Cybersecurity and AI Ethics

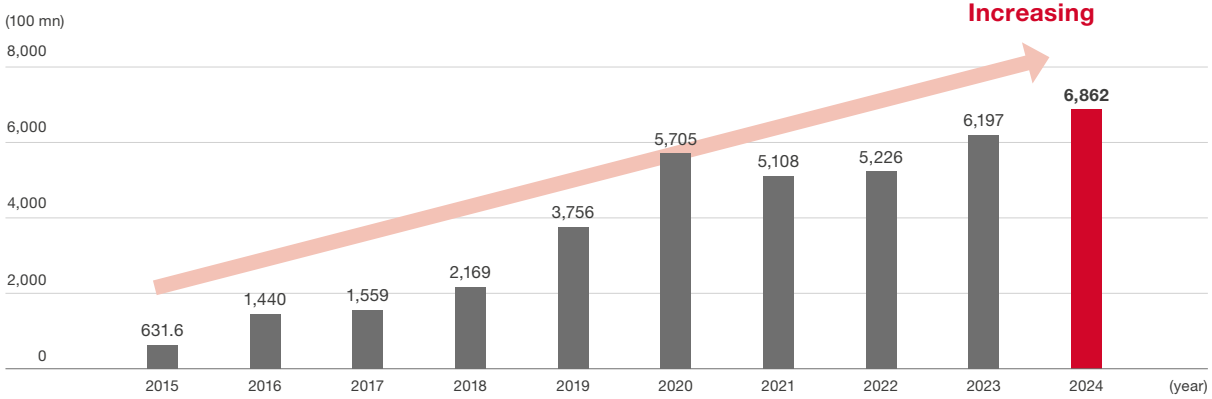
The management of digital-related risks, particularly those centered on information security, is becoming increasingly important. For example, in past incidents involving attacks on the servers of a major publishing company and a major beverage manufacturer, the damage was not limited to information leaks. In some cases, the attacks led to the stoppage of customer-facing sales systems and forced prolonged shipment stoppages or restrictions, resulting in significant financial impacts.

In the World Economic Forum's *Global Risks Report 2025*, cyber security–related risks rank among the top global risks in both the short term (within the next two years) and the long term (within the next 10 years).

Risk awareness is likely already widespread among corporate senior management teams, but the threats continue to intensify. In the Information Technology Promotion Agency's (IPA) *Top 10 Information Security Threats to Organizations* (2025 Edition), ransomware attacks remain the top threat, as they have consistently in previous years, while attacks targeting supply chains and vendors rank second. In addition, cyberattacks stemming from geopolitical risks have newly entered the rankings, underscoring the growing diversity of threats.

In recent years, malware and other types of cyberattacks have been on the rise. According to a survey by the National Institute of Information and Communications Technology (NICT), the total annual number of observed packets related to cyberattacks in 2024 reached 686.2 billion, representing an approximately tenfold increase over the past decade.

Total Annual Number of Observed Packets*



Source: Prepared based on the National Institute of Information and Communications Technology's *NICTER Observation Report 2024*
*Total number of packets related to cyberattacks observed in the NICTER Project

The actual damage is growing to a scale at which, in addition to direct losses and recovery costs, the impact on business operations can no longer be ignored. If the recovery process takes time, competitors may step in with substitute products or services, potentially leading to a loss of market share and prolonged negative impacts on business performance.

Also, for investors, deteriorating business performance can have an impact in the form of falling share prices and lower creditworthiness. It is also necessary to consider the degree of importance by sector. Cybersecurity is considered particularly critical for industries where cyberattacks could have major societal consequences, such as aviation, land transportation, and logistics; industries that support social infrastructure such as electric power and telecommunications; and financial institutions such as banks. E-commerce, in which consumers transact directly with companies online, is also of relatively high importance. In addition, companies may become targets for cyberattacks if they are seen as financially valuable or geopolitically significant.

For investors, it is challenging to possess the expertise needed to analyze cybersecurity in depth. As an approach, in addition to using external data, it is possible—particularly in important sectors—to identify gaps at a given company through comparisons within the industry. Examples include governance-related factors such as information security policies and the status of the organizational framework, as well as operational aspects such as the status of security monitoring. If such analysis results in improvements being deemed necessary, investors can engage with the company. While many companies have implemented countermeasures, disclosure is sometimes insufficient. Encouraging the disclosure that investors need is therefore also important.

