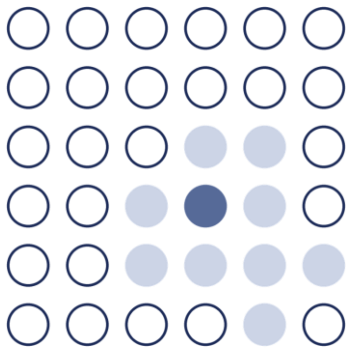




IRFRC Reports

What can we learn from cyber risk incidents to strengthen corporate resilience?

by Simon Ong Jia Jun, Sua Jia Ren Addison and Shinichi Kamiya

Insurance Risk and Finance Research Centre

Nanyang Business School, Nanyang Technological University

September 2026

JEL classification: G14; G22; G32; M14

Keywords: cyber risk; ransomware; operational resilience; event study; risk governance; cyber insurance; business continuity

Suggested citation: Ong, S. J. J., Sua, J. R. A., & Kamiya, S. (2026). What can we learn from cyber risk incidents to strengthen corporate resilience? IRFRC Reports No 202601. Insurance Risk and Finance Research Centre, Nanyang Business School, Nanyang Technological University.

Disclaimer: The views expressed in this report are those of the authors and do not necessarily reflect those of the Insurance Risk and Finance Research Centre (IRFRC) or Nanyang Technological University. This report is based solely on publicly available information and is provided for educational and informational purposes only; it does not constitute investment, legal or cybersecurity advice.

Data and sources: Market and financial data are drawn from S&P Capital IQ and Bloomberg; incident details from Asahi Group Holdings' public disclosures and news reporting; and peer comparisons from Kirin Holdings and Sapporo Holdings disclosures. Figures are correct as of the report date.

About the IRFRC: The Insurance Risk and Finance Research Centre at Nanyang Business School conducts research on insurance, risk management and finance. This publication is available at <https://www.ntu.edu.sg/irfrc>.

© Insurance Risk and Finance Research Centre, Nanyang Technological University 2026. All rights reserved. Brief excerpts may be reproduced or translated provided the source is stated.

Executive Summary

On 29 September 2025, Asahi Group Holdings ('Asahi') was hit by a major cyberattack that broke into its computer systems in Japan and East Asia. The attack took down core systems, badly disrupting production and deliveries and even delaying the company's financial reporting. Cleaning up and returning to normal took months—a sign of the serious and wide-reaching nature of the attack. Table 1 presents these key numbers at a glance.

Table 1: Summary of key numbers

Key Numbers at a Glance
Market capitalisation dropped by ~7% (~¥164 billion).
Revenue in Japan and East Asia dropped by 3.7% from Financial Year (FY) 2024 to FY2025.
Core operating profit in Japan and East Asia dropped by 16.1% from FY2024 to FY2025.
November 2025 monthly sales of Asahi's flagship product, Super Dry Beer, fell by 25% year-on-year (YoY) compared with November 2024.
More than 1.5 million pieces of personal information and records were exposed.
Release of financial results for FY2025 was delayed for more than six months. FY2025 results were eventually published on 8 July 2026.

To measure the financial hit, we tracked how Asahi's share price moved around the attack after stripping out normal market swings—what analysts call the 'abnormal return'. In the one-, two- and five-day windows around the announcement, Asahi's shares lagged on the market by 2.28%, 2.54% and 2.76%, respectively. These gaps are small, and statistically they cannot be separated from Asahi's normal day-to-day price movements; the wider windows look worse mainly because they add up to more trading days. In other words, the stock market did not react in a clearly measurable way.

The hit on day-to-day operations was far bigger. The attack forced Asahi to stop shipments, delay production and switch to manual processes just to keep running. The timing made it worse: the disruption ran straight into the November–December holiday season, the busiest time of year for beer in Japan. In Japan and East Asia, revenue fell by 3.7% and core operating profit fell by 16.1% from FY2024 to FY2025. November 2025 monthly sales of Asahi's flagship product, Asahi Super Dry, dropped sharply by 25% compared with November 2024—a major reason for the lower revenue and profit.

In short, the financial and operational pictures point in different directions. The share price barely moved, but the operational damage was deep and costly for Asahi. Over the following months, though, Asahi's performance did weaken—its returns and risk-adjusted returns were worse after the attack than before, even as its main rivals' shares rose—showing that a market reaction too small to be 'statistically significant' can still accompany a real loss of value: about ¥164 billion, roughly 7% of Asahi's market value.

The incident also shows why strong risk management and board oversight matter. Asahi's own risk management and governance did not prevent the attack: despite a framework on paper—group-wide security standards, subsidiary checks and incident-reporting procedures—attackers still broke in and halted operations, exposing gaps in access control, monitoring and detection, and internal-control design.

Asahi's response—establishing an Emergency Response Headquarters (ERH), leaning on its business-continuity plans and tightening security (for example, adopting a 'zero-trust' model that trusts no user or device by default)—shows how a company's governance shapes how well it

handles a crisis. Boards and executive teams also need members who genuinely understand cybersecurity, so they can oversee this risk properly and make better-informed decisions.

The Asahi case offers other companies five practical lessons. First, a calm stock price can hide serious operational damage, so firms should judge an attack on more than their share price reaction. Second, cyber risk is a company-wide business risk, not just an information technology (IT) problem. Third, risk frameworks only help if the controls and recovery plans behind them actually work when tested. Fourth, cyber insurance bears limitations, and firms cannot fully depend on it to recover all costs. Last, it is important that firms ensure that their leaders are equipped with cyber technical knowledge to remain resilient in managing cyber risk. Companies that build cyber risk into their everyday risk management are far better placed to limit the damage when an attack hits.

Contents

1. Introduction	7
1.1. September 2025 attack	7
1.2. Timeline of key events	7
2. Structure of the Attack.....	9
2.1. Overview of the incident.....	9
2.2. Initial access and entry point	9
2.3. Ransomware deployment and more than 1.5 million records exposed	9
3. Impact of the Attack.....	11
3.1. Financial impact	11
3.1.1. Stock price analysis in the short term.....	11
3.1.2. Trading volume analysis.....	12
3.1.3. Further analysis on financial impact in the longer term.....	12
3.1.4. Analyst forecast revisions.....	14
3.2. Operational Impact.....	15
3.2.1. Impact on revenue and business performance	15
3.2.2. Sales volume analysis	16
3.3. Key findings	17
4. Board and Corporate Governance.....	19
4.1. Board of Directors and Executive Committee	19
4.1.1. Board of Directors.....	19
4.1.2. Executive Committee	20
4.2. Board's response.....	21
4.2.1. Immediate response	21
4.2.2. Business continuity measures	21
4.2.3. Delay in disclosures.....	21
4.2.4. Further discussions regarding disclosure requirements in Japan	21
5. A Closer Consideration of Governance	23
5.1. Root causes.....	23
5.1.1. Access control.....	23
5.1.2. Monitoring and detection	23
5.1.3. Internal control design and containment.....	23
5.2. Risk management and internal control framework	23
5.2.1. Enterprise risk management and cybersecurity governance	24
5.2.2. Assessing the gaps against the National Institute of Standards and Technology (NIST) Cybersecurity Framework	24
5.2.3. Risk transfer and cyber insurance.....	24
5.2.4. Evolving risk disclosure.....	25
5.3. Post-incident reforms	26
6. Lessons to be Learned	27
6.1. Key takeaways from the cyberattack	27
6.1.1. Market reactions may understate the overall impact	27
6.1.2. Cyber risk is an enterprise-wide business risk, beyond just a standalone risk.....	27

6.1.3. Risk frameworks must work in practice.....	28
6.1.4. Cyber insurance has limitations	28
6.1.5. Recommendations for building cyber resilience.....	28
7. Conclusion	29
References	30
Appendix A: Timeline of events	33
Appendix B: Event study methodology	36
Appendix C: Hypothesis testing methodology	37
Appendix D: Trading volume.....	38
Appendix E: Annualised returns and standard deviation.....	39
Appendix F	41

1. Introduction

1.1. September 2025 attack

In September 2025, Asahi suffered a cyberattack that spread quickly from an IT problem into a company-wide crisis. What started as a break-in to Asahi's systems soon shut down logistics, halted shipments and disrupted order processing across its Japanese operations. Asahi is one of Japan's largest drinks makers, so the impact was visible to the public.¹ Systems that normally run quietly in the background failed all at once, showing how heavily modern business depends on digital infrastructure—and how fast a cyberattack can spill over into supply chains and everyday operations.

This report uses the Asahi attack to show how large companies are affected by—and respond to—a cyberattack. Instead of discussing cyber risk in the abstract, we will walk through how the incident unfolded and explore its financial and operational impacts, the role of management and the board and how Asahi handled the whole event. The timing and wording of Asahi's public statements also reveal the hard choices companies face in staying transparent although they are still piecing together what happened.

Overall, Asahi is a useful case because it shows so many sides of cyber risk at once. By tracing how the attack played out, we draw practical lessons on resilience, governance and crisis preparedness for large companies operating in an increasingly connected world.

1.2. Timeline of key events

The attack began quietly. Investigators later found that intruders had been inside Asahi's network for roughly 10 days before anything surfaced—an undetected 'dwell time' that ran from around 19 September 2025 (see Table 2 for the timeline and refer to Appendix A for more details).^{2–16} The crisis became public on 29 September 2025 when Asahi disclosed the cyberattack at 18:36 JST, suspended its order and shipping systems, confirmed the disruption and encrypted files, isolated its network and established an ERH to manage the response.

Recovery started within days but in stages. From 1 to 3 October, Asahi fell back on manual order processing and shipments, resumed production at six domestic factories on 2 October and issued a second update on 3 October that confirmed ransomware—the first point at which the Chief Executive Officer (CEO) spoke publicly. The following week brought both clarity and setbacks: the Qilin Ransomware Group claimed responsibility on 8 October, and soft drinks production fully recovered on 9 October, but on 14 October, Asahi announced it would postpone its Quarter 3 (Q3) financial results—the first sign the attack had spread from operations to financial reporting.

Through October and November 2025, the picture kept widening. Partial shipments of alcohol products resumed on 15 October, and on 26–27 November, Asahi disclosed its investigation findings, set a target of full logistics recovery by February 2026 and announced a further delay—this time to its full-year FY2025 results.

The final phase, from December 2025 to May 2026, concerned recovery, damage assessment and catching up on delayed reporting. After a quiet December 2025 to February 2026 recovery period, the CEO gave a performance-and-incident update on 26 February, and Asahi finally released its Q3 2025 results on 10 March, noted the postponement of its Q1 FY2026 results on 24 March and confirmed on 22 May that the delayed FY2025 results would be published on 8 July 2026—showing that the reporting disruption lingered for months after operations themselves had recovered.

