Research Question: "To what extent can Coupang be held ethically responsible for the harm caused to its stakeholders by the 2025 data breach?"

Introduction

Known as the Amazon of South Korea, Coupang is the leading e-commerce company in South Korea, where half of the Korean population are active buyers. Coupang offers a wide range of services, including online retail, restaurant delivery, video streaming, and more under brands that include Coupang, Coupang Eats, and Coupang Play. In 2025, Coupang announced a data breach incident in which the personal information of 33.7 million users was exposed. The leaked data included full names, phone numbers, email addresses, physical addresses, and order details (Chia).

The key concept of this investigation is **ethics. Ethics** refers to the moral principles that guide business behavior and decision-making, including responsibilities toward customers, employees, shareholders, and society.

The data breach incident raised **ethical** questions regarding whether Coupang fulfilled its **ethical** responsibility to protect customer data. As the incident resulted in harm to its stakeholders, this investigation will answer the research question: "To what extent can Coupang be held **ethically** responsible for the harm caused to its stakeholders by the 2025 data breach?"

Methodology

Corporate social responsibility (CSR) will be used to evaluate whether Coupang fulfilled its **ethical** responsibility to protect customer data by examining its management's resource allocation decisions in cybersecurity.

Stakeholder analysis will be used to evaluate how the data breach incident harmed different stakeholders, including customers, employees, shareholders, and the government.

Financial ratio analysis will be used to quantify the harm caused to its stakeholders by the data breach. In particular, the gross profit margin and net profit margin in Q4 2024 and Q4 2025 will be analyzed to measure the financial harm borne by shareholders as a consequence of the incident.

Corporate social responsibility

Corporate social responsibility refers to the value of an organization that positively impacts the society and considers the interests of its stakeholders. CSR will be used to evaluate the extent to Coupang **ethically** responsible for the data breach incident.

Coupang's investment in cybersecurity was only 0.21% of its annual sales. In 2024, Coupang generated sales of 41.2901 trillion won but invested only 86 billion won in its cybersecurity system. In comparison, Amazon invested approximately 1% of its sales in cybersecurity in 2023 (SD #1). This suggests that Coupang's investment in cybersecurity is a much smaller proportion of its revenue than the global e-commerce companies.

This relatively small investment was due to the fact that Coupang prioritized rapid business expansion over internal security systems. Coupang's sales tripled over five years, but its investment in cybersecurity did not grow at the same pace. Lee Jong-woo, a professor at Ajou University, stated that Coupang focused on "increasing its market share and maximizing profits in the short term" rather than investing in a cybersecurity system (Lee). This highlights Coupang's resource allocation decisions in which more investment was directed toward growth and expansion than toward security infrastructure.

Additionally, this investment decision can also be attributed to legal factors. Under the Personal Information Protection Act, penalty surcharges are calculated based only on the sales directly related to the data breach rather than on the company's total sales (SD #1). As a result, the expected financial penalties are low, reducing the incentive for Coupang to invest heavily in cybersecurity before an incident happens.

Therefore, Coupang can be held **ethically** responsible to a significant extent for the harm caused to its stakeholders by the 2025 data breach. Its relatively low investment in cybersecurity suggests that the company failed to fulfil its corporate social responsibility to protect customer data as a major e-commerce company handling the personal information of more than 33 million customers. Although greater investment in cybersecurity would have increased short-term costs, it could have reduced the risk of a data breach and the resulting harm to its stakeholders.

Stakeholder analysis

A stakeholder analysis is used to identify how stakeholders are affected by Coupang's data breach incident. Stakeholders can be divided into two categories: internal stakeholders are groups who are part of the organization, and external stakeholders are those outside the organization but harmed by the business. Since every stakeholder has a different perspective on the Coupang data breach incident, it is important to assess Coupang's **ethical** impact on each stakeholder.

Customers: The breach exposed the personal data of 33.7 million users. According to an executive director at the Korea Chainstores Association, "Consumer trust in Coupang has been shaken." Coupang faced a 6.3% decline in average daily consumer spending, from 139.2 billion won (US$97 million) in November (SD #2). This highlights that Coupang's failure to protect

customer data reduced customer trust and loyalty despite Coupang's offer of a ₩50,000 voucher to every affected user.

Coupang Partners Association: The data breach incident caused financial harm to Coupang Partners who relied on the platform through reduced order volume and lower income. According to a Coupang parcel driver in his 30s, since the data breach, fewer orders have meant less money, and he struggles to support his family and pay bills (SD #3). The association also raised concerns that "excessive sanctions beyond the scope of responsibility could severely damage operations, eliminate delivery and logistics jobs, and threaten the livelihoods of thousands of families" (SD #3).

