption, data theft, shock to stock price, regulatory fines, reputation damages
- Accelerated by COVID-19: remote work and online activities increase vulnerability

Growing Cyber Vulnerability

- Heavier the program (more codes) ⇨ more errors and more difficult to fix problems
- More connected, more frequent access ⇨ more difficult to fend off attacks and fix problems
- Hacking is lucrative ⇨ R&D in hacking + harder to hire experts on defensive side

Vulnerability is Hard to Find

- No single security expert can find all the vulnerabilities
- Vulnerabilities can be found by way of various sham attacks
- Insiders/white hackers must find the vulnerabilities ahead of the black hackers.

⇨ This feature created **Cybersecurity Vulnerability Market**

= marketplace where information on s/w vulnerabilities that are not publicly known or have not yet been patched are traded

= white market (bug bounty), grey market, black market

When Vulnerability is Found….

- If white hackers find it, they will disclose it:
  - Full disclosure
  - Responsible disclosure
  - Coordinated disclosure (Need a coordinator as a medium)
- If black hackers find it, they will use it:
  - Threat and demand ransom
  - Retain and develop attack methods
  - Sell to others
- Not fundamentally distinguishable! (fair compensation for coordinated disclosure vs. ransom)

Thus,

- Cyber vulnerabilities can't be zero.
- Cyber risk can't be zero.
- Need to take a risk management approach.
  - Rather than legal v. illegal dichotomy
  - Identify, assess, and manage different types of risks: ROLF
    - Reputational, operational, legal, financial
  - Not only substantive, but also procedural approach
    - Systems for detecting, reporting, and fixing the problem

Duties and Liability of Directors and Executives

Cyber Risk: Loss or Harm

- Direct financial loss: theft of funds, payment fraud, ransomware demands
- Data loss: theft, destruction, or alteration of sensitive data, including personal information
- Operational disruption: denial of service (DOS), system failures, or loss of productivity
- Reputational damage: which may lead to loss of trust, customers, and market share
- Physical harm: cyber attacks on critical infrastructure, such as energy grids and transportation systems
- National security threats

Cyber Risk: Loss or Harm

- All of these losses can be financial loss
  - Decrease in revenue (e.g., business interruption)
  - Decrease in stock price (e.g., damage in reputation)
  - Liability to third parties (e.g., data theft)
  - Criminal and regulatory fines (e.g., noncompliance of data security measures)

Cyber Risk Related Claims

- Such losses can be translated into claims
  - Decrease in revenue / Criminal and regulatory fines
    - Company's loss ⇨ Company's claim against wrongdoers
    - S/Hs may enforce the claims via derivative action, if the wrongdoers are directors/executives
  - Decrease in stock price
    - S/H's loss ⇨ S/H's claim against wrongdoers
  - Company's liability to third parties (e.g., data leakage due to system error)
    - Third party's loss ⇨ Third party's claim against the company and other wrongdoers
    - If the company pays the claim, then the company incurs loss ⇨ Company's claim against wrongdoers
    - S/Hs may enforce the company's claim via derivative action, if the wrongdoers are directors/executives

Cyber Risk Related Claims

- So, we have a few potential claims….
  - Company's claim against wrongdoers [1]
  - S/H's claim against wrongdoers (directly [2] and derivatively [3])
  - Third party's claim against the company [4] and other wrongdoers [5]

- If directors/executives are wrongdoers,
  - They are liable to the company [1][3][4]
  - They are liable to the shareholders [2]
  - They are liable to the third party victims [5]

When Does a Director/Executive Become a Wrongdoer?

- 1. Breach of Oversight Duty
  - US: Caremark claims - failure to build and operate an internal control system
  - Germany: Siemens case (Fleischer(2014), Bachmann(2014))
  - Korea: similar to Caremark claims (discussed later)
- 2. Breach of Statutes and Regulations
  - Breach of disclosure obligation under the securities regulation
    - ➢ Vulnerability, cyber risk, actual incident
  - Breach of technical standards and regulations on security measures

1. Oversight Duty

2. Statutes/ Regulations

Oversight Duty - US

- Caremark (1996), Stone (2006)
  - Duty to assure that a company has “a reasonable information and reporting system.”
  - “An utter failure to attempt to assure” such a system and “a sustained or systematic failure of the board to exercise oversight” may lead to “lack of good faith.”
  - Rhetorically impressive, but deemed very hard for plaintiffs to win.