Table 2: Summary of Events Related to Asahi's Cyberattack from September 2025 to May 2026

Period	Event
~19 Sep 2025	• Pre-announcement/pre-cyberattack period: Unauthorised access detected within ~10 days dwell time
29 Sep 2025	• Announcement day: First public disclosure of cyberattack at 18:36 JST and operations suspended • System disruption confirmed and encrypted files found • Network isolated and ERH activated
1 Oct 2025 – 3 Oct 2025	• Manual order processing and shipments began • 2 Oct: Production resumed at six domestic factories • 3 Oct: Second public update confirming ransomware with CEO making first public comments
8 Oct 2025 – 14 Oct 2025	• 8 Oct: Qilin Ransomware Group claimed responsibility • 9 Oct: Full recovery of soft drinks production • 14 Oct: Asahi's announcement that Q3 financial results were postponed
Oct 2025 – Nov 2025	• 15 Oct: Partial shipments of alcohol products resumed • 26–27 Nov: Investigation results disclosed; logistics recovery targeted for full recovery by Feb 2026: Announcement made to postpone FY2025 financial results
Dec 2025 – May 2026	• Dec 2025–Feb 2026: Recovery and impact assessment period • 26 Feb: CEO update on performance and cyberattack made • 10 Mar: Q3 FY2025 financial results announced • 24 Mar: Announcement that Q1 FY2026 results postponed • 22 May: Announcement that FY2025 financial results scheduled for public disclosure on 8 July 2026

2. Structure of the Attack

2.1. Overview of the incident

The incident was a ransomware attack that caused widespread disruption to Asahi's operations, hitting beer and soft drinks production in particular.¹⁷ It also crippled core processes such as order-taking and shipping¹⁸, forcing the group back to manual processes to keep going.¹⁹ In short, a single IT failure was enough to bring much of a huge company to a standstill—a stark example of how tightly today's operations are tied to digital systems.

2.2. Initial access and entry point

Asahi's investigation found that the attackers accessed the data centre network through a piece of network equipment.¹¹ This points to a weakness in Asahi's defences that let the attackers gain access and reach the systems that run its operations. Asahi did not release full technical details, but experts believe that stolen or weak login credentials and loose access controls gave the attackers the small opening they needed to work their way into large parts of the business.²⁰ The episode exposes a key weakness at the network's perimeter: once inside, the attackers could move sideways through Asahi's network and reach both operational systems and confidential data with little to stop them.

2.3. Ransomware deployment and more than 1.5 million records exposed

The attack ended with ransomware being planted across many of Asahi's servers, locking up files and critical systems and bringing operations to a halt.²¹ The scale and coordination suggest that the attackers had mapped Asahi's internal network in advance and timed the strike to produce the most damage.

The fallout was severe; reported data leaks affected both customers and employees. Table 3 lists the impact as reported on Asahi's website.² The Qilin Ransomware Group said that it had stolen 27GB of Asahi's data, and it later posted about 1,440 files and folders of that stolen information for anyone to download on the dark web.²² Ransomware groups often use stolen data to pressure victims into paying, but once the data are posted publicly, they tend to spread. In Asahi's case, the files were left open for download, so the exposed information could easily be copied and even resold on dark web markets.

The exposure also opens a distinct liability channel. Under Japan's Act on the Protection of Personal Information (APPI), a business that suffers a leak of personal data likely to harm individuals must report the breach to the Personal Information Protection Commission (PIPC) and notify those affected; failure to safeguard or notify can draw administrative orders and penalties. Beyond regulators, exposed customers and employees can seek damages, and Japanese courts have awarded compensation for leaked personal data in earlier breaches. For Asahi, more than 1.5 million records reportedly exposed are, therefore, not only a reputational risk but also a potential stream of notification costs, regulatory scrutiny and civil claims.

Table 3: Personal information that may have been exposed (as of 26 November 2025)

Affected Parties	Description	Approximate Count
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

Affected Parties	Description	Approximate Count
External contacts to whom Asahi had 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

Notes: 1) Credit card information is not included; 2) not all the information listed under 'Description' is included in each individual record.

3. Impact of the Attack

3.1. Financial impact

3.1.1. Stock price analysis in the short term

To measure the financial impact, we ran an ‘event study’—a standard method for checking how a company’s share price reacts to specific news. We treated 30 September 2025 as day zero (T_0 , the first trading day after the announcement). Asahi disclosed the attack at 18:36 JST on 29 September 2025, after the Tokyo market had closed, so the first chance for the price to react was the next day. We, therefore, used T_0 as the day the market could first respond.

To separate Asahi’s own share-price movements from general market ups and downs, we compared its stock with the Nikkei 225, Japan’s main market index. The difference is the ‘abnormal return’—the part of the move specific to Asahi. Appendix B explains the method in full.

Our main window was the day before to the day after the announcement ($[-1,1]$), which captured the immediate reaction. To check that the results held up, we also used wider windows of $[-2,2]$ and $[-5,5]$ days to catch any slower or delayed response. Table 4 shows the results.

In every window, the abnormal return was negative—a mild negative reaction. Asahi’s shares underperformed on the market by 2.28% in the $[-1,1]$ window, and by 2.54% in the $[-2,2]$ window as investors digested more news in the days after the announcement. The figure slipped further to 2.76% in the $[-5,5]$ window, which also captured the 3 October follow-up announcement that there had been a potential unauthorised transfer of data. However, a bigger negative number in a wider window does not necessarily mean investors turned sourer—a longer window simply adds up more trading days. As shown later, none of these figures are statistically significant. The bottom line is that the market’s reaction was small across every window.

To check whether this was specific to Asahi or just the industry, we ran the same test on its main rivals, Kirin Holdings (‘Kirin’) and Sapporo Holdings (‘Sapporo’). If investors thought Asahi’s troubles would send customers to competitors, we would expect Kirin and Sapporo shares to have risen. They did not: all three companies had negative abnormal returns in every window, so the reaction appears market- or industry-wide rather than unique to Asahi.

To test whether the whole market was down, we also looked at the Nikkei 225 itself over the same windows. The index was down by 2.47% in the $[-1,1]$ window and 2.95% in the $[-2,2]$ window, so part of the early drop simply tracked a weaker market. Over the $[-5,5]$ window, though, the index was up by 3.34%, whereas all three drinks makers stayed negative. That gap hints at some mild, industry-specific caution tied to the attack even as the broader market recovered.

Table 4: Cumulative Abnormal Returns (CAR) calculation for respective event windows and N225 index

Window	Asahi’s CAR	Kirin’s CAR	Sapporo’s CAR	Nikkei 225 Cumulative Return
$[-1,1]$	-2.28%	-2.77%	-4.32%	-2.47%
$[-2,2]$	-2.54%	-2.77%	-4.65%	-2.95%
$[-5,5]$	-2.76%	-2.65%	-1.91%	3.34%

Although Asahi, Kirin and Sapporo all had negative abnormal returns, none was statistically significant—even at the most generous (10%) threshold. Appendix C explains the test. Put simply, the price moves were too small, next to each stock’s normal volatility, to tell them apart from random noise.

3.1.2. Trading volume analysis

It also helps to consider the trading volume—how many shares changed hands—around the announcement, since a jump in volume would signal a burst of investor activity. We measured the trading volume over the same windows, comparing the volume on and around the event with the averages before and after it occurred.

Table 5: Change in average trading volume following the announcement

Change in Trading Volumes			
Window	Asahi	Kirin	Sapporo
[−1,1]	1.19%	29.28%	−12.46%
[−2,2]	−19.25%	18.33%	−16.43%
[−5,5]	−31.85%	−1.32%	−1.91%

Note: Values of the trading volume were extracted from S&P Capital IQ.

Table 5 compares the change in Asahi’s trading volume with Kirin and Sapporo, our stand-ins for the wider Japanese drinks sector. Asahi’s volume rose by just 1.19% in the [−1,1] window—a muted response—then fell by 19.25% and 31.85% in the wider [−2,2] and [−5,5] windows, respectively. The benchmarks were mixed, too; Kirin was up in the shorter windows and Sapporo down. Appendix D gives the full figures.

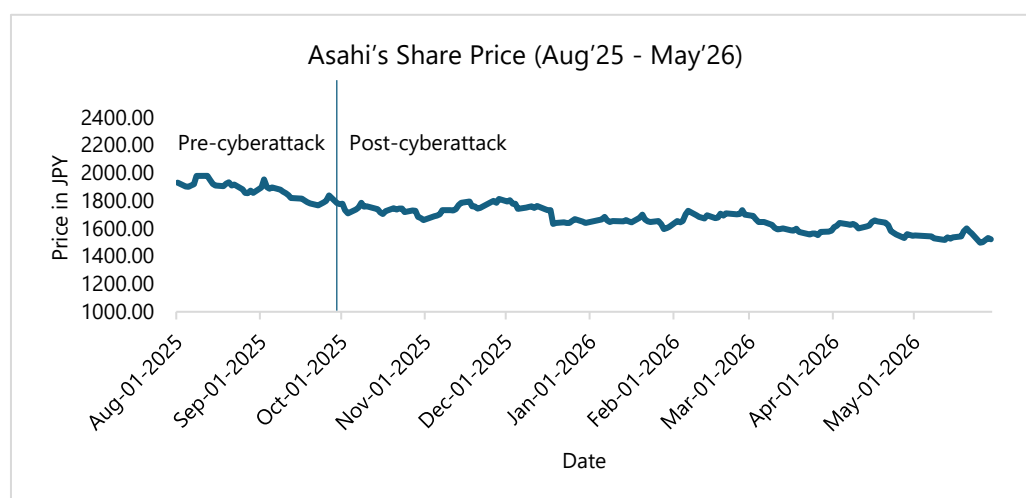
Hence, there is no clear sign of an Asahi-specific spike in trading. Its volume rose only slightly in the narrowest window before falling off, and its rivals moved in mixed directions.

The announcement seems to have drawn some immediate attention, but the effect was small and short-lived. With the volume showing no clear Asahi-specific spike, and with the negative abnormal returns too small to be statistically significant, the evidence points to a mild reaction and limited investor attention rather than a decisive negative verdict—the market signal was weak in both price and volume.

3.1.3. Further analysis on financial impact in the longer term

To move beyond the event study, Figure 1 plots Asahi’s share price from August 2025 to May 2026. This wider view—about 10 months—shows how the stock behaved before the attack, in the immediate aftermath and during the recovery, and sets the scene for the return, volatility and risk-adjusted figures discussed below. It also shows whether the price moves were short-lived or sustained.

Figure 1: Asahi's closing share price from August 2025 to May 2026



Here, we consider two measures: the Sharpe ratio (return earned for each unit of risk taken) and the average stock price. Appendix E sets out the method and presents calculations and more elaboration regarding annualised returns and standard deviation. To keep things simple over this short period, we treated the risk-free rate as effectively zero; given the short horizon and low interest rates, this makes no meaningful difference to the results, and the Sharpe ratio is still a useful gauge of return per unit of risk.