In the Digital Inclusion Benchmark conducted by the World Benchmarking Alliance, companies' and other organizations' efforts toward an inclusive digital economy and society are evaluated from four perspectives: access to digital technology; digital skills; the use of digital technology; and innovation. Among these, elements related to a company's information security governance include the establishment of policies and systematic frameworks, incident response, and acquiring ISO27001 certification.

We also place particular importance on three major elements. The first is the formulation and disclosure of policies that demonstrate commitment from top management. The second is the establishment of a peacetime framework, including the identification of responsible personnel and the creation of a framework such as a CISO (Chief Information Security Officer) and expert committees. The third is the establishment of an emergency response framework, namely a CSIRT (Computer Security Incident Response Team).

According to our research (as of September 2025), the status of policy formulation, peacetime frameworks, and emergency response frameworks among TOPIX 100 constituent companies has improved compared with one year earlier, as shown in the table below. However, we believe that a relatively significant challenge remains in terms of the development of peacetime frameworks, such as identifying responsible officers and establishing committees. In particular, many companies still do not have a CISO in place, and the shortage of qualified personnel is likely one of the reasons for this. In this context, talent development is an issue not only in terms of those with overall responsibility but also for employees at the working level. In addition, efforts to address global supply chains are also a challenge. In particular, business partners at overseas locations may raise concerns about cybersecurity vulnerabilities. Companies are therefore expected to assess cybersecurity risks within their supply chains and continue monitoring those risks.

Status of Information Security Measures among TOPIX 100 Companies

		Policy	CISO	Committees	CSIRT	All measures in place
Overall TOPIX 100 (Previous survey: December 2024)	Number of companies with measures implemented	70	64	49	80	41
Overall TOPIX 100 (Current survey: September 2025)	Number of companies with measures implemented	77	70	59	85	63
Difference (Previous → Current)		**7**	**6**	**10**	**5**	**22**

Source: Nomura Asset Management, based on disclosed company materials and websites

Next, when looking at the risks associated with the use of AI, a wide range of risks exist, from technical risks and social risks (the amplification of existing risks), to information security issues, misinformation, and ethical concerns.

Looking at the state of AI use in companies, the use of language-based generative AI is advancing with the aim of improving internal productivity. One of the major concerns for companies is the leakage of information outside the company, and there is a growing need to establish AI governance to enable the responsible use of AI in practice. The *AI Guidelines for Business* issued by the Ministry of Internal Affairs and Communications and the Ministry of Economy, Trade and Industry call not only for legal compliance, but also for respect for human rights, diversity, and a sustainable, fair, and equitable society, while emphasizing the importance of operating a PDCA cycle.

As for regulatory trends overseas, there is movement towards enacting legislation in Europe, but there is also opposition to regulation, which is creating a fluid situation.

Meanwhile, as a way to assess companies from an external perspective, the aforementioned World Benchmarking Alliance has proposed evaluating companies on criteria including whether they have publicly disclosed their own ethical AI principles and how those principles are being implemented.