Oversight Duty - US

- Recent Delaware cases on oversight duties
  - Marchand (2019): listeria in ice cream caused 3 deaths and recall (Blue Bell Creamery)
    - Monoline company ⇨ food safety is "mission critical"
  - Clovis (2019): violation of FDA protocol (Clovis Ontology)
    - Monoline company in highly regulated industry ⇨ compliance with FDA protocol is "mission critical"
  - Hu (2020): accounting fraud
  - Chou (2020): subsidiary's reg. violation in treating oncology vial overfills
    - Absence of board action even after internal warnings ("mission critical")
  - Boeing (2021): error in sensor of Boeing 737 MAX
    - absence of monitoring system for product safety, unlike other airplane manufacturers

⇨ These five Caremark claims survived a motion to dismiss.

Oversight Duty - US

- Oversight Duty Applicable to Cyber Risks?
  - Pace/Trautman, *Mission Critical: Caremark, Blue Bell, and Director Responsibility for Cybersecurity Governance*, Wisconsin Law Review (2022)
    - "Caremark liability for directors are greater than just a few years ago"
    - "Caremark liability will be centered on failure to provide board-level oversight of mission critical risks."
    - "**Cybersecurity is mission critical to effectively all large companies today."**
  - Ferrillo etc., HLS Forum of Corp Gov (2020)
    - "Blue Bell Creameries opens the door for a Caremark-like cybersecurity claim of bad faith against directors"

How to Fulfill Oversight Duty?

- Council of Institutional Investors (CII) of US: a list of questions for investors to pose to boards

1. How are the company's cyber risks communicated to the board, by whom, and with what frequency?
2. Has the board evaluated and approved the company's cybersecurity strategy?
3. How does the board ensure that the company is organized appropriately to address cybersecurity risks? Does management have the skill sets it needs?
4. How does the board evaluate the effectiveness of the company's cybersecurity efforts?
5. When did the board last discuss whether the company's disclosure of cyber risk and cyber incidents is consistent with SEC guidance?

How to Fulfill Oversight Duty?

- US National Association of Corporate Directors, Cybersecurity Handbook (2017): Five Principles
  - Principle 1: Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue.
  - Principle 2: Directors should understand the legal implications of cyber risks as they relate to their company's specific circumstances.
  - Principle 3: Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on board meeting agendas.
  - Principle 4: Directors should set the expectation that management will establish an enterprise-wide cyber-risk management framework with adequate staffing and budget.
  - Principle 5: Board-management discussions about cyber risk should include identification of which risks to avoid, which to accept, and which to mitigate or transfer through insurance, as well as specific plans associated with each approach.

Oversight Duty - Korea

- Daewoo Case (2008)
  - accounting fraud case: company's creditors (who were defrauded by the wrong financial statements) brought lawsuit against directors
  - executive directors who were not in charge of accounting matters were held liable for breach of "oversight duty" because they failed to build/operate internal control system
  - heavily affected by Caremark ("utter failure", "sustained or systematic failure of oversight")

Oversight Duty - Korea

- Union Steel Case (2021)
  - S/H's derivative action for the company' loss (=penalty paid to competition authority due to cartel [price fixing collusion])
  - CEO was found to be liable for breach of "oversight duty" (=failure to prevent such a cartel) due to lack of internal control system
- Daewoo Construction Case (2022)
  - S/H's derivative action for the company' loss (=penalty paid to competition authority due to cartel [repeated collusions in government biddings])
  - Not only executives but also independent (outside) directors were found to be liable for breach of "oversight duty" due to lack of internal control system

❖ In these two cases, the Korean Supreme Court said that "in areas where **high legal risks** are expected, oversight duty requires having an internal control system in place and operating it…" (influenced by "mission critical"?)