Table 6: Asahi's and rivals' pre- and post-event figures

Firm	Annualised Metric	Pre-event (30 Sep 2024 to 29 Sep 2025)	Post-event (1 Oct 2025 to 31 Mar 2026)
Asahi	Average Stock Price	¥1,826.74	¥1,689.59
	Sharpe Ratio	-0.15	-1.12
Kirin	Average Stock Price	¥2,087.45	¥2,395.12
	Sharpe Ratio	0.02	1.39
Sapporo	Average Stock Price	¥1,518.26	¥1,611.83
	Sharpe Ratio	-0.10	1.04

Table 6 sets Asahi's Sharpe ratio against that of Kirin and Sapporo. Asahi's fell sharply, from -0.15 to -1.12, whereas Kirin's rose from 0.02 to 1.39 and Sapporo's from -0.10 to 1.04. That contrast suggests that Asahi's weaker risk-adjusted performance over these six months was specific to the company, not a sector-wide slump. Looking before and after the attack this way helps show whether the damage lasted beyond the short event-study windows, especially as later disclosures kept shaping investor expectations. Overall, Asahi delivered weaker returns and worse risk-adjusted returns—investors judged its prospects more harshly, even though the stock did not become more volatile.

Table 6 also sets out the average stock price of Asahi, showing a decline from ¥1,826.74 before the cyberattack (30 September 2024 to 29 September 2025) to ¥1,689.59 after the cyberattack (1 October 2025 to 31 March 2026), a drop of about 7.5%. This decline reinforces the deterioration that we see in the Sharpe ratio and how the cyberattack affected Asahi's valuation. In contrast, the average stock prices of its rivals increased over the same horizon, highlighting that Asahi's weaker performance was likely firm-specific in the longer run.

This also reconciles the earlier event-study result. In the short window around the announcement, Asahi moved with its drinks sector peers, so the immediate reaction looked industry-wide rather than Asahi-specific. Over the following months, the paths diverged—Asahi’s risk-adjusted performance and share price fell and its rivals’ rose—a divergence consistent with the operational damage and with some customers switching to competing brands during the peak season (see Section 3.2). The short window share prices simply had not yet reflected these responses.

3.1.4. Analyst forecast revisions

We also checked whether outside analysts cut their forecasts for Asahi’s earnings after the attack, using estimate changes between 29 September and 30 November 2025. We chose the end of November as the cut-off because Asahi’s 26–27 November updates gave a much clearer picture of how bad the disruption would be and how long it would last—including the delay of its FY2025 results and a logistics recovery stretching into February 2026.

Because Asahi announced the attack after the Tokyo market closed on 29 September, we treated that day’s figures as ‘before’ the event. We used the closing consensus on 29 September as the starting point and the latest revision in our window, on 27 November 2025, as the end point.

Individual analysts moved in both directions—several cut their estimates in October and early November, and then some raised them again later—as they reassessed Asahi while the recovery played out. However, despite a few large individual changes, the overall consensus barely moved. Table 7 summarises the net change in the FY2026 consensus between 29 September and 27 November 2025.

Table 7: Changes in FY2026 analyst consensus estimates following the cyberattack

Metric	Estimate for 29 September 2025	Estimate for 27 November 2025	Change
Revenue (¥ billion)	3,030.60	3,020.93	–0.32%
EBIT (¥ billion)	301.28	300.64	–0.21%
Net income (GAAP) (¥ billion)	205.28	202.92	–1.15%
EPS (GAAP) (¥)	142.14	140.69	–1.03%

Note: The information is retrieved from S&P Capital IQ. Generally accepted accounting principles (GAAP) figures refer to reported earnings under Asahi’s applicable accounting standards, as classified by S&P Capital IQ, rather than normalised or adjusted earnings. EBIT, earnings before interest and taxes; EPS, earnings per share.

As Table 7 shows, the consensus fell by 0.32% for revenue, 0.21% for EBIT, 1.15% for net income and 1.03% for EPS. The slightly larger cuts to net income and EPS suggest that analysts were slightly more worried about Asahi’s bottom-line profit than its sales. Even so, all four changes are small—so although a few analysts cut hard, the group as a whole did not turn sharply negative.

Several things likely kept the consensus from fully reflecting the attack’s impact. First, the estimates are for full-year FY2026, so a disruption concentrated in late 2025 becomes diluted across a whole future year—and analysts appear to have treated the hit as a one-off that Asahi would largely recover from, not a lasting dent in its earning power. Second, the delayed catch-up in shipments (the October 2025 backlog that inflated sales) made the damage look smaller in the near-term numbers than its true size. Third, analysts were working with limited hard data: Asahi had postponed its financial results, so there were few concrete figures to plug into forecasts, and many contributors may have held off on revising until clearer numbers arrived—leaving stale

estimates anchoring the average. Finally, the damage was concentrated in Japan and East Asia and partly offset by steadier performance elsewhere, softening the effect at the group level that is described by these forecasts. In short, the muted consensus is less a sign that the attack was immaterial and more a reflection of the forecast horizon, incomplete information and an assumption of recovery—the same reasons, echoed in our share-price results, why outside indicators can understate the true operational severity of a cyber incident.

3.2. Operational Impact

3.2.1. Impact on revenue and business performance

The operational disruption fed straight through to Asahi's finances. Ironically, the attack also made the damage harder to measure, because it hit the very systems Asahi uses for financial reporting and delayed its disclosures. Table 8 shows the management reports for Asahi's operational regions.²³

Table 8: Summary of revenue and core operating profit impact in Asahi's operational regions

Region/Segment	Revenue Impact (FY24 to FY25)	Core Operating Profit (FY24 to FY25)
Japan & East Asia	–3.7%	–16.1%
Europe	+0.7%	+8.1%

Table 9: Summary of revenue and core operating profit impact for Asahi, Kirin and Sapporo²³⁻²⁵

Firm	Revenue Impact (FY24 to FY25)	Core Operating Profit (FY24 to FY25)
Asahi	–1.5%	–7.8%
Kirin	+4.1%	+19.3%
Sapporo	–1.1%	+48.8%

As Table 8 shows, the damage was concentrated in Japan and East Asia, which host Asahi's main production and logistics systems. Revenue and profit fell far more there than anywhere else, which points to the attack's shipment delays and lost production capacity dragging down profitability. Europe, by contrast, held up, reinforcing that the hit was largely a Japan and East Asia problem.

Looking group-wide, in Table 9, the like-for-like comparison uses core operating profit, which strips out one-off and non-core items and so better reflects each firm's underlying operations. On that basis, Asahi's core operating profit fell by 7.8% (on revenue down 1.5%) whereas Kirin's rose by 19.3% and Sapporo's 48.8%, so Asahi clearly underperformed against its rivals on the measure most closely tied to the attack. The flip side is that Asahi's loss reflects its rivals' gain. Kirin's revenue actually grew by 4.1% while Asahi's fell, and both rivals' core operating profits rose even as Asahi's dropped—the pattern expected when displaced demand flows to competitors. During the November–December peak, when Asahi Super Dry and other lines were in short supply, retailers and consumers appear to have switched to Kirin and Sapporo, handing them sales, shelf space and distribution that Asahi could not fulfil. The read is not clean—Sapporo's revenue was roughly flat (–1.1%), so its large profit jump owes more to its own margins and mix than to captured volume, and rivals' results move with their own costs and pricing too—but part of any switching could prove durable if some customers do not switch back, so a prolonged outage at

one firm can hand competitors a measurable, and potentially lasting, share gain. Hence, the disruption weighed on Asahi's overall results even as its rivals gained.

3.2.2. Sales volume analysis

The attack also shows up in sales volumes, especially for Asahi Super Dry, the company's flagship beer. Because it is one of Asahi's best-known and best-selling products, its sales are a useful gauge of how the attack hit production, logistics and distribution. We track sales as a percentage of the same month one year earlier: 100% means flat, above 100% is growth and below 100% is decline. Figure 2 shows this for Asahi Super Dry from May 2025 to March 2026.

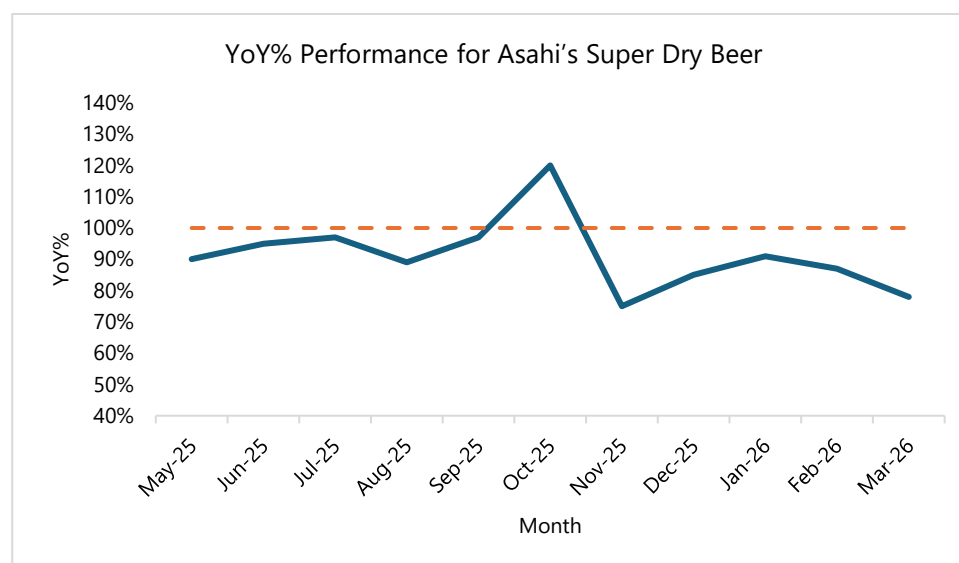
The immediate hit to sales was small. There is a slight dip, in line with a short disruption starting on 29 September, but because the attack struck with only a day or two left in the month, September sales stayed close to normal, at 97% of the prior year.¹⁰ The small dip fits the short window before month-end, though it may also be an early hint of something bigger—the halted order processing and shipments on 29 September.

October is where it becomes counter-intuitive: sales jumped to 120% of the prior year.¹⁰ That spike was artificial. Shipments that should have gone out in the last two days of September were held up and only processed once systems came back in early October, so they landed in October's numbers—a temporary 'catch-up' effect. Asahi's reliance on manual processing (see Section 4.2.2) added to the pile-up of delayed orders.

The real damage showed up in November, once the October catch-up had washed out: sales fell to 75% of the prior year.¹⁰ Asahi's supply chain was still struggling more than a month after the attack.²⁶ The timing hurt: November and December are the peak drinking season in Japan, when households and businesses hold year-end gatherings. With Asahi Super Dry and other products in short supply, retailers switched to rival brands to meet demand.²⁷ Asahi missed out on this seasonal surge, denting its profits for the quarter and likely the full year.

The drop in Super Dry sales matched the wider picture across Asahi's domestic businesses. Over October–December 2025, Asahi Breweries ran at roughly 80% of the prior year's sales, Asahi Soft Drinks at around 70% and Asahi Group Foods at around 90%. The attack clearly hit every business, just to different degrees, and Asahi Group Foods' milder drop likely reflects a supply chain and distribution setup less exposed than beer and soft drinks.¹⁰ Overall, the degree to which each business was hit came down to how much it depended on Japan's domestic production and logistics systems.

