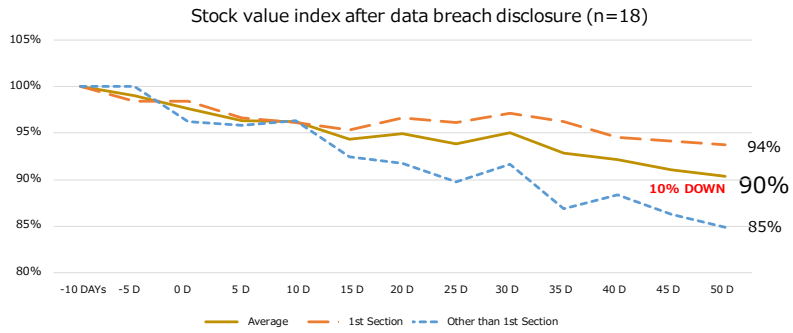
September 2018

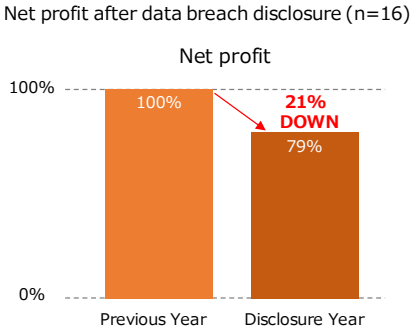
A cyber-risk estimation model to discuss in board of directors meetings

- Quantifying Cyber Risk Survey -

[Outline]

- Close to ¥63 trillion, nearly 0.8% of global GDP, was lost due to cybercrime in 2017, which is up from the CSIS and McAfee 2014 survey that put global losses at around ¥47 trillion[1]. For its part, the economic impact of cybercrime in Japan is estimated at around ¥1 trillion.
- According to our survey, the stock value index of 18 companies declined by an average of 10% from the day on which a data breach was disclosed, and the companies experienced an average decrease of 21% in net profit. Furthermore, there are many cases in which Japanese companies have faced a massive amount of direct financial loss and their CEOs gave up their salaries for several months to take responsibility.





- Unlike overseas companies, the majority of Japanese companies haven't discussed cyber risks in board of directors meetings. From the twin aspects of the responsibilities of board of directors and the rise of cyber risks, Japanese companies should discuss cyber risks as part of their corporate governance.
- The Japanese government should encourage and support an increased awareness of cyber risks by directors and managements of companies, as a critical issue to protect the progress of Japan's growth strategy.

What Japan should do to address cyber risks in board of directors meetings.

1. **Add a cyber-risk item to Japan's Corporate Governance Code**
   FSA, METI and the Japan Exchange Group should cooperate to add cyber-risk items to Japan's Corporate Governance Code.
2. **Cyber-risk estimation model**
   A cyber-risk estimation model (see Page 4) is needed to aid understanding of the business impact of cyber risks for directors and managements who are not familiar with information technologies.
3. **Increase awareness and develop training programs for directors and managements**
   An awareness program and a management training program are needed to help directors and managements understand cyber risks properly.

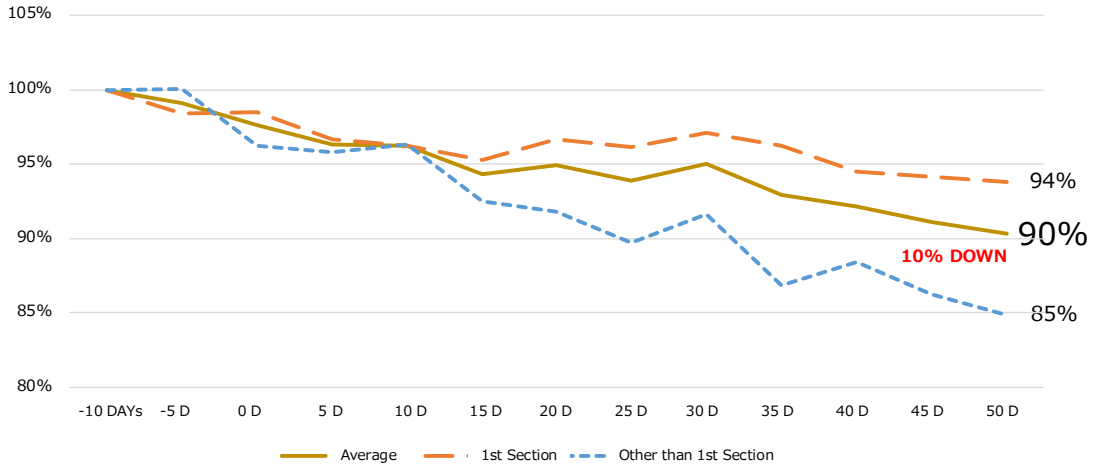
1 "Economic Impact of Cybercrime (2018)" https://www.mcafee.com/enterprise/ja-jp/about/newsroom/press-releases/press-release.html?news_id=2018030801

1. Why are cyber risks a management issue?

When cybersecurity is discussed within an organization, the tendency is for matters to be discussed from a technical point of view, such as new vulnerabilities being discovered or the fact that the number of new cyberattacks is increasing. However, directors and the managements of companies are more likely to be concerned with the potential financial impact and their responsibilities rather than with technical trends. Japanese companies should quantify their cyber risks, which is a common language of management, to aid understanding among executives who are not familiar with information technologies.

