

Abstract

1. The advance of digitalization is being accompanied by the rise of cyber risks that can have a huge impact on corporate value, financial and capital markets, the economy and society as a whole, and in some cases people's lives. As such, cybersecurity is becoming an increasingly important issue.
2. A wide range of measures that respond to the threat of cyber risks are being taken by the financial institutions that are key stakeholders in financial and capital markets, corporations that need to raise funds in the financial markets, investors that provide that funding, evaluation agencies, financial regulators and supervisory authorities, governments, and other entities in many countries and regions. These measures include multilayered initiatives based on corporate governance, information disclosures, investor behavior, valuations, financial product development, financial regulation and supervision, and other guidelines. The various initiatives of self-discipline being taken by the financial and capital markets and by each stakeholder are encouraging stronger measures by all concerned parties.
3. Cyber risks are constantly becoming more serious and complex, and while the initiatives mentioned above must be sustained, there are some other issues that need to be addressed. One of these is strengthening the development of human resources that will be needed to respond to and mitigate cyber risks not only in financial markets but also in society at large. The advancement of digital transformation (DX) and artificial intelligence (AI) and the intensification of geopolitical risks must be closely monitored for their potential to create new cyber risk threats.
4. In addition to the individual initiatives of financial and capital markets, financial institutions, corporations, and investors, cooperative and collaborative efforts will be needed to reduce of cyber risks and realize a sustainable society.

I. Reasons for Establishing the “Research Group on Cybersecurity Related to Investment and Financial Systems” and its Objectives

The Nomura Institute of Capital Markets Research (NICMR) established the Research Group on Cybersecurity Related to Investment and Financial Systems (hereafter, the Research Group) in July 2023. The Research Group consists of academics and other professionals with experience related to cybersecurity (see Appendix 1: Members of the Research Group on Cybersecurity Related to Investment and Financial Systems).

The advance of digitalization is being accompanied by the rise of cyber risks that can have a huge impact on corporate value, financial and capital markets, the economy and society as a whole, and in some cases people’s lives. As such, cybersecurity is becoming an increasingly important issue. How to best respond to cyber risks in the financial and capital markets has become a topic of discussions in many countries and regions around the world, with a focus on corporate governance, information disclosures, evaluation, investor behavior, and financial product development. In the United States, financial securities are making greater efforts to strengthen the financial sector’s response to cyber risks, with a focus on regulatory reforms in the securities markets. In Japan, it is widely recognized that the promotion of thorough measures, including systemic measures, will be indispensable to the preservation and enhancement of corporate value and the sound development of Japan’s financial markets.

NICMR’s keen awareness of these issues led it to establish the Research Group to conduct research focused on cybersecurity from the perspective of investment and financial systems and identify the current situation and issues in Japan from multiple perspectives that take into consideration trends in other countries and then determine the responses required of stakeholders. The Research Group held ten meetings from July 2023 to April 2024 at which it discussed research reports that focused on cybersecurity from a wide range of perspectives, including corporate management and governance, information disclosures, investment, evaluation, financial products, financial regulation, and human resource development. (See Appendix 2 for a list of the main themes covered by the Research Group)

These themes include a wide range of issues that need further consideration and discussion as the situation is constantly changing. For this reason, rather than rushing to draw conclusions that present a unified view and recommendations, the Research Group focused on highlighting the various issues needing to be addressed in each theme and valuing the knowledge gained from identifying the trends in each specialized field.

II. Views & Insights Presented at Research Group Meetings

The Research Group has maintained this unbiased stance while reviewing research reports and holding discussions at its meetings. As a result, the Group has been able to obtain a wide variety of views and insights. The following is a summary of the topics covered during group meetings and, in line with the Research Group’s stance stated above, does not represent a unified view or recommendations of group members.