Small and mid-sized merchants: The data breach incident caused harm to merchants because reduced consumer confidence lowered demand on Coupang. Since they relied on Coupang as a primary sales channel, the incident caused revenue losses. According to the Korea Federation of Micro Enterprises, merchants selling on Coupang reported average sales declines of 30-40% since the data breach. Agricultural merchants especially said that "farmers and fresh food producers are often the first to be affected when demand declines because they can't endure prolonged disruptions" (SD #3).

Executives: After the incident, CEO Park Dae-jun resigned, taking responsibility and accountability for the data breach incident. This also led to Harold Rogers, the Chief Administrative Officer of its parent company in the United States, taking over as Interim Chief Executive Officer (Kim). This highlights that the **unethical** practice damaged the reputations of the senior management and reduced confidence in Coupang's leadership.

Shareholders: Coupang's share price fell after the breach incident became public. On November 28, the price was US$28.16, while on December 19, the price fell to US$23.20 (SD #3). As a result, shareholder wealth was reduced by US$8 billion in market value. Additionally, U.S. shareholders filed a class-action lawsuit against Coupang, claiming that Coupang delayed disclosure of the breach, which violated the U.S. Securities and Exchange Commission (SEC) rules requiring corporations to disclose material cybersecurity incidents within four business days, and misled investors (SD #3). Coupang's **unethical** decision caused shareholder harm by reducing confidence and failing to meet shareholder value objectives.

Government: The government incurred costs in order to respond to the data breach incident. For example, the government conducted an emergency meeting to respond to the incident and launched an investigation to determine whether Coupang violated its obligations to implement adequate safeguards. Additionally, the government warned citizens about phishing and smishing scams using Coupang's name ("Government Holds Emergency Meeting"). In June 2026, the Personal Information Protection Commission imposed a fine of 624.7 billion won (US$410

million) over the data breach incident (Lee). The government's response and the fine reflect the severity of the incident and demonstrate that Coupang failed to meet its **ethical** obligation to protect customer data.

Overall, the stakeholder analysis reveals that customers and shareholders are the most harmed stakeholders. This is because customers experienced privacy violations due to Coupang's limited investment in cybersecurity systems, while shareholders were harmed by financial losses and the delayed disclosure of the data breach. Therefore, the widespread and severe harm experienced by multiple stakeholder groups highlights that Coupang can be held **ethically** responsible to a significant extent for the 2025 data breach.

Financial ratio analysis

Financial ratio analysis will measure the financial harm borne by shareholders as a consequence of the data breach incident. Financial ratio analysis will be used to quantify the harm of the data breach on Coupang's profitability and the financial harm to shareholders. In particular, the Gross Profit Margin, a profitability ratio that measures an organization's gross profit as a percentage of its sales revenue, and the Net Profit Margin, a profitability ratio that measures a firm's operating profit (profit before interest and tax) as a percentage of its sales revenue, will be used.

Partial financial statement of Coupang in Q4 2024 and Q4 2025

	Q4 2024	Q4 2025
Sales Revenue	7,965	8,835
Cost of sales (calculated)	5,474	6,291
Gross profit	2,491	2,544
Expenses (Calculated)	2,179	2,536
Profit before interest and tax	312	8

$$Gross\ Profit\ Margin\ = \frac{Gross\ Profit}{Sales\ Revenue} \times 100$$

$$Net\ Profit\ Margin\ = \frac{Net\ Profit\ before\ interest\ and\ tax}{Sales\ Revenue} \times 100$$

Coupang's Profitability Data in Q4 2024 and Q4 2025

	Q4 2024	Q4 2025	% Increase/Decrease

			from Prior Year
Revenue (US$ million)	7,965	8,835	+11%
Gross Profit (US$ million)	2,491	2,544	+2%
Operating Income/ Profit before interest and tax (US$ million)	312	8	-97%
Gross Profit Margin	31.27%	28.80%	-2.47
Net Profit Margin	3.92%	0.09%	-3.83

Coupang's profitability declinedbetween Q4 2024 and Q4 2025 despite an 11% increase in sales revenue. Gross profit margin fell from 31.27% to 28.80% while net profit margin declined from 3.92% to 0.09%. According to Coupang's Q4 2025 earnings report, the data breach negatively affected customer activity, WOW membership growth, and profitability beginning in December, providing evidence that the breach contributed to this decline (SD #4).

However, the decline in profitability cannot be attributed entirely to the data breach. Increased competitive pressure was another factor, as rivals such as Naver sought to gain market share following declining customer trust in Coupang. Coupang's monthly active mobile users fell by 3.5% between November and January, while Naver's increased by 23% (SD #2).

