NEWS RELEASE

Measures to Prevent Recurrence of System Disruption by a Cyberattack and Strengthening the Governance System

(Tokyo, Japan - February 18, 2026) – Asahi Group Holdings, Ltd. has been conducting an investigation into the sequence of events that led to the system disruption caused by the cyberattack on September 29, 2025, its root cause, and potential exposure of information. The following is a summary of the details and scope of the investigation completed as of February 18, 2026, and the measures to prevent recurrence, including strengthening our governance system.

1. Overview of the incident
   - At approximately 7:00 a.m. JST on September 29, 2025, a disruption occurred in our company system, and the subsequent investigation confirmed the presence of encrypted files.
   - That same day, at approximately 11:00 a.m. JST, we disconnected the network and implemented measures to isolate the data center to minimize the impact.
   - Subsequent investigations revealed that, although the specific date and time could not be determined, an external attacker had gained unauthorized access to the Asahi Group network through the network equipment located at our Group's site approximately ten days before the system disruption occurred.
   - It is believed that the attacker entered the Company's main data center, exploited a password vulnerability to gain administrative privileges, and then made unauthorized use of the accounts they had gained to search the internal network for information, repeatedly accessing and reconnoitering multiple servers, mainly after business hours.
   - On September 29, the ransomware was deployed across the affected systems, encrypting the data of several servers and some computer terminals that were running within the range of network connections.
   - During our efforts to investigate the extent and details of the impact, by focusing on the systems targeted in the attack we identified that some data from company-issued PCs provided to employees had been exposed.
   - There is a possibility that personal information stored on servers in the data center may have been exposed. However, we have not confirmed any instance of such personal information being published on the internet.
   - The impact of the attack on our systems is limited to those managed in Japan.

2. Impact and response to system disruption caused by the cyberattack

   ■ Impact on systems
   - Several servers and some company-issued PCs prior to the transition to a zero-trust model* were encrypted.
   - We have confirmed that some of the information stored on company-issued PCs prior to the

transition to the zero-trust model was stolen.

* A zero-trust model is a security model based on the principle of “trust nothing.” It requires strict authentication and authorization for all users, devices, and network connections, both internal and external, for each access to information assets.

■ Containment response (measures to prevent damage from spreading)

- All remote access VPNs[*1], the inter-site network (approximately 300 sites), and dedicated communication lines for inter-cloud[*2] connectivity, have been disconnected.
- In addition, as an emergency measure to stop the attack from spreading (infecting other systems), we disconnected the Internet and completely isolated the data center.

*1 Remote access VPN is a technology used to connect to a company network from outside the company via the Internet, enabling access to company systems and data from home or while away from the office.

*2 Cloud services provide external computer resources (servers and storage) for use via the Internet or other means.

■ Impact of our containment response on the system

- All data center systems were shut down, making access to our business systems impossible.
- To maintain the integrity of our backup data, our backup system was temporarily suspended.

■ Forensic investigation[*]

- A forensic investigation was conducted by external experts to verify the soundness of each system and to scrutinize the presence or absence of any breaches and the extent of any impact.

*A forensic investigation seeks to determine the causes and routes of unauthorized access, virus infections, etc. that occur in a computer or network.

3. Recovery from system disruption

■ Recovery efforts

- In cooperation with several external experts, we have established a secure recovery process.
- System recovery was performed using backup data that was confirmed to be safe.
- The soundness of all affected servers has been confirmed since rebuilding.
- Additional security measures were implemented as necessary based on the results of the forensic investigation.
- We are conducting a phased restoration, starting with systems that have been confirmed to be resilient.

■ Resumption of secure data transfer to/from external parties and integration with external systems

- Data integration with external systems has been resumed sequentially, starting with systems that have been confirmed to be resilient.
- File transfers via cloud storage with virus detection and removal functions have been resumed.
- Email routing has been rebuilt, and email sending and receiving have resumed after confirming system integrity.