Current Situation in Japan and the World

The rapid advance of the information society around the world since the late 1990s has been accompanied by the rise of cybercrime. The impact of attacks on companies and concerns about the wider effect on society as a whole is increasing the importance of cybersecurity. In recent years, the materialization of cyber risks has caused declines

in the stock prices of some companies, and financial institutions that have come under cyberattacks have had their payment and settlement functions temporarily disabled. In some cases, customer information has also been leaked. Such events have made security measures essential in the financial markets.

The May 2021 ransomware attack on U.S. oil pipeline operator Colonial Pipeline contributed to a greater awareness among corporate executives of the importance of cybersecurity in corporate governance. Research Group discussions have recognized that there are differences in corporations' awareness of the importance of cybersecurity and that information disclosure is important for securing the trust of stakeholders, including investors.

Corporate Management

When considering cybersecurity, it is also important to consider changes in the environment from the perspectives of security, systems, and management. In recent years, environmental changes such as the spread of the COVID-19 virus have accelerated the digitalization of society, giving rise to the view that all industries are now exposed to the threat of cyberattacks. Given this condition, one view expressed at Research Group meetings is that, while corporate executives are highly aware of cyber risks, they need to increase their knowledge of cybersecurity. Another view that has been expressed is that an effort should be made to increase small business' efforts to strengthen cybersecurity. Organizational issues that business enterprises and financial institutions must deal with include securing human resources, raising management's understanding, and securing necessary budgets.

Corporate Governance

When discussing Japanese companies' efforts to address cybersecurity risks, several members of the Research Group mentioned that companies need a greater awareness of the relationship between management and cybersecurity. It has been noted that Japan's Corporate Governance Code and Guidelines for Investor and Company Engagement do not sufficiently address cybersecurity from the perspective of corporate governance. Meanwhile, it was pointed out that data security has become an important item of governance in other countries, and it was suggested that corporate directors should seek to discuss and decide on the development of systems and information disclosures from a corporate governance perspective.

Current State of Information Disclosure

In addition to reports required by regulatory authorities, which focus on compliance with conventional regulations and the occurrence of problems, in recent years there has been greater promotion of investment-related information disclosures that take into consideration such factors as corporate value and investment decisions. One view expressed at Research Group meetings was that greater recognition by investor groups of cybersecurity as an issue of corporate governance could promote more discussions of investment-related information disclosures.

ESG (Environment, Social, and Governance) disclosure frameworks are increasingly pushing bond issuers to disclose their cybersecurity measures, and cyber risk factors are beginning to be reflected in investor decisions and ESG rating agencies' evaluations. Japan is seeing an increase in activities promoting engagement between investors and corporations, such as the Ministry of Economy, Trade and Industry's surveys of investors and research seminars held by private-sector companies. It was pointed out during Research Group meetings that disclosures of cybersecurity-related

information need to be based on a clear understanding of what is being requested and by whom.

Investors' Perspectives

If institutional investors base investment decisions on their evaluations of companies' cybersecurity risks and the measures taken to prevent those risks from materializing, it could encourage companies to proactively improve disclosures. The Research Group was presented with a case study of an asset management company that quantifies, scores, and integrates cybersecurity risks into its ESG investment decisions.

While such progressive initiatives are beginning to be seen, it was pointed out that there still are differences in the perception of cybersecurity as a major business risk among companies and among investors. It has also been pointed out that cybersecurity-related regulations are far from sufficient, and there is a lack of information disclosure about cyber incidents. It has been also told that investors' engagements with companies often revealed that management does not regard cybersecurity as a topic for discussion and that it is therefore necessary to raise management awareness of the importance of cybersecurity.

Financial Regulatory Authorities' Stance

Given the frequent occurrence of cyberattacks on the financial sector, financial authorities and international organizations around the world are pushing financial institutions to make greater efforts to address cyber risks. Authorities in the United States are promoting measures that may affect the business operations of financial institutions, while international organizations are focused on raising the international baseline. Going forward, the areas that are most meaningful for national authorities and international organizations to address are cyber human resource development in financial institutions, the state of risk sharing, and the cyber risks included in related measures.