Figure 2: YoY% sales for Super Dry Beer



3.3. Key findings

Our analysis shows a clear split between the stock market reaction and the operational damage to Asahi. On the market side, Asahi's abnormal returns were negative across all three windows, but our statistical tests show that investors did not treat the attack as a real threat to Asahi's near-term value—and, as noted in Section 3.1.1, even that small dip was not all down to the attack.

The operational damage, by contrast, was severe. The attack halted production, delayed order processing and raised the risk of stolen data leaking, among other problems. Revenue in Japan and East Asia fell by 3.7% and core operating profit fell by 16.1% from FY2024 to FY2025 (Table 8). The pain dragged on for months, delaying Asahi's financial reporting, and pushed the company to speed up its digital and cybersecurity upgrades to close the gaps the attack exposed. All of this was immediate, costly and stretched well beyond the short windows in our share-price analysis.

One objection is worth confronting: a muted price reaction to a shock of this kind need not signal a market failure. Equity prices reflect the present value of a firm's long-run cash flows, so a disruption that proves largely recoverable within a quarter or two—as Asahi's ultimately was—may rationally warrant only a small move, denting current-year earnings far more than long-run earning power. On that reading, the market was forward-looking, not blind. Two things, though, keep this from fully explaining the gap. First, the damage was not purely transitory: Asahi's risk-adjusted performance and share price stayed weak for months and diverged from rivals that rose (see Section 3.1.3), a firm-specific deterioration that a clean transitory-shock story does not predict. Second, and more fundamentally, outsiders cannot easily observe operational fragility in real time—how close core systems came to prolonged failure, how weak the controls were, how far recovery leaned on manual workarounds—so a price can look calm precisely because the market cannot see what it would need to price. The muted reaction thus reflects information asymmetry as much as rational discounting, which is why it still understates the operational and governance risk the incident exposed.

Putting the two together, the message is clear: the attack caused no statistically significant market reaction yet did major operational damage, resulting in lasting consequences for governance and digital resilience. That reflects that a company's short-term share price can badly understate the severity of a cyberattack. To judge cyber risk properly, firms need to look beyond financial metrics—the stock price is an easy but incomplete gauge, and the market may simply

not have conceived the fragility of operations. Table 10 breaks down the incident's main cost channels and how far cyber insurance would reach across them.

Table 10: Anatomy of the loss—the incident's cost channels and how far cyber insurance reaches

Cost Channel	What Asahi Incurred	Rough Magnitude (from this Report)	Typically Insurable?
Response & restoration	Forensics, outside experts, system rebuild (zero-trust)	Not disclosed	Yes—breach-response & restoration cover
Business interruption	Halted production and shipments; fallback to manual processing	Japan & East Asia revenue –3.7%, core operating profit –16.1% (FY2024→FY2025); Super Dry –25% (Nov)	Partly—business insurance cover, but waiting periods and sub-limits apply
Lost market opportunity	Peak-season sales ceded to Kirin and Sapporo	Some share losses are likely permanent	No
Data-breach liability	~1.5–1.9M records exposed; notification and potential claims	Not yet quantified	Yes—liability & regulatory cover
Reporting disruption	Q3 and FY2025 results delayed into 2026	Multi-month delay	No
Market capitalisation & reputation	Share-price slide and reputational harm	≈¥164bn drop occurred over the week of the cyberattack; 7% lower average price after the attack ^{28,29}	No

4. Board and Corporate Governance

4.1. Board of Directors and Executive Committee

The financial and operational damage in Section 3 makes one thing clear: cyber risk is a core business risk that can threaten operations, financial reporting and stakeholder trust. Managing it well takes clear structures and strong oversight from the top. In big listed companies such as Asahi, the board is central—it sets how much risk the company will accept, makes sure controls are adequate and oversees the response when a crisis hits. Hence, we look next at how Asahi's board and executive team handle cyber risk, and how their peers compare.

4.1.1. Board of Directors

As of 30 April 2026, Asahi's board mixes executive and independent non-executive directors (Table 11),³⁰ a setup meant to balance inside knowledge with independent oversight. Table 11 summarises each director's background, drawn from S&P Capital IQ. For context, we also compare Asahi's board with that of its main domestic rival, Kirin Holdings, whose full board is presented in Appendix F; the comparison is explained following Table 11.

Table 11: Summary of Asahi's board members

Board Member	Position	Core Expertise	Cyber Risk Background?
Shigeo Ohyagi	Outside Director, Chairperson of the Board	Corporate governance, large-scale leadership, cross-industry oversight, prior Chief Information Officer (CIO) experience	Yes
Atsushi Katsuki	President and Group CEO	Global business management, strategy, finance, international expansion	No
Keizo Tanimura	Group Chief People Officer	Human capital strategy, senior corporate management	No
Kaoru Sakita	Group Chief Financial Officer	Financial governance, capital strategy, enterprise-wide finance leadership	No
Yukitaka Fukuda	Director	Corporate finance, internal controls, group financial management	No
Akiko Oshima	Director	Corporate strategy, financial risk management, compliance auditing	No
Kenichiro Sasae	Outside Director	Diplomacy, geopolitical strategy, global negotiations, security affairs	No
Tetsuji Ohashi	Outside Director	Manufacturing, production systems, business planning, industrial operations	No
Mari Matsunaga	Outside Director	Consumer business, digital entertainment, healthcare, innovation-driven governance	No
Sanae Tanaka	Outside Director	Corporate law, governance, compliance, audit	No
Chika Sato	Outside Director	Human resources (HR) leadership, talent strategy, organisational development	No
Melanie Brock	Outside Director	Japan–Australia relations, government advocacy, corporate governance	No
Akiko Miyakawa	Outside Director	International finance, public accounting, cross-border risk governance	No

Asahi's directors bring deep experience in governance, finance, risk management, compliance and general management, and the board did not change after the attack. In short, they are strong on traditional governance and enterprise risk—but light on cybersecurity and IT know-how. Of the

13 directors, only Shigeo Ohyagi has a clear IT background: he was CIO of Teijin Limited and has information-security experience. However, he held that role back in the early 2000s, when cyberattacks were far less common and CIOs mostly kept systems running rather than fending off attackers.³¹ Two decades on, IT and cybersecurity have changed beyond recognition, and after his stint as CIO, Ohyagi moved into general management roles at Teijin.

Kirin, by contrast, has Shingo Konomoto on its board—an independent director with about 30 years in IT consulting and far more current knowledge of digital systems and cyber risk. He is also a professor at Kyoto University’s Graduate School of Management, where he works on digital transformation and AI.³² That background suggests deep, up-to-date technical and governance knowledge of today’s cyber landscape.

This points to a likely gap in Asahi’s governance: no director with current and deep technical expertise appears to clearly own cybersecurity oversight. That matters, because cyber risk is different from ordinary business risk—challenging it properly takes a hands-on understanding of the threats, not just governance and risk management experience. Without that, Asahi’s otherwise strong board may find it hard to push back on management about technical issues or judge whether current controls are sufficient—which raises real questions about who is accountable for cyber oversight.

4.1.2. Executive Committee

Table 12: Summary of Asahi’s Executive Committee members³⁰

Name	Position
Atsushi Katsuki	President and Group CEO, Director and Representative Executive Officer
Keizo Tanimura	Group Chief People Officer, Director and Executive Officer
Kaoru Sakita	Group Chief Financial Officer, Director and Executive Officer
Naoko Nishinaka	Corporate Secretary, Executive Officer
Taemin Park	Group Chief Growth Officer, Executive Officer
Manabu Sami	Group Chief Research and Development (R&D) Officer, Executive Officer
Drahomira Mandikova	Group Chief Corporate Affairs Officer, Executive Officer
Naohiko Maeda	Group Chief Supply Chain Officer, Executive Officer

The committee in Table 12 is the holding company’s group-level executive team—its role is to set strategy for and oversee the operating subsidiaries (Asahi Breweries, Asahi Soft Drinks, Asahi Group Foods and the regional businesses), not to run any of them day-to-day.

Two things stand out. First, there is no Chief Risk Officer (CRO) or CIO on the committee. That matters, because how a company organises its top team usually signals its priorities and where it allocates resources. Asahi had flagged cyber risk as a key risk as far back as 2019 in its annual and integrated reports,³³ yet with no senior executive dedicated to this issue, cybersecurity seems to have been treated as an operational task pushed down into the subsidiaries rather than a strategic risk owned at the top. Group-wide rules, such as Asahi’s Group Cybersecurity Standards, are set at this level, but they are implemented at the subsidiary and factory levels—and without a clear owner and budget on the group committee, cyber risk depends on information climbing the group-function reporting lines to gain attention, of which it has likely received less than other parts of the business.

Second, the committee's composition itself is worth noting. It is made up entirely of group-function heads; the operating-company presidents who actually run the breweries, soft drinks and foods businesses do not sit on the committee. Kirin, by contrast, appears more deliberate on both counts. It has named Toshihito Hama its Chief Risk Management Officer and placed Mitsuharu Yamagata in charge of Digital and Information Strategy, and it seats its operating-company heads—such as the presidents of Kirin Brewery and Kirin Beverage—directly on its Executive Committee (Appendix F). That structure treats risk and IT as strategic priorities and keeps subsidiary leadership close to group-level oversight.

Without equivalent roles—and with subsidiary operations overseen only indirectly through group functions—Asahi likely had weaker visibility of cyber threats across its operating companies and a smaller ability to anticipate, watch for and respond to them, which likely left cyber risk under-prioritised and under-resourced relative to its severity—the organisational backdrop against which the technical failures of 29 September 2025 unfolded (see Section 5.1).

4.2. Board's response

4.2.1. Immediate response

As soon as it found the attack, Asahi's management set up an ERH on 29 September 2025 to investigate, and later confirmed its servers had been hit by ransomware.³ This is the classic centralised crisis-response model—run by senior management and overseen by the board in large companies.³⁴ Acting this fast shows that the leadership treated containment and data protection as top priorities, likely suspecting early on that data might have been stolen.

4.2.2. Business continuity measures

With its digital systems down and operations affected, management put business-continuity measures in place to keep things running.³ These included the following:

- Switching to manual order processing and shipments
- Gradually restoring call centre operations
- Prioritising product supply to customers despite system disruption

Having these fallback plans ready shows Asahi was prepared to keep operating by hand when systems failed. But leaning on manual processes also exposed its limits: the company could not keep up a normal output while systems were down.

4.2.3. Delay in disclosures

The timing and content of Asahi's announcements say a lot about how it handled the crisis. The attack hit on 29 September 2025, and Asahi went public the same day, then kept issuing updates on its recovery from October 2025 to May 2026—a sign that it took accountability to the public and customers seriously. Crucially, the attack also hit Asahi's accounting systems, cutting off access to financial data and delaying its reporting.⁸ As a result, on 14 October 2025, Asahi stated that it would push its Q3 2025 results past the usual 45-day deadline.⁸ A later update, on 27 November 2025, added that Asahi would also postpone its full-year 2025 results, showing the hit to financial reporting was worse than first expected.¹¹

4.2.4. Further discussions regarding disclosure requirements in Japan

Asahi's approach also highlights how Japan's and the US's disclosure rules differ. Companies on the Tokyo Stock Exchange must disclose material information promptly under the Timely Disclosure Rules and the Financial Instruments and Exchange Act.³⁵ But Japan sets no fixed deadline specifically for cybersecurity incidents. The US is stricter: since 2023, the Securities and Exchange Commission (SEC) has required firms to disclose a material cyber incident within four

business days of deciding it is material.³⁶ Asahi's step-by-step updates fit Japan's principles-based approach, where firms keep investors posted as information emerges rather than filing one full report within a tight deadline.

