Noriko Fujita

Director
CIO (Chief Information Officer)
CISO (Chief Information Security Officer)
CSO (Chief Sustainability Officer)
Division General Manager of Group Administrative Headquarters
Bandai Namco Holdings Inc.

President and CEO
Bandai Namco Business Arc Inc.

CIO/CISO'S MESSAGE

We are working to build an environment that supports sustainable growth by integrating IT infrastructure and information security

Bridging Between Group Strategies and Day-to-Day Business Execution

In my position as CIO, I provide support for data utilization across Group companies around the world in corporate and business divisions through the establishment of IT infrastructure. At the same time, as CISO, I strive to improve our level of information security. The IT infrastructure that is necessary differs across our diverse range of businesses. Accordingly, we are working on both the development of a shared Groupwide foundation and the creation of tailored environments for individual companies based on their specific business characteristics.

In these efforts, it is crucial to engage in decision-making and take action based on Groupwide perspectives and an understanding of the operating environment of each business. It is also important to promote collaboration to build a unified approach across all Group companies. Drawing on my experience at our business companies, I will work to bring new business perspectives to our IT initiatives, giving proper consideration to how each initiative will be implemented at each individual company. In this way, I will strive to bridge the gap between Group strategies and day-to-day business execution.

In consideration of our efforts to raise the level of IT and information security, which are currently in a transitional phase, I believe it is extremely logical to hold the dual role of CIO and CISO. By ascertaining the current state of security measures from the perspective of CISO while closely examining our IT environment from the standpoint of CIO, this dual role enables a more disciplined and responsive IT governance.

With regard to data utilization, in addition to Groupwide initiatives led by the CW360 Division, each individual company and business division are promoting a broad range of their own efforts. In corporate divisions as well, we are engaging in activities such as establishing systems shared across the Group and standardizing data.

The utilization of AI is another important aspect to consider. To that end, we are formulating guidelines for AI utilization on a Groupwide and individual company basis, examining utilization methods through ongoing discussions. Moreover, we have commenced the trial utilization of AI in corporate divisions with the aim of enhancing operational efficiency. While maintaining an awareness of the risks posed by AI, we will continue to extensively examine the potential of its utilization moving forward.

Enhancing Our Groupwide Security Level

Due to the diverse nature of the Group's business operations, the content, volume, and management method of data handled by each company differs. From the perspectives of data utilization and enhanced security, we will conduct a comprehensive data inventory and implement appropriate response measures.

To raise awareness among employees at Group companies around the world, we are implementing e-learning programs on an ongoing basis, conducting initial response drills in the event an incident occurs, and taking steps to keep employees informed about incidents that have occurred both inside and outside the Group. Additionally, we hold regular study sessions, both online and in-person, for IT and security personnel worldwide business companies and regional management companies. At these sessions, we share information on current issues and promote an understanding of response measures.

Through these efforts, we have made great progress in recent years with the standardization of groupware and IT infrastructure. We are also collaborating with responsible personnel at each company to manage relevant data and promote security measures for front-office applications and public websites.

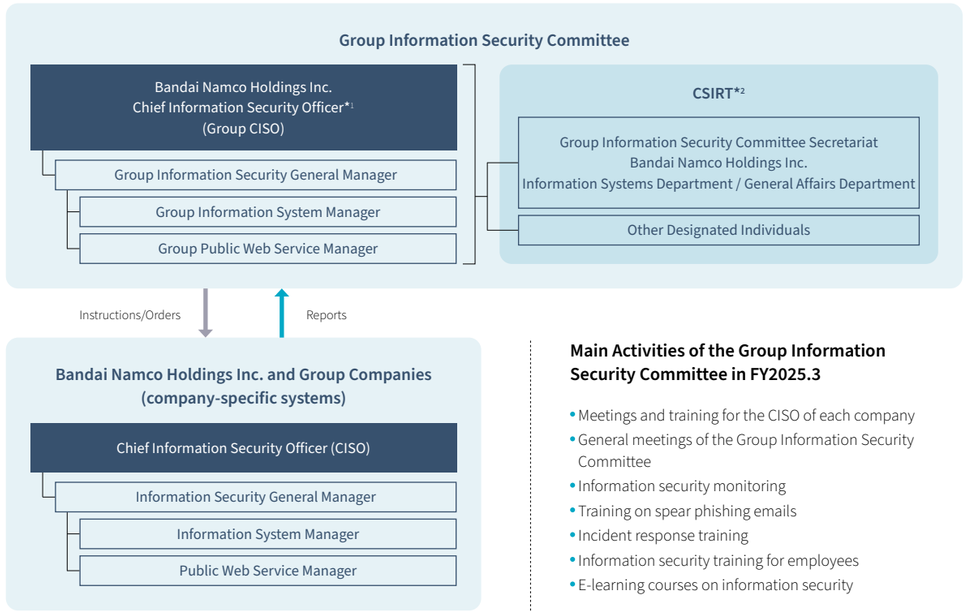
In terms of establishing and operating our information security framework, we will continue to monitor social trends and changes so that we may constantly update our knowledge while continuously pursuing response measures to minimize any vulnerabilities.

Realizing a Future Supported by IT

Guided by our Purpose, which is the ultimate definition of the Group, we aim to create 360° connections with our fans around the world, which include IP fans, a wide range of business partners, shareholders, Group employees, and society as a whole. To achieve this aim, it is imperative that we promote IT strategies and data utilization. Doing so is also essential for our day-to-day operations.

We will therefore focus our attention on building an IT infrastructure and implementing more robust security measures while deepening collaborations with each company and region. We will also promote measures that support the daily activities of our employees. By doing so, we will strive to achieve a future in which we are more broadly and deeply connected with fans. As we seek to achieve growth in our diverse businesses and expand our areas of operations, we will continue to promote Group strategies from an IT perspective so that we can maximize our business opportunities while minimizing risks.

Overview of the Group's Information Security Framework



Main Activities of the Group Information Security Committee in FY2025.3

- Meetings and training for the CISO of each company
- General meetings of the Group Information Security Committee
- Information security monitoring
- Training on spear phishing emails
- Incident response training
- Information security training for employees
- E-learning courses on information security

*1 Director responsible for the Information Systems Department
*2 Computer security incident response team; an organization that implements information security countermeasures.