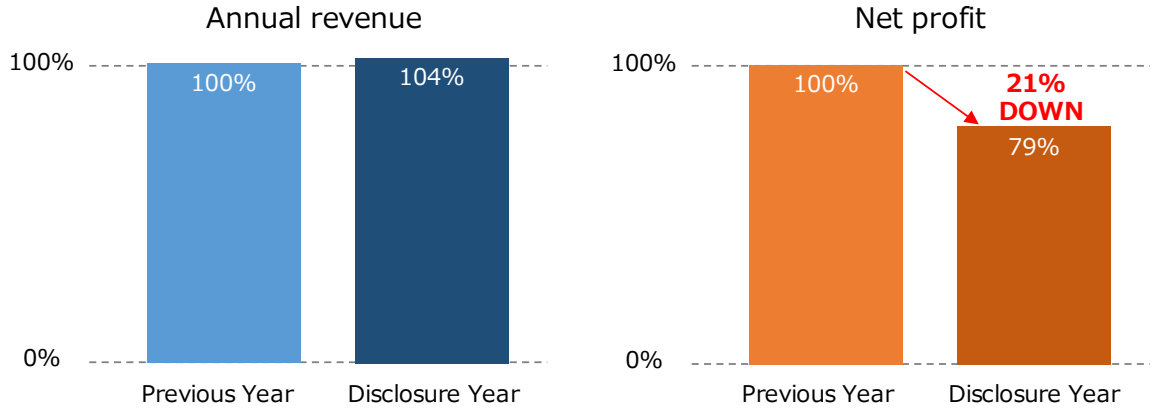
According to a JCIC survey, the stock value index of 18 companies declined by an average of 10% from the day on which a data breach was disclosed (see Figure 1). As the stock value index for other than the first section of the Tokyo Stock Exchange declined by an average of 15%, the survey made it clear that the impact of a data breach on small to midsize companies was greater than for large enterprises. This is because small to midsize companies depend on a single business model and the impact of cyber risk affects their business directly.

(Figure 1) Stock value index after data breach disclosure (n=18) (JCIC survey)



Moreover, 16 companies that disclosed data breaches experienced an average decrease in net profit of 21%. The reason for such a large decrease in net profit was an extraordinary loss for incident response, investigation, and additional security measures.

(Figure 2) Annual revenue and net profit after data breach disclosure (n=16) (JCIC survey)

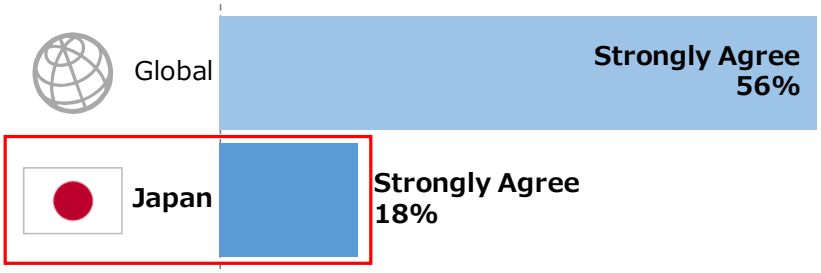


Thus it can be clearly seen that cyber risks lead to a decline in stock price and net profit. Furthermore, there are many cases in which Japanese companies have faced a massive amount of direct financial loss and their CEOs have given up their salaries for several months to take responsibility. The impact of cyber risks is so huge that cybersecurity is no longer just an IT department matter, but one of the top priorities for management.

2. Why haven't Japanese organizations discussed cybersecurity in board of directors meetings?

In order to enhance Japan's corporate governance, an amendment to the Companies Act was promulgated in May 2015. The amendment was enacted to encourage the supervisory function of boards of directors. Because cyber risks are one of the top priorities for management, more than half of global companies discuss cybersecurity in board of directors meetings. However, only 18% of Japanese organization said board of directors meetings should discuss cyber risks, compared with 56% of global organizations (see Figure 3).

(Figure 3) Question: Should boards of directors discuss cyber risks?