This contrast is a genuine trade-off, not simply a laxer regime. Deadline-driven disclosure (the SEC model) protects investors by releasing material news fast, but risks releasing figures that later prove wrong while an investigation is still open; principles-based, rolling disclosure (Japan's approach) lets a firm update as the facts firm up, at the cost of leaving investors with an incomplete picture for longer. Asahi sits at the heart of this tension: its drip feed of updates from September 2025 to May 2026 kept the market informed as the damage became clear, but the very gradualness may have muted the price reaction—each increment was small, so no single disclosure forced a sharp repricing even as the cumulative operational damage grew large. That is a subtle cost of rolling disclosure: it can smooth the market signal enough that the share price understates the true severity—echoing this report's central finding.

5. A Closer Consideration of Governance

5.1. Root causes

The Asahi attack exposed not just technical flaws but weaknesses in how the company governed and managed cyber risk. The break-in arose through unauthorised network access, but the root causes are best seen as three governance gaps: access control, monitoring and detection, and internal control design.

5.1.1. Access control

As Section 2 described, the attackers exploited weak spots to access Asahi's systems, which suggests there were real gaps in its controls for verifying and limiting who could access what information. Breaking in through the virtual private network (VPN) and other network equipment points to loose password and credential management. More fundamentally, it suggests that access control was treated as a technical setting rather than a governance priority. Good governance keeps a constant eye on these entry points—monitoring, testing and reviewing them—because they are the doors to the whole system. The attack suggests that such discipline was missing.

5.1.2. Monitoring and detection

Asahi could not detect or stop the attackers while the intrusion was underway. Its investigation found that the attackers had remained inside the network—after gaining access through equipment at a company site—for approximately 10 days before the systems went down.² However, it remains unclear whether Asahi's security tools failed to flag the suspicious activity or whether they generated warnings that were not properly reviewed, escalated or addressed.

Had the intrusion been detected and acted upon promptly, the attack might have been contained before it caused widespread disruption. The incident, therefore, indicates a weakness in either technical detection or the governance processes surrounding the review and escalation of security alerts. Effective cyber governance requires appropriate alert thresholds, clear escalation procedures and management accountability for responding to unusual activity. Regardless of whether the failure lay in the monitoring tools or the handling of their warnings, 10 days of uninterrupted attacker activity suggests that cyber risk was not sufficiently integrated into Asahi's monitoring and oversight framework.

5.1.3. Internal control design and containment

A third issue was internal control design. The speed and reach of the attack show that the network was not built to contain a breach. Investigators found that, once inside, the attackers deployed ransomware across many active servers and some personal computers (PCs) at the same time.¹¹ So, the controls in place could not slow the attack down. A well-designed network is split into segments, which boxes in an attack and limits the damage.³⁷ The fact that the attackers reached so many connected systems suggests that this segmentation was weak or not enforced. This indicates a broader governance problem: controls existed but were never stress-tested against a worst-case attack. Good governance keeps testing those controls to ensure they can actually contain a breach.

5.2. Risk management and internal control framework

Having pinpointed the gaps in access, monitoring, detection and containment, we now step back to Asahi's wider risk management and internal control framework.

5.2.1. Enterprise risk management and cybersecurity governance

Asahi had a risk management framework in place before the attack, and it listed cyber risk as one of the group's key risks. The company said it had rolled out group-wide cybersecurity standards, run security checks across its subsidiaries and set up procedures for reporting incidents.² Thus, the real question is not whether Asahi had cyber governance on paper but whether that governance actually worked.

The scale of the attack points to a big gap between naming cyber risk on paper and managing it effectively in practice. Asahi had the frameworks, yet attackers still broke in and halted operations—a sign that risk management was not translating into real resilience, and that cyber risk may not have been fully wired into day-to-day decisions and planning. Effective risk management is not just about listing risks; it means constantly checking that controls still hold up. It also leans heavily on formal reporting lines, where information about a risk climbs step by step up to the board and executives.³⁸ On paper, that is a tidy chain of command. However, in a fast-moving cyberattack, it can become a bottleneck—attacks can escalate within hours, and slow, layered reporting can rob a company of the speed it needs to act.

5.2.2. Assessing the gaps against the National Institute of Standards and Technology (NIST) Cybersecurity Framework

These gaps can also be read through a cyber-specific lens. The NIST Cybersecurity Framework³⁹ organises cyber risk management into six functions—Govern, Identify, Protect, Detect, Respond and Recover. Asahi's failures cluster in Identify (it had named cyber risk as a key risk but had not fully weighed how a large-scale attack could ripple through operations, logistics and distribution), Detect (an intrusion went unnoticed for roughly 10 days, because alerts were either absent or not escalated), Protect (weak access control and limited network segmentation) and Govern (no board-level owner of cyber risk and no CRO or Chief Information Security Officer [CISO], as Section 4 shows). Its response was comparatively strong on Respond and Recover—the ERH, staged restoration and zero-trust rebuild. Japan's own Ministry of Economy, Trade and Industry/Information-technology Promotion Agency Cybersecurity Management Guidelines make the same point at the top: they treat cybersecurity as a management responsibility with a clearly named owner, which is precisely the accountability that Asahi lacked.

5.2.3. Risk transfer and cyber insurance

Asahi has not publicly said whether it carried company-wide cyber insurance. Its disclosures focus on recovery, the investigation and fixing its systems and governance, not on insurance. Thus, from public information alone, we cannot tell whether any of the losses were covered by insurers.

Still, the attack shows why cyber insurance belongs in a broader risk management strategy. Even though Asahi did not disclose its coverage, the policies sold by major Japanese insurers show the kinds of losses for which such cover is designed. For example, products from insurers such as Tokio Marine⁴⁰ typically cover the following:

- TM Cyber 365: Designed to help an organisation pay for any financial losses they may incur in the event of a cyberattack or data breach. Coverage for cyber insurance includes these key costs:
 - o Liability settlement and defence costs
 - o Regulatory defence and penalties
 - o Breach response costs, such as legal costs to comply with privacy regulations, credit monitoring, public relations and notification costs where legally required
 - o Cyber extortion expenses and extortion monies
 - o Restoration costs of damaged digital assets
 - o Income loss and interruption expenses

These match closely with Asahi's experience: operational disruption, hiring outside cyber experts, restoring systems and exposing customer and employee data. However, cyber insurance has limits. Business-interruption cover might offset some costs, but it cannot bring back the seasonal sales Asahi lost while it could not operate. The beer it could not sell during the November–December peak represents revenue that was simply gone, and which could not be replaced by insurance. Insurance also cannot easily undo intangible damage, such as a hit to the reputation—money alone will not fix that problem.

Even where cover applies, cyber business-interruption insurance is narrower than the headline loss. It is usually triggered by a security failure rather than physical damage but pays only after a waiting period and up to sub-limits set well below the overall policy limit, and it indemnifies lost profit during the outage—not the market share and shelf space that a rival captures and may keep (Section 3.2). For a seasonal, brand-driven business struck at peak demand, that ceded share is the loss that matters most and is the least insurable. Liability and regulatory cover are also uneven: breach-response and defence costs are typically insurable, but regulatory penalties often are not, so Asahi's APPI exposure (Section 2.3) would be only partly transferable.

Firms also rarely spell out their cyber cover, treating it as confidential: revealing details such as limits and deductibles could show rivals where a company is underinsured. In principle, firms should disclose more. However, in practice, doing so risks handing competitors useful information.⁴¹

There is also a feedback loop that ties insurance back to governance. As cyber losses have mounted, insurers have tightened underwriting: cover increasingly requires the very controls Asahi lacked—multi-factor authentication, network segmentation, endpoint detection and a named security owner—and insurers price up or decline coverage for firms that cannot demonstrate these controls. Insurance is thus becoming a private standard-setter, pushing firms toward the controls that good governance demands anyway.

Hence, cyber insurance is no substitute for solid governance and controls. It can absorb some of the financial blow, but it cannot undo the operational disruption caused by an attack. It is best seen as one complementary tool—a way to transfer some risk—within a wider risk management strategy.

5.2.4. Evolving risk disclosure

Another part of managing cyber risk is how openly firms flag it in their official filings. Under the Financial Instruments and Exchange Act, listed Japanese firms must include a business-risk section in their Annual Securities Report (the Yukashoken Hokokusho, Japan's version of the US 10-K) to tell investors about the main risks to their business, governance and finances.

Kirin's Annual Securities Reports for 2024 and 2025 show a clear shift in how it frames cyber risk. In its 2024 filing⁴², cyberattacks sat mainly under information security—treated narrowly as an IT problem. By 2025, Kirin had widened this inclusion, spelling out how a cyberattack could hit its supply chain, not just its IT.⁴³ This likely reflects what happened to Asahi: Kirin acknowledged that cyber threats could disrupt procurement, logistics and broader operations. The change shows a growing recognition that cyber risk is not confined to IT but can cascade through the business in very real ways.

Asahi's own 2025 Annual Securities Report was filed on 27 July 2026, after the cyberattack forced it to extend the statutory deadline—and it went further than a broadened risk factor. Management disclosed that Asahi's internal control over financial reporting was not effective as of 31 December 2025, citing a material weakness caused by the cyberattack: the ransomware incident cut off access to accounting data and exposed gaps in how the group's information-system and security-management rules had been implemented in parts of its Japan operations.⁴⁴

Asahi paired the admission with remediation—an Information Security Committee to surface and monitor security risks, and tighter access-privilege, administrative-rights, password and monitoring controls. This is an unusually candid confirmation of the very access-control and internal-control gaps this report diagnoses: a group that had listed cyber risk on paper was compelled, after the attack, to admit those controls had not worked. It also marks the shift we anticipated—from treating cyberattacks narrowly as an information-security matter toward recognising them as a material, whole-business risk, echoing Kirin’s earlier move.

Two features of risk-factor disclosure limit how much investors can actually learn from this disclosure, however. First, it tends toward the boilerplate: flagging cyberattacks as a risk is easy and near-universal, but only specific, entity-relevant disclosure—of the kind Kirin adopted in 2025, spelling out the supply-chain cascade—genuinely informs a valuation, and firms face real disincentives to that specificity, since detailing where they are exposed can tip off attackers, invite litigation if a later breach suggests the risk was already known and unsettle investors. Second, because these sections are refreshed only once a year, they lag events: Asahi’s updated framing arrived only with its next Annual Securities Report, long after the attack, so the most informative version came precisely when it was least useful as an early warning. Cross-firm learning is thus reactive—Kirin broadened its disclosure after watching Asahi, not before—reinforcing this report’s wider theme that external indicators trail, and understate, the operational reality.