Oversight Duty - Korea

- STX Case (2022)
  - S/H's suit under the Capital Markets Act (false disclosure for accounting fraud)
  - CEO was held liable for breach of "oversight duty"
  - Court did not mention "high legal risk": no need to mention in an accounting fraud case

Oversight Duty - Korea

- Oversight Duty Applicable to Cyber Risks?
  - Would make sense in US, given hundreds of lawsuits against the companies & directors for cyber security issues
  - Reported 761 data breach cases in US between 2012-2016 [Park(2019)]
    - Including hacking, transfer by mistake, insider's leakage, disclosure by mistake, phishing etc.
    - Mainly customer class action; partly shareholder derivative suit, employee class action, insurer claim, acquiror's claim
  - Such suits are not so perverse and threatening in Korea: lack of class action, punitive damages, discovery + court requires strict proving of damages

Oversight Duty - Korea

- Oversight Duty on Cyber Risks in Korea?
  - No precedents yet.
  - In the future, probably yes.
    - ➢ Recent trends increasingly highlight the oversight duty of directors.
  - If similar security incidents happened repeatedly but the board did not take any action and no control system is in place, then the board members may be held liable for breach of oversight duty.

1. Oversight Duty

2. Statutes/Regulations

Cyber Security Statues/Regulations - Korea

- 1. Electronic Financial Transaction Act (“**EFTA**”) and its sub-regulations govern financial services industry
- 2. The Personal Information Protection Act (the “**PIPA**”) and other statutes govern data protection
- 3. The Act on the Promotion of IT Network Use and Information Protection (the “**Network Act**”) governs IT networks.

Financial Service Industry

- The EFTA requires financial institutions to comply with a set of regulations to ensure the security of their information systems and protect customer data.
- Key regulations:
  - Technical standards for IT systems and facilities
  - Obligation to hire cyber security experts
  - Notification of security incidents to the authority
  - Third-party risk management, such as due diligence on third-party service providers
  - Regular security audits
  - Penalties for non-compliance

Data Protection

- Relevant statutes:
  - The Personal Information Protection Act (the "**PIPA**") acts as a general law on processing and protecting personal data.
  - The Credit Information Use and Protection Act (the "**Credit Information Act**") regulates entities that collect, use, investigate, manage or provide credit information.
  - The Act on the Protection and Use of Location Information (the "**Location Information Act**") specifically targets the protection of "location information."
- Relevant authorities:
  - Personal Information Protection Commission ("**PIPC**") for PIPA
  - Financial Services Commission ("**FSC**") and Financial Supervisory Service ("**FSS**") for the Credit Information Act
  - Korea Communications Commission ("**KCC**") enforces the Location Information Act

IT Networks

- The **Network Act** prohibits any unauthorized access to a network system by means of a transfer or distribution of a program that may damage, destroy, alter or corrupt the network system, or its data or programs.
- It also obligates the operator of IT networks to satisfy certain security standards.

Cyber Security Statutes/Regulations – Korea

- Financial institutions are under tight regulations on cyber security by the regulators.
- Data protection is important and its enforcement is getting stronger, but private lawsuits are not yet very threatening (due to lack of punitive damages, discovery, and class action).
- IT Networks are regulated under Network Act, but the regulator cannot catch up the hackers' technology.
- EFTA, PIPC, and other statutes pay no attention to the role of board.

Conclusion

- Statutes/Regulations (rule-based approach) are still important for cyber security.
  - In particular, financial industry needs strict supervision and enforcement for the cyber security measure.
  - Existence of (and violation of) statutes/regulations gives rise to damage claims where duty of directors becomes at issue.
- But technical/mechanical compliance with these regulations are not sufficient.
  - because cyber risks take variable forms and keep changing (outsmarting the regulators).
- Oversight duty of directors needs further development, as a flexible standard-based approach to cope with cyber risks.
  - Should not be *no-fault-result-only* liability.
  - Should accompany with development of effective internal control system.

Selected Bibliography

- Edwards(2019), Cybersecurity Oversight Liability, Georgia State University Law Review 35, 663-677
- Evans(2019), Managing Cyber Risk
- Kempf(2022), The duty to monitor: how the mission critical doctrine in Marchand informs directors liability for cybersecurity breaches, Notre Dame Journal of Law, Ethics & Public Policy 36, 375-397
- Pace/Trautman(2022), Mission Critical: Caremark, Blue Bell, and director responsibility for cybersecurity governance, Wisconsin Law Review 2022, 887-952
- Sangchul Park(2019), Why information security law has been ineffective in addressing security vulnerabilities, International Review of Law and Economics 58, 132-145
- Trautman/Ormerod(2017), Corporate directors' and officers' cybersecurity standard of care: the Yahoo data breach, American University Law Review 66, 1231-1291

Thank you

Vielen Dank

谢谢

ありがとうございます

감사합니다