There are three reasons why Japanese organizations don't discuss cyber risks in board of directors meetings (see Figure 4). 1) There are no regulations or guidelines for doing so from the corporate governance point of view; 2) There are no indicators that directors can easily understand the cyber risk; and 3) Low awareness among directors, auditors, investors and management. Below are solutions for each issue.

1) FSA, METI and the Japan Exchange Group should cooperate to add cyber-risk items to the Japan's Corporate Governance Code. Since the Code has just been revised in June 2018, METI should add cyber-risk items to the CGS (Corporate Governance Systems) guidelines as a first step. In addition, it would also prove effective to amend the importance of the responsibilities of boards of directors in the Cybersecurity Management Guidelines.

2) A cyber-risk estimation model is needed to aid understanding of the business impact of cyber risks for directors and managements who are not familiar with information technologies.

3) Encouraging an increased awareness of cyber risks is also important. An awareness program and a management training program are needed to help directors and managements understand cyber risks properly. To maintain quality of the program, the issuance of certificates for the training program and lectures should be considered.

(Figure 4) Recommended solutions to raise awareness of directors

Issues	Recommended Solutions
1) No regulations or guidelines from the corporate governance point of view	Add a cyber-risk item to **Japan's Corporate Governance Code, CGS guidelines, Cybersecurity Management Guidelines** and more.
2) No indicator that directors can easily understand cyber risks	**A cyber-risk estimation model** is needed to aid understanding of the business impact of cyber risks for directors and managements who are not familiar with information technologies.
3) Low awareness among directors, auditors, investors and managements	**Raise awareness and develop a training program** for directors, auditors, investors and managements.

3. Cyber-risk estimation model

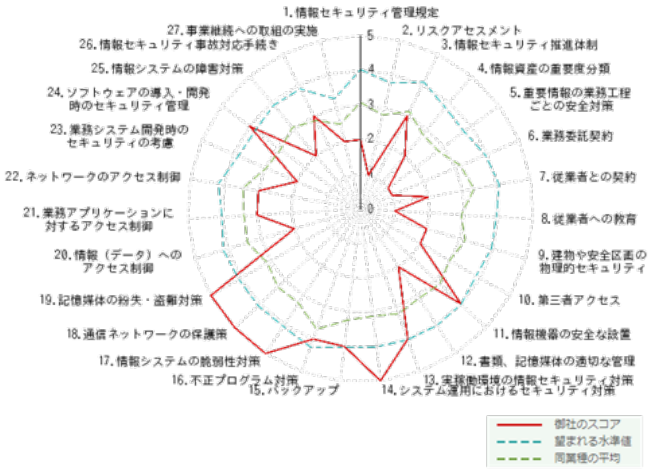
An example of a cyber-risk estimation model is shown below (Figures 5 and 6). The diagram shows an illustration of a company with annual revenue of ¥100 billion. The purpose of the model is for submission to board of directors meetings to encourage discussion among directors and managements.

(Figure 5) Probable maximum loss (An example of a company with an annual revenue of ¥100 billion)

		Probable Maximum Loss	Note
Direct Loss	①Loss of Personal Identified Information Leakage	- ¥8 B	Calculated by JO Model (JNSA) Value of Basic Information X Degree of Information Sensitivity X Degree of Ease in Identifying X Degree of Social Responsibility X Appraisal of Post-Incident Response X Number of Leakage
	②Loss of Business Downtime	5 Days - ¥2 B	Calculated by internal interview (production per day X product unit price) + (online sales per a day)
	③Fines and Penalties by Violation of Law	- ¥4 B	Example of fines of EU-GDPR 4% of annual global turnover or €20 M (whichever is greater)
	④Incident Response Fee	- ¥60 M	Calculated by prior incident or interview Investigation Cost + Recovery Cost +Prevention Cost and more
Indirect Loss	⑤Loss of Net Profit	- ¥1 B	Calculated by JCIC survey Last Fiscal Year's Net Profit X 21%
	⑥Loss of Market Capitalization	- ¥30 B	Calculated by JCIC survey Market Capitalization X 10%

(Figure 6) Benchmark and Investment

⑦Benchmark Results	Deviation Value 42.7	Our organization faces high risk, as a result of industry benchmark.
⑧The total investment to meet industry's ideal level	5 years total ¥1.3 B	To achieve deviation value of 50, our organization needs the following investment. Initial : ¥300 M Running : ¥200 M X 5 years



Score	76 / 135 points (Deviation Value 42.7)
Industry Ideal Level	107 / 135 points
Industry Average	84 / 135 points

Source : IPA
Information Security Management Benchmark

The cyber-risk estimation model above is simplified for the use of any industry or any size company. More-detailed risk estimation services are provided by insurance companies or consulting firms.

[Author]

Kenji Uesugi, JCIC Senior Fellow uesugi@j-cic.com

Toshihiro Hirayama, JCIC Senior Fellow hirayama@j-cic.com