5.3. Post-incident reforms

After the attack, Asahi rolled out a series of measures to shore up its cybersecurity and prevent a repeat. According to its February 2026 investigation report, these included tighter monitoring and network-security controls and a rebuild of its IT setup toward a ‘zero-trust’ model. In practice, that meant disconnecting about 300 inter-site network and internet links, isolating data centres, and requiring identity checks for every user and device.²

Beyond the technical fixes, Asahi tightened its group cybersecurity standards, improved how it collects and reports incidents across the group and strengthened its overall response system. The response clearly went beyond just fixing systems.² It signals a shift toward continuous oversight and more disciplined risk management, addressing the loose governance that had left it exposed. As noted in Section 4, Asahi kept its board and executive team unchanged, choosing to overhaul systems and processes rather than people.

Asahi also stressed training, making sure staff know how to react in a cyber incident. The aim is to keep employees up to date on the latest attack methods so everyone can respond more confidently next time.

Asahi has not put a number on what all this cost. It has described the governance improvements in its updates but has not disclosed any specific spending figure.

Taken together, these steps show Asahi moving toward more structured, proactive management of cyber risk after seeing the scale of potential damage from an attack—shifting from firefighting the crisis to longer-term reforms that treat cyber risk as a major business risk.

6. Lessons to be Learned

6.1. Key takeaways from the cyberattack

The Asahi attack offers wider lessons on resilience: a months-long hit to production, logistics, order processing and financial reporting drew only a mild, statistically insignificant market reaction—the gap that frames the takeaways below.

6.1.1. Market reactions may understate the overall impact

Asahi's shares underperformed on the market after the attack, but not by a statistically significant margin, and the trading volume showed no clear, lasting spike.

The operational damage, though, was clear. The attack hit production, shipments and financial reporting for months and likely dragged down results in Japan and East Asia. A quiet market reaction, in other words, does not mean an attack is harmless. Cyberattacks should be judged on more than financial metrics—including operational measures such as lost sales, reporting delays and recovery costs. The victim's loss is not the whole story: Asahi's missing sales partly resurfaced as rivals' gains (Section 3.2), so a cyberattack can redistribute market share, not just destroy value.

Asahi's experience is not unique. Comparable cyberattacks on consumer-facing and logistics firms (Table 13) show the same signature—deep, months-long operational disruption whose cost dwarfs the initial headline—even where, as with Asahi, the immediate market reaction was modest.

Table 13: Asahi in context—comparable operational cyberattacks on consumer-facing and logistics firms

Incident	Year	Sector	Operational Disruption	Reported Financial Impact
Asahi (this report)	2025	Beverages	Production and shipping halted for months; manual processing; financial reporting delayed	Japan & East Asia revenue –3.7%, core operating profit –16.1%; Super Dry –25% (Nov)
Marks & Spencer	2025	Retail	Online orders suspended ~7 weeks; click-and-collect down ~15 weeks	H1 pre-tax profit –55%; ≈£300m FY operating-profit hit (partly insured)
Clorox	2023	Consumer goods	Product shortages; manual order processing for months	Q1 net sales –20% (≈\$356m); ≈\$49m direct response costs
Maersk (NotPetya)	2017	Shipping & logistics	76 port terminals halted; ~10 days to rebuild; 4,000 servers / 45,000 PCs replaced	≈\$200–300m loss

6.1.2. Cyber risk is an enterprise-wide business risk, beyond just a standalone risk

The attack began in Asahi's IT systems but quickly spread to production, logistics, customer service and financial reporting—proof that cyber risk is not just an IT problem. One digital failure can knock out several parts of a business at once and grow into a full operational and governance crisis. Cyber risk, therefore, needs to sit inside company-wide risk management, subject to clear oversight from the board and senior leaders. Directors are not expected to run the technology themselves, but they should grasp the business consequences of cyber threats and be able to ask whether the controls and resources in place are enough. Firms also gain from stronger in-house cyber expertise and a clear owner for cyber risk at the top.

6.1.3. Risk frameworks must work in practice

Asahi had already flagged cyber risk as a key risk and set up cybersecurity standards and reporting procedures before the attack. Yet the intruders reportedly sat in its network for about 10 days and reached several connected systems—a clear gap between naming the risk and being ready for its arrival.

Thus, risk frameworks have to be backed by controls that actually work: strong access controls, real monitoring and ways to contain a breach. Business-continuity plans should be stress-tested regularly to check that critical operations can keep going through a long outage. Asahi's post-attack reforms—better monitoring and a move to zero trust—tackle some of these gaps but they will only pay off if the company keeps implementing and testing them, rather than just having the policies on paper.

6.1.4. Cyber insurance has limitations

Because the disruption struck during peak demand, Asahi's cyberattack cost the business sales that insurance cannot restore: the beer it could not ship during the November–December peak represents revenue that was simply lost. Reputational harm and other intangibles are likewise hard to compensate with money. Cyber insurance may cover system restoration and liability, but it cannot recover lost market opportunity or undo operational disruption—firms should treat it as one complementary tool within cyber risk management, not a panacea.

6.1.5. Recommendations for building cyber resilience

Drawing the report's threads together, we distil a set of concrete, non-exhaustive practices that firms can adopt to manage cyber risk as an enterprise-wide business risk, grouped by where the action sits:

1. **Board and leadership:** seat a director with current cybersecurity expertise, create a CRO or CISO role and give a board-level risk or technology committee a standing cyber mandate.
2. **Controls and resilience:** enforce multi-factor authentication, network segmentation and endpoint monitoring; move toward a zero-trust architecture; and stress-test the business-continuity plan against a prolonged outage, not just a brief one.
3. **Disclosure and assurance:** benchmark breach-disclosure timelines against external standards (such as the US SEC four-day rule), and write specific, entity-relevant cyber risk factors rather than using a boilerplate.
4. **Risk transfer:** treat cyber insurance as one layer within the strategy, align controls to what insurers now require and map cover against the actual loss channels—recognising that lost sales and ceded market share are largely uninsurable.

Having these practices in place allows cyber risk to be managed properly and ensures that firms are more resilient to cyberattacks.

7. Conclusion

Overall, Asahi's cyberattack incident shows that resilience is not just about preventing attacks but about how well a company detects, contains, recovers from and learns from them. The mild market reaction badly understated the operational damage, and the way the attack spread across production, logistics and financial reporting shows that cyber risk is a whole-business issue, not just a technical one. It also shows that policies and frameworks are worthless unless backed by real controls, clear oversight and hard stress-testing against worst-case scenarios. Moreover, cyber insurance can only do so much in supporting firms' cyber risk management practices. To improve resilience, firms can also adopt some best practices to ensure the leaders overseeing the firm have some degree of technical expertise. This case also shows that cyber risk is partly a competitive, market structure risk: an attack can hand rivals sales and shelf space that some may keep, giving competitors, insurers and regulators their own stake in any one firm's resilience.

Our study covers a single company using public information, but the lesson travels: real cyber resilience requires pairing technical safeguards with practical preparedness and company-wide governance.

References

- ¹ Notice of System Failure Due to Cyberattack | Newsroom | ASAHI GROUP HOLDINGS. (2025, September 29). Asahi Group Holdings, Ltd. <https://www.asahigroup-holdings.com/en/newsroom/detail/20250929-0202.html>
- ² Measures to Prevent Recurrence of System Disruption by a Cyberattack and Strengthening the Governance System | Newsroom | ASAHI GROUP HOLDINGS. (2026, February 18). Asahi Group Holdings, Ltd. <https://www.asahigroup-holdings.com/en/newsroom/detail/20260218-0201.html>
- ³ Update on System Disruption Due to Cyberattack (2nd) | Newsroom | ASAHI GROUP HOLDINGS. (2025, October 3). Asahi Group Holdings, Ltd. <https://www.asahigroup-holdings.com/en/newsroom/detail/20251003-0204.html>
- ⁴ Asahi Group's Production Halted by Cyber Attack | The Straits Times. (2025, September 30). The Straits Times. <https://www.straitstimes.com/asia/east-asia/japans-beer-giant-asahi-group-cannot-resume-production-after-cyberattack>
- ⁵ Japan's Asahi Restarts Beer Production Following Cyberattack | Reuters Staff. (2025, October 6). Reuters. <https://www.reuters.com/world/asia-pacific/japans-asahi-restarts-beer-production-following-cyberattack-2025-10-06/>
- ⁶ Cybercriminals Claim Hack on Japan's Asahi Group | Vicens, A. J. (2025, October 7). Reuters. <https://www.reuters.com/world/asia-pacific/cybercriminals-claim-hack-japans-asahi-group-2025-10-07/>
- ⁷ Update on System Disruption Due to Cyberattack (3rd) | Newsroom | ASAHI GROUP HOLDINGS. (2025, October 8). Asahi Group Holdings, Ltd. <https://www.asahigroup-holdings.com/en/newsroom/detail/20251008-0201.html>
- ⁸ Update on System Disruption Due to Cyberattack (4th) | Newsroom | ASAHI GROUP HOLDINGS. (2025, October 14). Asahi Group Holdings, Ltd. <https://www.asahigroup-holdings.com/en/newsroom/detail/20251014-0203.html>
- ⁹ Notice Regarding Postponement of Disclosure of Financial Results for the Third Quarter of the Fiscal Year Ending December 31, 2025 Due to System Disruption Caused by Cyberattack | Newsroom | ASAHI GROUP HOLDINGS. (2025, October 14). Asahi Group Holdings, Ltd. <https://www.asahigroup-holdings.com/en/newsroom/detail/20251014-0102.html>
- ¹⁰ Monthly Sales Reports | Financial Information | Investors | ASAHI GROUP HOLDINGS. (n.d.). Asahi Group Holdings, Ltd. https://www.asahigroup-holdings.com/en/ir/financial_data/monthly_data/
- ¹¹ Investigation Results and Future Measures on Cyberattack Data Exposure | Newsroom | ASAHI GROUP HOLDINGS. (2025, November 27). Asahi Group Holdings, Ltd. <https://www.asahigroup-holdings.com/en/newsroom/detail/20251127-0204.html>
- ¹² Notice Regarding Postponement of Disclosure of Financial Results for the Fiscal Year Ending December 31, 2025 | Newsroom | ASAHI GROUP HOLDINGS. (2025, November 27). Asahi Group Holdings, Ltd. <https://www.asahigroup-holdings.com/en/newsroom/detail/20251127-0201.html>
- ¹³ Fiscal 2025 Business Update Conference | ASAHI GROUP HOLDINGS. (2026, February 26). Asahi Group Holdings, Ltd. https://www.asahigroup-holdings.com/ir_library_file/file/2025_4q_update_presentation_en.pdf
- ¹⁴ Asahi Group Holdings Q3 2025 Financial Results | Newsroom | ASAHI GROUP HOLDINGS. (2026, March 10). Asahi Group Holdings, Ltd. <https://www.asahigroup-holdings.com/en/newsroom/detail/20260310-0202.html>
- ¹⁵ Notice Regarding Postponement of Disclosure of Financial Results for the First Quarter of the Fiscal Year Ending December 31, 2026 | Newsroom | ASAHI GROUP HOLDINGS. (2026, March 24). Asahi Group Holdings, Ltd. <https://www.asahigroup-holdings.com/en/newsroom/detail/20260324-0204.html>
- ¹⁶ Notice Regarding the Announcement Date of Financial Results for the Fiscal Year Ended December 31, 2025 | Newsroom | ASAHI GROUP HOLDINGS. (2026, May 22). Asahi Group Holdings, Ltd. <https://www.asahigroup-holdings.com/en/newsroom/detail/20260522-0203.html>
- ¹⁷ Asahi Says More Than 1.5 Million Customers' Data Potentially Leaked in Cyber-attack | Chia, O. (2025, November 27). BBC News. <https://www.bbc.com/news/articles/ce86n44178no>
- ¹⁸ Super Dry Maker Asahi Aims to Restore Logistics by February Following Cyberattack | The Business Times. (2025, November 27). The Business Times. <https://www.businesstimes.com.sg/companies-markets/consumer-healthcare/super-dry-maker-asahi-aims-restore-logistics-february-following-cyberattack>
- ¹⁹ Japan's Asahi Ships Beer Manually After Ransomware Attack | The Straits Times. (2025, October 4). The Straits Times. <https://www.straitstimes.com/asia/east-asia/japans-asahi-ships-beer-manually-after-ransomware-attack>