4. Impact on business and recovery status

- Since the system disruption, systems related to order placement and product shipment—both of which are directly involved in supplying products to our customers—have been suspended, and these operations have been handled manually.

- Order placement and product shipment using logistics-related systems were resumed via the EOS (Electronic Ordering System) on December 3, 2025 for Asahi Breweries, Ltd. and Asahi Soft Drinks Co., Ltd., and on December 2, 2025 for Asahi Group Foods, Ltd.
  In addition, overall logistics operations have normalized as lead times for deliveries, which had remained limited, returned to normal by February 2026.
- We plan to gradually expand the number of items that can be shipped.

	Asahi Breweries, Ltd.	Asahi Soft Drinks Co., Ltd.	Asahi Group Foods, Ltd.
Cumulative revenue for October-December 2025 YoY	Low 80%	Around 70%	Around 90%
Number of items handled as of December 2025	107 items (composing 83% of revenue)	350 items (composing 95% of revenue)	944 items (composing 98% of revenue)

5. Exposure of personal information
   - On September 30, 2025, the day after the cyberattack occurred, we submitted a preliminary report to the Personal Information Protection Commission.
   - On October 8, we submitted a follow-up report to the Personal Information Protection Commission after confirming that the information suspected to have been exposed had been identified on the Internet.
   - On November 26, we reported the possibility of information exposure to the Personal Information Protection Commission as a final report.
   - On December 10, we submitted an additional report to the Personal Information Protection Commission confirming that further information suspected to have been exposed had been identified on the Internet.
   - Those whose information has been confirmed as exposed, as well as those who may be at risk, are being notified in due course.

■Personal information that may have been exposed (as of November 26, 2025)

Affected parties:	Description:	Count (approx.)
Those who contacted the Customer Service Centers of Asahi Breweries, Asahi Soft Drinks, or Asahi Group Foods	Name, gender, address, phone number, email address	1,525,000
External contacts to whom we have sent congratulatory or condolence telegrams	Name, address, phone number	114,000
Employees (including retirees)	Name, date of birth, gender, address, phone number, email address, other	107,000

Family members of employees (including retirees)	Name, date of birth, gender	168,000

(Note) 1. Credit card information is not included.
2. Not all of the information listed under 'Description' is included in each individual record.

■ Personal information that has been exposed (as of February 18, 2026)

Affected parties:	Description:	Count
Employees (including retirees)	Name, gender, address, phone number, email address, other	5,117
Directors and employees of business partners, as well as individual business partners and their employees, and others	Name, phone number, other	110,396

(Note) 1. The count for employees (including retirees) is included in the corresponding count under "Personal information that may have been exposed."
2. Not all of the information listed under 'Description' is included in each individual record.

6. Measures to prevent recurrence and strengthening of governance system

We prioritize the risk of cyberattacks as one of the most important management risks under our risk management system— The Asahi Group Enterprise Risk Management[*1]. We formulate, execute, and monitor plans to address this risk.

As part of these efforts, we have established the Cybersecurity Standards to be complied with across our Group, and we have been working to ensure their thorough implementation and operation. We have used these standards to assess our responses to cyberattacks across our Japanese and overseas group companies. We have also been working to maintain and improve our security systems and to improve security in order to prevent such risks from materializing. Moreover, under these standards, we have clearly stated the rules for reporting incidents when they arise, consolidated incident information across our Group, and worked to develop a system to strengthen our risk response.

In light of the recent cyberattack, we will further strengthen our efforts to date, shifting to a system based on continuous monitoring and improvements, and strengthen our system to minimize the impact in the event of an emergency.

Based on system operations that emphasize safety and reliability, we have been and will continue to work to prevent recurrence by responding to changes in the environment and changing threats. The main measures include thorough management of IT assets such as network equipment, servers, and PCs, updating and upgrading security tools including EDR (Endpoint Detection and Response) [*2], and ensuring that all employees are familiar with information management regulations. In addition, by strengthening our governance system, we will further elevate our information management and security management to an even higher level.

