Samvid Multidisciplinary Research Journal
Where researchers meet their destiny...
ISSN 2582-015X

Assessment of Relationship Between Cyber Security Expenditure and Financial Performance of Steel Companies

Dr. Harsha N. Dangar

Assistant Professor (Commerce and Accountancy)
Shri V.R. Patel College of Commerce , Mehsana
(M.Com , PhD , P.G.D.C.A. , B.Ed , M.A(Yoga & Sol) , M.P.A (Kathak)

Jinal Bharatbhai Prajapati

Assistant Professor (Commerce and Accountancy)
Research Scholar (HNGU , Patan
M.Com , GSET
Oswal Arts and Commerce College , Juna Deesa , Banaskantha

ABSTRACT :
The steel industry has been forced to combine information technology (IT) and operational technology (OT) due to the fast digitalization of the manufacturing sector, often known as Industry 4.0. Although efficiency is improved by this convergence, cyber threats have an exponentially larger attack surface. This study examines the relationship between large steel firms' financial performance and cybersecurity spending. The purpose of the study is to ascertain whether investing in strong cybersecurity frameworks is a strategic investment that supports financial measures like Return on Equity (ROE) and Return on Assets (ROA) or if it is just a sunk cost. Research tests the claim that increased cybersecurity spending reduces operational downtime risks using secondary financial data and correlation analysis on a sample of five well-known steel businesses so safeguarding sources of income and maintaining financial stability. The results point to a moderately positive association, suggesting that cybersecurity resilience is a crucial factor in determining the long-term financial health of the contemporary steel industry.
KEYWORDS: Cybersecurity Expenditure, Financial Performance, Steel Industry, Return on Assets (ROA)

1. INTRODUCTION

The global steel industry is at a turning point when automated, networked digital technologies are quickly replacing traditional manufacturing processes. Although this paradigm shift has increased productivity, it has also created a serious vulnerability: the possibility of cyberattacks. A compromise can stop blast furnaces, interfere with supply chains, and result in significant financial losses for steel producers, making it more than just a data privacy concern. As a result, funding for cyber security risen significantly, with IBM (2024) reporting that industrial organizations face higher breach costs than the global average due to the high cost of operational downtime. Furthermore, EOXS (2025) emphasizes that as steel manufacturers adopt smart technologies, their exposure to ransomware and IP theft increases, making cyber resilience synonymous with operational continuity. A single day of downtime

in a large steel production can result in millions of dollars in lost revenue, which has significant financial ramifications (EY, 2023). Therefore, it is crucial for financial managers and commerce researchers to evaluate the connection between these protective expenditures and common financial performance indicators like Return on Assets (ROA). According to this analysis, spending on cybersecurity should be viewed as an asset protection strategy that maintains shareholder value rather than merely as a cost.

2. LITERATURE REVIEW

1. Impact of Cyber Breaches on Financial Statements:
Al-Amosh and Khatib (2024) studied the connection between financial performance and cybersecurity disclosure. According to their research, which was published in relation to the banking and industrial sectors, stakeholder confidence is greatly increased when cybersecurity readiness is transparent. They discovered a positive relationship between firm valuation and cybersecurity disclosure quality, indicating that investors consider cyber-resilient companies to be lower-risk investments.

2. The Cost of Underinvestment:
Gordon et al. (2018) noted in a seminal study on private sector investment that companies often underinvest in cybersecurity since it is challenging to calculate the Return on Investment (ROI). According to their empirical data, businesses frequently view cyber security as a box-ticking exercise for compliance rather than a strategic financial instrument resulting in serious financial shocks when they happen.

3. Industrial Sector Vulnerabilities:
The particular hazards that heavy manufacturing faces were examined in a Fortune Business Insights (2025) research on the Industrial Cybersecurity Market. According to the literature, the steel industry is particularly vulnerable because of its reliance on outdated OT systems. According to the study's findings, "reactive" spending—that is, spending that occurs after a breach—harms financial performance measures considerably more than "proactive" spending.

4. Operational Downtime and Revenue Loss:
Operational Downtime and Revenue Loss: The manufacturing sector incurs some of the greatest expenses associated with system outages, according to IBM's Cost of a Data Breach Report (2024). The literature makes a distinction between indirect financial effects (reputational harm) and direct expenses (ransom payments, technical recovery).Higher preventative spending is correlated with lower overall breach costs, according to the study.

5. Cybersecurity as a Public Good in Finance:
5. Cybersecurity as a Public Good in Finance: Although the SUERF (2023) study on financial stability focuses on banks, steel conglomerates can benefit greatly from its concepts. Cybersecurity, according to the authors, is a "weakest-link" issue. Investing in cybersecurity protects not only the company but the entire value chain for steel firms with extensive supply chains, securing the company's long-term financial position against systemic shocks
.

3. RESEARCH METHODOLOGY

3.1 Objectives of the Study

- To examine the trend of cybersecurity spending over the past five years in the chosen steel businesses.
- To assess these businesses' financial performance using Return on Equity (ROE) and Return on Assets (ROA)..
- To ascertain the statistical correlation between cybersecurity spending and the chosen steel firms' financial performance.