- ²⁰ Decoding the Asahi Brewery Ransomware Attack | Shieldworkz. (2026). Shieldworkz. <https://shieldworkz.com/reports/decoding-the-asahi-brewery-ransomware-attack>
- ²¹ Asahi Weighs Dedicated Cybersecurity Unit after Ransomware Disruption | Easton, J. (2025, December 15). National Technology News. https://nationaltechnology.co.uk/Asahi_Weighs_Dedicated_Cybersecurity_Unit.php
- ²² Hacker Group leaks Suspected Asahi Group Data on Dark Web | Nippon TV News 24 Japan. (2025, December 11). Nippon TV NEWS 24 JAPAN. <https://www.ntv.co.jp/englishnews/articles/2021mdhfmYOU5r039lIf.html>
- ²³ Financial Highlights | ASAHI GROUP HOLDINGS. (2014). Asahi Group Holdings. https://www.asahigroup-holdings.com/en/ir/financial_data/highlights.html
- ²⁴ Management Analysis of Financial Position, Operating Results, and Cash Flows | Financial Data | Kirin Holdings. (n.d.). Kirin Holdings Company, Limited. Retrieved 16 August 2026 from <https://www.kirinholdings.com/en/investors/finance/analysis/>
- ²⁵ Financial Highlights | Sapporo Breweries. (2026). Sapporo Breweries. <https://www.sapporobreweries.com/en/ir/financial/highlight/>
- ²⁶ A Month after Asahi Cyberattack, Japan's Beverage Industry Still High and Dry | The Japan Times. (2025, October 29). The Japan Times. <https://www.japantimes.co.jp/business/2025/10/29/companies/asahi-beer-cyberattack/>
- ²⁷ Cyberattack Leaves Asahi Struggling as Rival Brewers Gain Ground | The Business Times. (2025, November 11). The Business Times. <https://www.businesstimes.com.sg/international/global/cyberattack-leaves-asahi-struggling-rival-brewers-gain-ground>
- ²⁸ Japan Faces Beer Crunch After Cyberattack Hobbles Asahi's Output | Matsuyama, K., & Yoshida, K. (2025, October 3). Bloomberg. <https://www.bloomberg.com/news/articles/2025-10-03/7-eleven-running-out-of-super-dry-beer-after-asahi-cyberattack>
- ²⁹ Asahi Blames Ransomware for Crippling Japanese Beer Plants | Yoshida, K. (2025, October 3). The Japan Times. <https://www.japantimes.co.jp/business/2025/10/03/companies/seven-eleven-super-dry-asahi/>
- ³⁰ Management | Our Group | ASAHI GROUP HOLDINGS. (2016). Asahi Group Holdings, Ltd. <https://www.asahigroup-holdings.com/en/company/board/>
- ³¹ Council Post: The Evolution of the Chief Information Officer Role | Zunino, A. (2024, September 9). Forbes. <https://www.forbes.com/councils/forbestechcouncil/2024/09/09/the-evolution-of-the-chief-information-officer-role/>
- ³² Professor Shingo KONOMOTO | Kyoto University. (2020, November 11). Graduate School of Management, Kyoto University. <https://www.gsm.kyoto-u.ac.jp/en/faculty/451194/>
- ³³ Integrated Report Various Reports | IR Library | Investors | ASAHI GROUP HOLDINGS. (2023). Asahi Group Holdings, Ltd. <https://www.asahigroup-holdings.com/en/ir/library/annual/>
- ³⁴ How Boards can Support Resiliency in the Face of Constant Crisis | EY Center for Board Matters. (2023, October). EY Center for Board Matters. <https://www.ey.com/content/dam/ey-unified-site/ey-com/pt-br/campaigns/board-matters/documents/ey-cbm-how-boards-can-support-resiliency-in-the-face-of-constant-crisis.pdf>
- ³⁵ Overview of Timely Disclosure | Japan Exchange Group. (2025). Japan Exchange Group. <https://www.jpx.co.jp/english/equities/listing/disclosure/overview/index.html>
- ³⁶ Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure | SEC. (2023). U.S. Securities and Exchange Commission. <https://www.sec.gov/resources-small-businesses/small-business-compliance-guides/cybersecurity-risk-management-strategy-governance-incident-disclosure>
- ³⁷ Top 8 Network Segmentation Best Practices in 2023 | Chin, K. (2023, January 5). UpGuard. <https://www.upguard.com/blog/network-segmentation-best-practices>
- ³⁸ Corporate Governance Guidelines 2026 | ASAHI GROUP HOLDINGS. (2026, March 24). Asahi Group Holdings, Ltd. https://www.asahigroup-holdings.com/pdf/en/company/governance/policy/260324_CGguidelines_en.pdf
- ³⁹ The NIST Cybersecurity Framework (CSF) 2.0 | National Institute of Standards and Technology. (2024, February 26). National Institute of Standards and Technology. <https://doi.org/10.6028/nist.cswp.29>
- ⁴⁰ Cyber Insurance | Tokio Marine. (2023). Tokio Marine. <https://www.tokiomarine.com/sg/en/non-life/products/business/liability/cyber-insurance.html>

- ⁴¹ Should Insurance be Disclosed in Corporate Financial Statements? An Analysis of the Views of Stakeholders | Adams, M. (2025). Journal of International Accounting, Auditing and Taxation, 58, 100686. <https://doi.org/10.1016/j.intaccaudtax.2025.100686>
- ⁴² Limited Annual Securities Report | Kirin Holdings Company. (2024). Kirin Holdings Company. <https://pdf.irpocket.com/C2503/wOrc/mbHL/bpS6.pdf>
- ⁴³ Limited Annual Securities Report | Kirin Holdings Company. (2025). Kirin Holdings Company. <https://pdf.irpocket.com/C2503/LseR/sxVQ/LwT7.pdf>
- ⁴⁴ Notice Regarding a Material Weakness in Internal Control over Financial Reporting | Newsroom | ASAHI GROUP HOLDINGS. (2026, July 27). Asahi Group Holdings, Ltd. <https://www.asahigroup-holdings.com/en/newsroom/detail/20260727-0204.html>

Appendix A: Timeline of events

Date/time	Event	Further Elaboration
~19 Sep 2025 – 28 Sep 2025	Findings revealed that unauthorised access occurred ~10 days before the 29 September 2025 cyberattack	Dwell time of ~10 days where Asahi's IT systems did not flag unusual activities and, therefore, no escalation upwards as no one was likely aware
29 Sep 2025 (~07:00 JST)	- System disruption occurred in company system - Subsequent investigation confirmed presence of encrypted files	First confirmed detection in the public record via announcement by Asahi
29 Sep 2025 (~11:00 JST)	Network was disconnected and data centre was isolated to minimise the impact	Decision to contain attack suggested that crisis response was activated by late morning
29 Sep 2025 (~18:36 JST)	- First public disclosure that a cyberattack had caused disruptions to Asahi's Japanese operations at 18:36 JST - System-based order and shipment processes were suspended	- Fast public disclosure - Exact internal approval and escalation timing were not publicly disclosed
29 Sep 2025	ERH established upon detection of the cyberattack to investigate	Under Asahi's governance framework, major crises will trigger ERH, which is led by the President and Group CEO
30 Sep 2025	- Production was still suspended at Japanese factories - Asahi had 30 plants in Japan making beer, beverages and food products, and it was still investigating whether all of them had stopped production - Asahi submitted a preliminary report to the PIPC	Notification to regulator about data breach a day after the attack, showing escalation beyond operational teams
1 Oct 2025 – 3 Oct 2025	- Began partial manual order processing and shipment - ERH was still working in collaboration with external cybersecurity experts to restore the system as quickly as possible	- Business continuity plans activated - Investigations were still ongoing
2 Oct 2025	Asahi Breweries resumed production at all six of its domestic factories from 2 October 2025, and partial shipments of Asahi Super Dry had resumed	Recovery began for Asahi's products
3 Oct 2025	- Second public update to confirm ransomware - External cybersecurity experts were engaged - Manual order processing and shipment continued - Subsequent investigations had confirmed traces suggesting a potential unauthorised transfer of data	- Clearest public evidence of internal escalation and expert involvement - First comments by President and Group CEO about the cyberattack together with the second public update - Delay in comments by four days likely owing to Asahi handling the impact of the cyberattack
8 Oct 2025	- Qilin Ransomware Group claimed responsibility for cyberattack - Asahi said data suspected of unauthorised transfer had been identified online	Escalation from mere operational disruption to data breach incident

Date/time	Event	Further Elaboration
8 Oct 2025	- Follow-up report submitted to PIPC after confirming that the information suspected to have been exposed had been identified on the Internet - Asahi Soft Drinks had partially resumed production at six of its seven domestic factories as of 8 October 2025 - Asahi Group Foods had partially resumed production at all seven of its domestic factories as of 8 October 2025	Public and regulatory escalation continued in parallel with other operational recovery and investigation efforts
9 Oct 2025	All seven of Asahi's soft drinks factories resumed production	Full recovery of Asahi's soft drinks production
14 Oct 2025	Q3 2025 financial results postponed owing to delayed financial closing procedures and systems restoration	Cyber incident impact extended beyond operational to financial reporting and disclosure controls
15 Oct 2025	Beginning 15 October 2025, partial shipments of products including Asahi Draft Beer and Asahi Dry Zero had resumed, as part of ongoing recovery efforts	Phased recovery for Asahi's alcohol production
13 Nov 2025	- First post-cyber incident October sales overview published - Handling of orders and shipments was still performed manually	Useful notification to the public to disclose impact of cyberattack on the sales output for October 2025
26 Nov 2025 – 27 Nov 2025	- Asahi submitted a final report to the PIPC on 26 November 2025 - On 27 November 2025, Asahi published investigation results, personal data categories at risk and information on efforts spent containing the attack and restoring systems, and targeted logistics full recovery by February 2026 - Asahi said to postpone announcement of its financial results for 2025 - Public disclosure of updates included comments from President and Group CEO Atsushi Katsuki	- First broad forensic investigation milestone to account to the public on cyber incident's impact and measures undertaken by Asahi to minimise impact - Delay in publishing such details owing to assessment of impact and recovery efforts - Financial results for 2025 delayed owing to financial reporting systems being disrupted
2 Dec 2025 – 3 Dec 2025	Order placement and product shipment using logistics-related systems were resumed via Electronic Ordering System	Important recovery milestone highlighting the gradual recovery from the cyber incident
Dec 2025 – Feb 2026	Recovery and impact assessment period	- Following the restoration of production factories, Asahi focused on assessing financial and operational impacts and implementing measures to prevent future occurrences - No major announcement during this period, which may suggest focus on recovery and post-incident assessment
26 Feb 2026	President and Group CEO Atsushi made a business update announcement to highlight firm's performance and cyberattack updates	Business update by President and Group CEO on financial performances across different regions of Asahi operations