The first cybersecurity regulation imposed on China's securities industry is the Administrative Measures for Network and Information Security in Securities and Futures Sectors, which was announced in February 2023. The Measures include the establishment of a centralized data backup system by the China Securities Regulatory Commission (CSRC) and strengthening the management and supervision of IT service providers. Research Group members consider the effectiveness of the initiatives related to these Measures to be worthy of attention.

Financial Product Development

Cyber insurance is a possible cybersecurity initiative. While the global cyber insurance market is expanding, some Japanese companies' awareness of potential cyber risk-related crises is still quite limited. As such, Japan needs to make a greater effort to promote widespread use of cyber insurance. Issues that need to be addressed to support the spread of cyber insurance in Japan include (1) raising awareness of cybersecurity, (2) strengthening companies' cybersecurity measures, and (3) increasing the sustainability of nonlife insurance companies' cyber insurance business.

Evaluations

Major credit rating agencies S&P Global Ratings and Moody's Investors Service have been collaborating with cybersecurity rating agencies on measures to strengthen the provision of solutions related to cyber risk. S&P Global Ratings incorporates cyber risk as an element when assessing a company's management and governance during the rating process. Moody's has not specifically stated how it factors cyber risk into its credit ratings, but it has published a heat map showing cyber risk scores for each industrial sector. In addition, US cybersecurity rating companies SecurityScorecard and Moody's affiliate Bitsight quantitatively analyze companies' cybersecurity risks and assign scores from the perspective of their vulnerability to attacks.

The Research Group considers how nonfinancial information, including these credit rating agencies' evaluations of cyber risk, can be linked to corporate value as a subject for future study.

Development of Human Resources

Companies need to secure and maintain excellent human resources to steadily implement cybersecurity measures. However, Japanese companies have a serious shortage of cybersecurity human resources. The human resources being referred here, to include personnel in such strategic management areas as corporate risk management as well as on-the-ground technical areas. Considering the importance of gaining management's commitment and oversight by executive directors, it is essential that management and other personnel have a sound understanding of cybersecurity.

The Research Group had many discussions about the current status of cybersecurity human resource development and related curriculum development at academic institutions. These discussions tended to focus on (1) companies' management staff, (2) strategic management staff, and (3) on-site staff and technicians. Research Group members agreed that strategic management staff was the human resource that could best bridge the gap between management and on-site staff and technicians. As for the actual situation at Japanese companies, it was pointed out that many chief information security officers (CISOs) are generalists rather than specialists in the field of cybersecurity, and that management teams probably need to have the knowledge of a certified information security manager (CISM).

III. Conclusion

The Research Group has conducted deep discussions on a variety of cybersecurity-related issues. Following is a summary of its findings gained through the discussions from the perspectives of financial institutions and the financial and capital markets.

It was determined that financial markets and financial institutions need to promote two specific activities regarding cybersecurity and that it will be important to have entities that encourage these activities.

The first activity is the creation of governance systems in the self-disciplined manner, in the financial markets and at each financial institution and incorporating cybersecurity measures part of those systems. Financial markets and institutions play important roles in the economic and social infrastructure, and cyber incidents therefore can affect people's lives as well as the targeted financial market or business. It therefore can be said that cybersecurity activities by financial markets and the financial institutions active in those markets are important from the perspective of their responsibility to society as a whole.

The second activity is support for the cybersecurity efforts of corporations and investors, which are key stakeholders in the financial and capital markets. For example, financial markets and institutions should require that companies and other entities seeking to procure funding in the financial markets implement strong cybersecurity measures and make appropriate information disclosures that will contribute to the maintenance of their corporate value and ability to secure funding when needed. In addition, financial institutions should use their financial products and services to support corporate cybersecurity measures. With regard to investors who essentially supply the cash used to fund corporations, financial institutions should provide them with research information that will improve their investment performance and propose optimal investment portfolios related to cybersecurity. In addition, financial institutions and investors should use their investment and engagement activities to encourage companies to strengthen their cybersecurity measures.