Specific initiatives are outlined below.

*1 Asahi Group Holdings has introduced enterprise risk management to ensure appropriate risk-taking in the execution of our Medium- to Long-Term Management Policy, while controlling the total amount of risk in order to reduce significant risks that could impede the achievement of our goals. We have also established the Asahi Group Risk Appetite to clarify which risks should be taken and which should be avoided.

*2 EDR is a system that constantly monitors endpoints (PCs, servers, etc.) for suspicious activities, and when signs of an attack are detected, automatically or quickly takes action to prevent the impact from spreading.

■ Identification of attack routes and prevention of recurrence

- Completely eliminated remote access VPN equipment to prevent re-entry using network devices
- Rebuilt communication routes to eliminate old communication routes that may allow unauthorized access
- Completely eliminated devices at risk of external unauthorized access, as revealed by the identification of attack routes
- Centralized data storage onto cloud storage to reduce the risk of data theft from PCs, and implemented measures to prevent cache residency when using data stored in the cloud

■ Redesigning PCs, network, and system configuration

- Fully transitioned to dedicated PCs (compatible with a zero-trust model) that support more resilient systems in order to prevent the spread of attacks to other PCs in the event of an attack
- Newly established a resilient network area to block unwanted communications and disconnect from external networks
- Have cut off or limited network connectivity on all systems to prevent the spread of attacks
- Enhanced EDR settings for all PC endpoints to detect and block suspicious activities
- Enhanced monitoring with EDR in cloud environments with Internet connectivity
- Performed penetration testing—where an independent third party attempts intrusion from the internet—to objectively confirm that appropriate security controls are in place against known threats
- Continue to perform penetration testing and threat hunting (proactive threat investigation) to maintain and further improve security posture

■ Increasing the sophistication of monitoring, detection, and initial response

- Reviewed security rules and operational systems in order to speed up initial response when anomalies are detected
- Automated log analysis systems and security monitoring and blocking in order to quickly detect and respond to cyberattacks and anomalies and minimize damage

■ Strengthening authority management and account security

- Implemented password changes and strengthen authentication and authorization management across all systems
- Automated account creation, modification, and deletion to prevent human error and omission in deletion

■ Strengthening security of infrastructure and cloud environments

- Further strengthen network connectivity restrictions and improve infrastructure configuration to prevent the spread of attacks
- Automated continuous checks on cloud security status and corrective actions

■ Enhanced recoverability and fault tolerance

- Further enhance backup mechanisms to achieve much faster system restoration
- Periodically review recovery procedures and implement drills in order to ensure rapid recovery
- Streamline system configuration by organizing and integrating systems and data

■ Continued strengthening of human countermeasures

- Strengthen security training for employees, and conduct training on an ongoing basis
- Continue to conduct practical security training to prepare for the latest attack methods

■ Strengthening the governance system

- Establish an independent organization and dedicated executive in charge of information security
- Establish an Information Security Committee to visualize information security risks and monitor the planning and implementation of countermeasures
- Revise and uphold the Asahi Group Information Management Policies and the Asahi Group Information Security Regulation, monitor to ensure thorough implementation, and strengthen auditing
- Review the skill matrix of the Board of Directors and strengthen monitoring and oversight of cybersecurity through collaboration among the Board of Directors, the Information Security Committee, the internal audit function, and external experts

- **Related Releases**

September 29, 2025 Notice of System Failure Due to Cyberattack
October 3, 2025 Update on System Disruption Due to Cyberattack (2nd)
October 8, 2025 Update on System Disruption Due to Cyberattack (3rd)
October 14, 2025 Update on System Disruption Due to Cyberattack (4th)
November 27, 2025 Investigation Results and Future Measures on Cyberattack Data Exposure

For further information, please contact:
Corporate Communications, Asahi Group Holdings, Ltd.
Email: media@asahigroup-holdings.com