Date/time	Event	Further Elaboration
10 Mar 2026	Asahi announced its financial results for Q3 2025	- Long delay owing to financial reporting delays from cyberattack - Efforts needed to compile impact of the cyberattack while allowing systems to recover - Comments by President and Group CEO on Q3 2025 financial results
24 Mar 2026	Asahi announced that it had decided to postpone the disclosure of its financial results for the first quarter of the fiscal year ending 31 December 2026	Cyberattack resulted in delays in financial statements' preparation and review disclosures
Mar 2026 – May 2026	Ongoing financial reporting remediation	Continuous work on financial reporting owing to the delays
22 May 2026	Asahi announced that financial results for 2025 would be published on 8 July 2026	Cyberattack caused months of delay owing to financial and accounting systems closure and time taken to analyse impact and prepare financial statements

Appendix B: Event study methodology

Values of Asahi's stock price and Nikkei 225 Index position were extracted from S&P Capital IQ.

Using the market model, Asahi's actual returns (AR) can be calculated as

$$R_{Asahi,t} = \alpha_{Asahi} + \beta_{Asahi} R_{Market,t} + \varepsilon_t$$

where $R_{Market,t}$ represents the Nikkei 225 index return on day t . The parameters α and β were estimated using ordinary least squares (OLS) regression over a 120-trading-day estimation window from T-120 to T-11. This estimation window was chosen to obtain stable estimates of Asahi's normal relationship with the market and avoid potential contamination from information leakage immediately preceding the attack itself.

The expected return,

$$E(R_{Asahi,t}) = \hat{\alpha}_{Asahi} + \hat{\beta}_{Asahi} R_{Market,t},$$

was then used to calculate the AR as

$$AR_t = R_{Asahi,t} - E(R_{Asahi,t})$$

or equivalently,

$$AR_t = R_{Asahi,t} - (\hat{\alpha}_{Asahi} + \hat{\beta}_{Asahi} R_{Market,t}).$$

CAR were calculated as

$$CAR_{[\tau_1, \tau_2]} = \sum_{t=\tau_1}^{\tau_2} AR_t$$

where τ_1 and τ_2 represent the start and end of the event window.

Period	Relative Trading Days	Purpose
Estimation Window	T-120 to T-11	Estimate the market model parameters (α and β) using OLS regression
Buffer Period	T-10 to T-1	Excluded to minimise potential contamination arising from information leakage and anticipatory trading
Event Date	T ₀	30 September 2025, because the cyberattack announcement was made on 29 September 2025 at 18:36 JST, and owing to after-hours trading, prices will have been reflected the next day
Event Study Windows	[-1,1], [-2,2], [-5,5]	Assess the immediate and short-term stock market reaction to the cyberattack

Appendix C: Hypothesis testing methodology

To assess the statistical significance of each window's returns, we use the standardised-CAR test which compares the CAR with Asahi's normal stock volatility estimated from the pre-event period. Under the null hypothesis $H_0: CAR = 0$, the test statistic is defined as

$$t_{CAR} = \frac{CAR_i}{\sqrt{L \times \widetilde{\sigma}_i^2}}$$

where L represents number of days in the event window, σ_i^2 represents residual variance of the firm, and i represents the individual firm (Asahi, Kirin, Sapporo).

Given $M-2 = 108$, where M is the number of trading days (110), and since the market model uses two parameters, degree of freedom with the t-test is 108. The test statistics approximately follow a standard normal distribution:

$$T_{108} \approx N(0,1)$$

The significance is measured at 1%, 5% and 10%.

For simplicity, the standard error (SE) is calculated as $SE = \sqrt{L \times \widetilde{\sigma}_i^2}$. We omit the estimation period forecast-error correction term because including it would marginally increase the SE and make the test more conservative (i.e. t-value becomes smaller). However, in our test, it will not affect the statistical significance outcome because our result is already statistically insignificant.

Appendix D: Trading volume

Company	Event Window	Pre-event Trading Volume	Event-date Trading Volume	Post-event Trading Volume	Post-event Change
Asahi	[-1,+1]	8,270,700	8,153,000	8,369,300	1.19%
	[-2,+2]	9,435,200		7,619,050	-19.25%
	[-5,+5]	9,481,460		6,461,860	-31.85%
Kirin	[-1,+1]	2,543,200	2,223,100	3,287,900	29.28%
	[-2,+2]	2,416,950		2,860,050	18.33%
	[-5,+5]	2,703,860		2,668,260	-1.32%
Sapporo	[-1,+1]	1,003,000	914,500	878,000	-12.46%
	[-2,+2]	1,048,250		876,000	-16.43%
	[-5,+5]	940,600		922,600	-1.91%

Note: The pre- and post-event averages were calculated using trading days only. The event date was 30 September 2025. Kirin and Sapporo were included as industry benchmarks to assess whether changes in Asahi's trading volume reflected a company-specific response or broader movements in the Japanese beverage sector. Values were extracted from S&P Capital IQ.

Appendix E: Annualised returns and standard deviation

To further assess Asahi's share price performance before and after the cyberattack, our study compared Asahi's average daily returns, volatility and Sharpe ratio across the period from 30 September 2024 to 31 March 2026. The pre-event period covered 30 September 2024 to 29 September 2025 and the post-event period covered 1 October 2025 to 31 March 2026. The event date, 30 September 2025, was excluded from this pre- and post-event comparison to avoid the announcement-day reaction distorting either period.

1. Daily returns were calculated as

$$R_t = \frac{P_t - P_{t-1}}{P_{t-1}}$$

where R_t is Asahi's daily return on day t , P_t is the adjusted closing price on day t , and P_{t-1} is the adjusted closing price on the previous trading day.

2. Annualised returns were calculated as

$$\text{Annualised Return} = \frac{\sum R_t}{n} \times 252$$

where n is the number of trading days in the period.

3. Annualised volatility was measured using

$$SD = \sqrt{\frac{\sum (R_t - \bar{R})^2}{n - 1}} \times \sqrt{252}$$

where SD is the annualised standard deviation of returns, and n is the number of trading days in the period.

4. Finally, to evaluate the risk-adjusted performance, the Sharpe ratio was calculated as

$$\text{Sharpe Ratio} = \frac{\text{Annualised Return}}{S.D.}$$

Firm	Annualised Metric	Pre-event (30 Sep 2024 to 29 Sep 2025)	Post-event (1 Oct 2025 to 31 Mar 2026)
Asahi	Returns	−3.21%	−21.90%
	Standard Deviation	21.17%	19.62%
	Sharpe Ratio	−0.15	−1.12
Kirin	Returns	0.31%	33.18%
	Standard Deviation	18.10%	23.80%
	Sharpe Ratio	0.02	1.39
Sapporo	Returns	−2.78%	34.01%
	Standard Deviation	28.28%	32.74%
	Sharpe Ratio	−0.10	1.04

Asahi's annualised return fell from −3.21% before the attack to −21.90% after it—its shares clearly performed worse once the news broke, in line with the negative abnormal returns in Section 3.1.1. Its volatility, though, actually lowered, from 21.17% to 19.62%. In other words, the market absorbed the news by pushing Asahi's returns lower rather than by trading it more wildly. The

Sharpe ratio also dropped from -0.15 to -1.12 , meaning investors received much worse returns for the risk they took.

Appendix F

Kirin Holdings Board members' composition:

Board Member	Position	Core Expertise	Cyber Risk Background?
Yoshinori Isozaki	Representative Director of Board, CEO	Corporate planning, legal and risk management, global leadership, marketing, sustainability, HR, finance & investor relations (IR)	None disclosed
Takeshi Minakata	Representative Director of Board, President, COO	Corporate planning, global leadership, finance, HR, R&D, Quality assurance, sustainability, global leadership	None disclosed
Junko Tsuboi	Director of Board, Senior Executive Vice President	Corporate management, sustainability, legal and risk management, marketing, HR	None disclosed
Toru Yoshimura	Director of Board, Senior Executive Officer	Corporate management, sustainability, global leadership, finance & IR, R&D, HR, information and communication technology/digital transformation (ICT/DX), manufacture/quality assurance	None disclosed
Shinjiro Akieda	Director of Board, Senior Executive Officer	Corporate management, sustainability, global leadership, finance & IR, legal and risk management, marketing, ICT/DX	None disclosed
Hiroyuki Yanagi	Non-executive Director	Corporate management, R&D	None disclosed
Noriko Shiono	Non-executive Director	Corporate management, global leadership, marketing	None disclosed
Shinya Katanozaka	Non-executive Director	Corporate management, global leadership, HR	None disclosed
Yoshiko Ando	Non-executive Director	Sustainability, legal and risk management, HR	None disclosed
Shingo Konomoto	Non-executive Director	Corporate planning, finance/IR, ICT/DX	~30 years of experience as a Strategy and IT consultant at Nomura Research Institute
Naoko Mikami	Non-executive Director	R&D, HR, manufacture/quality assurance	None disclosed
Kenichi Fujinawa	Non-executive Director	Global leadership, legal and risk management, HR	None disclosed

Kirin Holdings Executive Committee's composition:

Member	Areas of Responsibility
Mitsuharu Yamagata	- Marketing, Corporate Brand Strategy - Digital, Information Strategy
Kazufumi Nagashima	- Supply Chain Management Strategy - Production Technology Strategy
Toshihito Hama	- Chief Risk Management Officer - Public Relations Strategy - Chief Legal Officer

Member	Areas of Responsibility
Daisuke Fujiwara	• R&D Strategy • President of R&D Division
Yoshiyuki Yonetani	• Chief Quality Assurance Officer
Hiroaki Takaoka	• General Manager, Corporate Strategy Department (Business Partnerships & Investment Strategy) • CSV Strategy
Hideki Horiguchi	• President and CEO of Kirin Brewery Co., Ltd.
Kazuhiro Inoue	• President and CEO of Kirin Beverage Co., Ltd.
Hideki Mitsuhashi	• President, Representative Director of FANCL Corporation
Alastair Symington	• CEO & Managing Director, Blackmores Limited