While financial markets and financial institutions are expected to conduct these two activities on their own, their efforts need to be encouraged by external entities demanding discipline through various evaluations (creditworthiness, ESG, cybersecurity ratings and scores, etc.), financial regulations and supervision, and government guidelines. These external parties' efforts can lead to better cybersecurity measures because will provide objective analysis of which measures are appropriate and recommend areas that should be strengthened.

The Research Group has clarified the need for the two activities mentioned above, but cyber risks are constantly becoming more serious and complex. Accordingly, while the above activities must continue to be promoted, there are some other issues that need to be addressed. One of these is strengthening the development of human resources that will be needed to respond to and mitigate cyber risks not only in financial markets but also in society at large. The advancement of digital transformation (DX) and artificial intelligence (AI) and the intensification of geopolitical risks must be closely monitored for their potential to create new cyber risk threats.

Another subject that must be considered as we aim to strengthen cybersecurity is the "risks and opportunities" presented by climate change. For example, the development of new cybersecurity-related financial products is expected to contribute to the improvement of cybersecurity in the financial and capital markets while also providing new investment opportunities. In addition, further empirical research on cyber risks and opportunities and how they may potentially affect corporate value is needed from the perspective of financial and capital markets and investors.

Although cyber risk threats are likely to increase in the future, the Research Group believes that reducing cyber risk and realizing a sustainable society can be achieved if all stakeholders, including the financial markets, financial institutions, companies, and investors, maintain constant individual and collaborative efforts to strengthen cybersecurity.

Details of the results of the Research Group's activities will be announced at a later date.

Appendix 1: Members of the Research Group on Cybersecurity Related to Investment and Financial Systems

(Members' titles are as of March 31, 2024)

Research Group Members

Gen Imagawa	Senior Officer, Investment Banking Business Development Department, Nomura Securities Co., Ltd.
Akane Enatsu	Head of Nomura Research Center of Sustainability, Nomura Institute of Capital Markets Research
Tomomi Kadokura	Research Associate, Nomura Institute of Capital Markets Research
Hideki Kanda	Professor, Gakushuin University Law School, Emeritus Professor, University of Tokyo
Jason Mortimer	Head of Sustainable Investment – Fixed Income, Nomura Asset Management
Kenji Tominaga	Senior Analyst, Nomura Institute of Capital Markets Research
Akiko Nomura	Managing Director, Nomura Institute of Capital Markets Research
Masayo Fujimoto	Professor, Institute of Information Security
Mitsuhiko Maruyama	Partner, PwC Consulting LLC
Chie Mitsui	Senior Researcher, Nomura Research Institute

Observers

Financial Services Agency

Ministry of Economy, Trade and Industry, Commerce and Information Policy Bureau, Cybersecurity Division

Appendix 2: Topics Covered at Past Meetings

First Meeting (July 4, 2023)

- Overview of cybersecurity from the perspective of financial markets

Second Meeting (August 29, 2023)

- Cybersecurity from perspective of investors
- Cybersecurity evaluation companies' views

Third Meeting (September 20, 2023)

- Recent trends in security
- Corporate management and cybersecurity

Fourth Meeting (October 25, 2023)

- Corporate cybersecurity risk and cyber insurance

Fifth Meeting (November 22, 2023)

- Cybersecurity and governance

Sixth Meeting (December 13, 2023)

- Credit ratings and cyber risks

Seventh Meeting (January 17, 2024)

- Cybersecurity and financial systems
- Cybersecurity and evaluations

Eight Meeting (February 6, 2024)

- Cybersecurity and information disclosures
- Recent trends in cybersecurity measures
- Some thoughts from recent U.S. cybersecurity conference

Ninth Meeting (March 6, 2024)

- Cybersecurity and human resources
- Nonfinancial corporations' cybersecurity operations
- Management responsibility for cybersecurity

Tenth Meeting (April 19, 2024)

- Future discussion topics