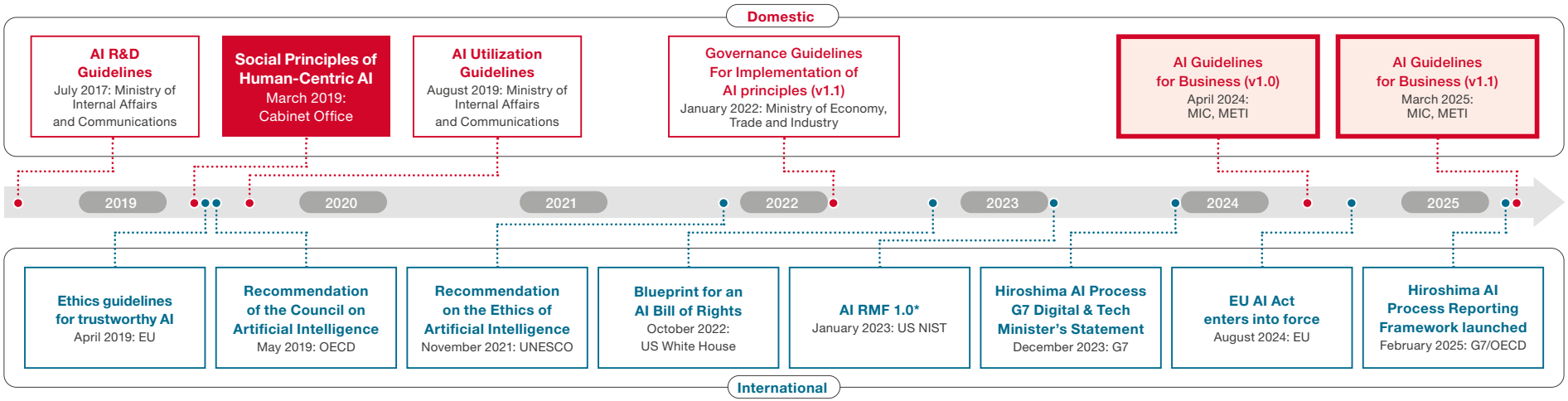
Specifically, this includes having an ethics committee whose existence and activities can be externally verified, as well as establishing AI guidelines.

Our approach is to leverage dialogue to encourage companies with identified issues to take appropriate actions. In conducting that dialogue, with regard to information security, we consider the three aforementioned elements to be key points, along with whether the scope of the company's efforts extends to overseas operations, group companies, and the supply chain. In some cases, companies also require their business partners to implement information security measures as a condition of doing business, which suggests that this may also have implications from a business perspective.

As for corporate disclosure, while some companies are lagging in their efforts, there are also good examples of companies providing comprehensive explanations on dedicated webpages or issuing annual reports focused specifically on information security.

Corporate initiatives related to AI ethics and governance are still at an early stage, but some companies—particularly in the information and communications sector—have drawn attention by providing detailed explanations on dedicated webpages. We will continue to encourage further efforts in this area.

Trends of Guidelines and Regulations Regarding the Use of AI



*AI Risk Management Framework 1.0

Source: Based on the overview of the *AI Guidelines for Business (Version 1.1)* issued by the Ministry of Internal Affairs and Communications and the Ministry of Economy, Trade and Industry

Example of Engagement **Japanese Equity**

Theme **Risk Management in the Digital Society**

Nomura Asset Management | **Japanese Electrical Equipment Company**

Background

In recent years, there has been growing concern about the impact of cyberattacks on corporate value. This company has been expanding its business by holding and utilizing vast amounts of data, including customers' personal information. Given this, we considered cybersecurity measures and related disclosure to be important and began engagement activities.

Engagement

When we checked the status of the company's cybersecurity measures, it reported that it had appointed responsible executives such as a Chief Digital Officer (CDO) and a Chief Information Security Officer (CISO), and had also designated responsible officers (EISOs) in each business division. However, explanations of these advanced initiatives are currently limited to the sustainability report, so we requested that disclosure be enhanced in future integrated reports and various meetings.

Company Response

We understand the importance of your comments. We will take the views you have provided into consideration in determining how we disseminate information going forward, including in our integrated report.

Results

"Cybersecurity Initiatives and Governance," which had previously been disclosed only in the sustainability report, began to be included in the integrated report starting in 2025.

Example of Engagement **Japanese Equity**

Theme **Risk Management in the Digital Society**

Nomura Asset Management | **Japanese Services Company**

Background

Given the high level of importance of data security for the company and its extensive M&A activity, we considered it necessary to strengthen group-wide information security initiatives and improve information disclosure, and therefore began our engagement activities.

Engagement

Given the high level of importance of data security for the company and its active M&A strategy, we asked the company to bolster its group-wide information security measures, and specifically the appointment of a responsible officer and more comprehensive disclosure. We also conveyed to the company that, because it is actively engaged in M&A and has many group subsidiaries, its information security framework should encompass the entire group.

Company Response

At present, the scope is limited to the company alone. However, since we recognize this as an important issue with respect to our business model, we want to address it promptly.

Results

In January 2025, the company set forth seven basic policies, one of which was the establishment of an Information Security Basic Policy. In addition, in October 2025 an investor report was prepared, and this report included information on information security.