Therefore, while other factors contributed to Coupang's declining profitability, the breach caused financial harm to Coupang and its shareholders. This shows that Coupang can be held **ethically** responsible for stakeholder harm because its failure to protect customer data reduced its ability to generate returns for shareholders. This suggests that Coupang's failure to fulfill its **ethical** responsibility to protect customer data undermined its profit and shareholder value objectives.

Conclusion:
By evaluating Coupang's corporate social responsibility, its impact on stakeholders, and the financial consequences of the breach, it can be concluded that Coupang can be held ethically responsible to a significant extent for the harm caused to its stakeholders by the 2025 data breach.

Although external legal factors reduced businesses' incentives to invest in cybersecurity, they do not remove Coupang's responsibility for managing and protecting customer data. Therefore, Coupang's prioritization of short-term growth and profitability over stakeholder protection

represents a failure to fulfill its corporate social responsibility. Furthermore, the decline in profitability and shareholder value following the data breach demonstrates that this prioritization harmed Coupang's long-term business performance. This suggests that ethical responsibility and profitability are not conflicting objectives; rather, failing to protect stakeholders can undermine both a company's ethical responsibilities and its long-term profitability.

Supporting Document

Supporting Document 1

Yeon, Ji-yeon. “Coupang Invests 86 Billion Won but Fails Internal Controls, Causing Data Breach - CHOSUNBIZ.” *Chosunbiz*, 2 Dec. 2025, https://biz.chosun.com/en/en-retail/2025/12/03/ISRRFDRIVNF4JJIMTP45YR6EJA/. Accessed 27 Aug. 2026.

Supporting Document 2

Yang, Heekyong. “Coupang Braces for Increased Competition Amid Fallout From South Korea Data Breach.” *Reuters*, 25 Feb. 2026, https://www.reuters.com/business/retail-consumer/coupang-braces-increased-competition-amid-fallout-south-korea-data-breach-2026-02-25/. Accessed 27 Aug. 2026.

Supporting Document 3

“As Coupang Data Leak Probe in South Korea Drags on, Delivery Workers and Sellers Bear the Cost.” *The Straits Times*, 5 Feb. 2026, https://www.straitstimes.com/asia/east-asia/as-coupang-data-leak-probe-in-south-korea-drags-on-delivery-workers-sellers-bear-the-cost. Accessed 27 Aug. 2026.

Supporting Document 4

“Coupang Announces Results for Fourth Quarter 2025.” *Aboutcoupang.Com*, 2025, https://ir.aboutcoupang.com/news-events/news/news-details/2026/Coupang-Announces-Results-for-Fourth-Quarter-2025/default.aspx. Accessed 27 Aug. 2026.

Supporting Document 5

Kim, Jong-yong. “Coupang Faces U.S. Shareholder Class Action Over Delayed Breach Disclosure - CHOSUNBIZ.” *Chosunbiz*, 20 Dec. 2025, https://biz.chosun.com/en/en-society/2025/12/21/LUIL36LGLVEH7D2RVUMZMJ6AFM/?outputType=amp. Accessed 27 Aug. 2026.

Works Cited

Chia, Osmond. “South Korea: Online Retail Giant Coupang Hit by Massive Data Leak.” *BBC*, 1 Dec. 2025, https://www.bbc.com/news/articles/c36zwywll02o. Accessed 29 Aug. 2026.

“Government Holds Emergency Meeting on Coupang Security Breach and Personal Data Leak.” *Ministry of Science and ICT*, 30 Nov. 2025, https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&mPid=2&mId=4&bbsSeqNo=42&nttSeqNo=1194. Accessed 29 Aug. 2026.

Kim, Heejin. “Coupang CEO Resigns After Online Retailer Hit by Massive Data Breach.” *Reuters*, 10 Dec. 2025, https://www.reuters.com/world/asia-pacific/coupang-ceo-resigns-after-online-retailer-hit-by-massive-data-breach-2025-12-10/. Accessed 27 Aug. 2026.

Lee, Min-hyung. “Coupang Pledges Legal Action Against Record $409 Mil. Fine Over Massive Data Breach.” *Koreatimes.Co.Kr*, The Korea Times, 11 June 2026, https://www.koreatimes.co.kr/amp/business/companies/20260611/coupang-pledges-legal-action-against-record-409-mi-fine-over-massive-data-breach. Accessed 29 Aug. 2026.

Lee, Sung-Hee. “Coupang Failed to Safeguard the Lives of Workers and Customer Security… the Unvarnished Reality of ‘Growth Without Substance.”경향신문, 30 Nov. 2025, https://www.khan.co.kr/en/article/202511302323027. Accessed 27 Aug. 2026.