

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

“Supporting Data Utilization Across Our Business Domains Through a Defensive Digital Strategy to Drive Group Growth”

Strengthening IT Infrastructure and Information Security in an Integrated Manner

As the CIO and CISO of the Company (holding company), my responsibilities can be broadly divided into two areas. First, as CIO, I am responsible for establishing the IT infrastructure that underpins the Group's growth, including management systems and data governance. Second, as CISO, I strive to strengthen information security so that we can continue to connect with fans and business partners in a secure and trustworthy manner. Looking back on my first year in these dual roles, I have reaffirmed the importance of pursuing these objectives while also gaining valuable insights into how best to advance the initiatives needed to achieve them.

The diversity of our Group's business portfolio and business models is one of our greatest strengths. At the same time, however, it presents unique challenges from the perspectives of IT and information security. Going forward, we will carefully determine which functions should be standardized across the Group and which should remain under the management of individual business Units or companies. Through this approach, we will establish an effective IT governance framework that balances Groupwide consistency with business-specific flexibility.

In April 2026, we also renamed the department responsible for promoting these initiatives from the Information Systems Department to the Digital Management Department. By adopting the broader and more

accessible concept of "digital," we aim to promote Groupwide initiatives that are directly linked to management priorities and business needs.

Building an IT Foundation That Supports the Growth of Our Diverse Businesses

The Group's businesses continue to grow by strengthening collaboration across business domains and expanding into new markets. Establishing a robust IT foundation is essential not only to support these ongoing operations but also to accelerate future growth. To this end, we are clearly defining which IT capabilities should remain tailored to the specific needs of individual companies and which should be standardized across the Group.

Through the implementation of a Groupwide ERP system and the integration of master data, we aim to improve data consistency, increase the speed of information sharing, enhance the efficiency of reporting and aggregation processes, promote more effective data utilization, and further strengthen information security.

Until now, many of our individual companies have relied on dedicated personnel with extensive experience to support their proprietary systems. Going forward, however, we will also foster IT talent through the deployment of the Group ERP system, enabling us to respond more flexibly to organizational restructuring and closer collaboration with our overseas operations.

Promoting AI Utilization and Strengthening Data Governance

Across our Group, the use of AI is expanding in both its business operations and corporate functions. We believe that the implementation of a Groupwide ERP system and the integration of master data will establish a more consistent data foundation, enabling greater Groupwide advantages in areas such as management control and back-office operations.

Until now, AI initiatives have primarily been developed to address the specific needs of individual businesses. As these initiatives have delivered results, however, opportunities to share successful practices and expertise across the Group have continued to increase, further expanding the potential applications of AI.

In response to these developments, we are strengthening our data governance framework to ensure that AI can be utilized securely and responsibly. By establishing clear governance structures, guidelines, and rules—including clarifying data ownership, accountability, and appropriate access rights—we aim to create an environment that encourages the effective use of data while maximizing its value. Through these efforts, we hope to empower both our businesses and our employees to further enhance their respective strengths.

Strengthening Groupwide Information Security

In the FY2026.3, we introduced a new framework for information security management. Under the previous framework, the holding company directly monitored each Group company. We have now transitioned to a structure in which monitoring is conducted in collaboration with our business management companies and regional management companies. Improving the effectiveness and speed of our security initiatives requires an approach tailored to the unique risk profiles of each business and region.

Enhancing the IT literacy of every employee is also essential to strengthening the Group's overall security. While we continue to reinforce communication from the holding company through training programs and awareness initiatives, we also work closely with the CISO of each Group

company to ensure that our messages are translated into each employee's day-to-day work and effectively embedded in day-to-day operations.

As CISO, I also take very seriously the incident involving the Bandai Channel video streaming service that occurred in November 2025. At the time of the initial report, we took the precautionary measure of temporarily suspending the service, as the possibility of unauthorized access resulting in the leakage of personal information could not be ruled out. We subsequently conducted a thorough investigation with the support of external specialists to identify the root cause and assess the extent of the impact. Based on the findings, we implemented the necessary countermeasures.

Although our initial response proceeded smoothly overall, we recognize that the investigation took longer than anticipated. We take these lessons seriously and are sharing them across the Group to further strengthen our information security measures going forward.

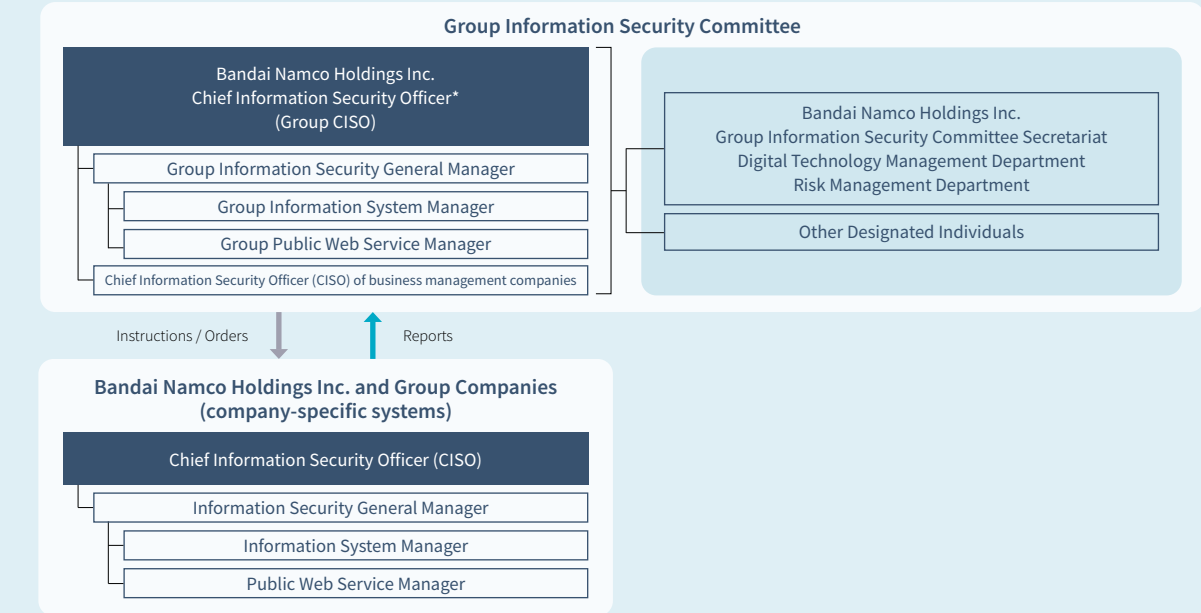
Balancing Offensive and Defensive Digital Strategies

As cyberattacks continue to grow in both complexity and frequency, preventing every security incident has become increasingly difficult. Rather than assuming that incidents can be eliminated entirely, we are strengthening our business continuity planning (BCP) based on the premise that incidents may occur and that rapid recovery is essential. Working closely with each business, we will continue to review and validate the effectiveness of our response capabilities.

From this perspective, it is equally important to reassess, during normal operations, how our systems are managed and how our data is stored across the Group. I believe that strengthening information security as CISO and building a robust IT foundation as CIO are inseparable responsibilities that together provide the foundation for resilient digital operations.

To deliver products and services that exceed the expectations of our fans, proactive data utilization across our business divisions is indispensable. We will contribute to the sustainable growth of the Group by supporting this "offensive" digital strategy with a "defensive" digital strategy centered on a strong IT foundation and robust information security.

Overview of the Group's Information Security Framework



* Director responsible for the Digital Management Department