3.2 Population and Sample Size

All significant steel manufacturing firms registered on India's National Stock Exchange (NSE) make up the study's population. Based on their market capitalization and data accessibility, the following five significant steel companies were chosen using purposive sampling :

1. Tata Steel Ltd.
2. JSW Steel Ltd.
3. Steel Authority of India Ltd. (SAIL)
4. Jindal Steel & Power Ltd. (JSPL)
5. Arcelor Mittal Nippon Steel India (AM/NS)

3.3 Research Design

A descriptive and analytical research design is used in this study. It describes the current situation of cyber spending in the sector, making it descriptive.To determine the statistical relationship between cybersecurity expenditure and the financial performance of the selected steel companies.

3.4 Data Collection

- **Secondary Data:** Financial data (Net Profit, Total Assets, Shareholder Equity) was sourced from the annual reports of the respective companies for the fiscal years 2019-2020 through 2023-2024. Cybersecurity expenditure data was derived from "IT and Systems" budget disclosures and industry estimation reports where specific line items were not public.

3.5 Hypothesis

- **H0 (Null Hypothesis):** There is no significant relationship between Cybersecurity Expenditure and Return on Assets (ROA) in steel companies.
- **H1 (Alternative Hypothesis):** There is a significant positive relationship between Cybersecurity Expenditure and Return on Assets (ROA) in steel companies.
- **H0 (Null Hypothesis) :** There is no significant relationship between Cybersecurity Expenditure and Return on Equity (ROE).
- **H2: (Alternative Hypothesis) :** There is a significant positive relationship between Cybersecurity Expenditure and Return on Equity (ROE**).**

4. DATA ANALYSIS AND INTERPRETATION

We examined the average yearly cybersecurity spending (as a stand-in for IT security investment) and contrasted it with the average return on assets (ROA) over a five-year period in order to evaluate the link. Due to the absence of publicly disclosed cybersecurity expenditure data, the study uses industry-based estimates for cybersecurity spending, while financial performance indicators such as net profit, total assets, and ROA are derived from audited financial statements.

Table 1: Comparative Analysis of Cyber Expenditure vs. Financial Performance (5-Year Average)

Company Name	Avg. Annual Cyber Security Exp. (₹ Crores)	Avg. Net Profit (₹ Crores)	Avg. Total Assets (₹ Crores)	Average ROA (%)
Tata Steel	90	13,970	2,54,133	**1.2 %**
JSW Steel	85	5,837	2.40,445	**2.4%**
SAIL	55	2,372	1,40,000	**1.7 %**
Jindal Steel	60	5.943	78,715	**7.5 %**
AM/NS India	45	-1200 loss	75,000	**-1.6 %**

5.Interpretation:

By connecting expected cybersecurity spending to financial performance and asset efficiency, the table offers a comparative perspective of a few Indian steel businesses. Due to their vast asset bases, international operations, and increased digital and operational complexity, large companies like Tata Steel and JSW Steel have higher estimated cybersecurity spending. Nevertheless, despite having the highest total assets, both companies record relatively low ROA, indicating that asset efficiency is limited by heavy capital intensity, high fixed costs, and cyclical market conditions. Jindal Steel & Power Ltd., on the other hand, gets the greatest ROA while having a relatively smaller asset base and a moderate cybersecurity investment, indicating better operational efficiency and asset utilization. SAIL's ROA and profitability are moderate, which reflects the consistent but inefficient asset allocation typical of public sector businesses. Despite maintaining minimum cybersecurity investment for operational continuity, AM/NS India shows negative net profit and ROA, indicating financial hardship and underutilization of assets. Overall, the table shows that rather than being a direct driver of short-term profitability, cybersecurity spending primarily serves as a risk-mitigation and stability-enhancing investment, and that operational management, cost control, and market conditions have a greater impact on asset efficiency and financial performance in the steel industry than does cybersecurity spending alone.

6.Hypothesis Testing (Correlation Analysis)

- **Cybersecurity Expenditure vs Return on Assets (ROA)** :
  - H_0 (Null Hypothesis): There is no significant relationship between cybersecurity expenditure and ROA in steel companies.
  - H_1 (Alternative Hypothesis): There is a significant positive relationship between cybersecurity expenditure and ROA in steel companies.

Observation from Data:

- Tata Steel and JSW Steel have high estimated cybersecurity expenditure but low ROA due to large asset bases and capital-intensive operations.
- Jindal Steel & Power Ltd. Has moderate cybersecurity expenditure but the highest ROA.
- AM/NS India reports negative ROA even with minimum cybersecurity investment.

Conclusion:

There is no consistent positive relationship between cybersecurity expenditure and ROA.

Decision:

H_0 accepted, H_1 rejected.

- **Cybersecurity Expenditure vs Return on Equity (ROE) :**

- H_0 (Null Hypothesis): There is no significant relationship between cybersecurity expenditure and ROE in steel companies.
- H_2 (Alternative Hypothesis): There is a significant positive relationship between cybersecurity expenditure and ROE in steel companies.

Observation from Data:

- Companies with higher cybersecurity spending do not consistently show higher ROE.
- ROE is more influenced by operational efficiency, leverage, and market conditions rather than cybersecurity investment.
- Some firms with moderate cybersecurity expenditure (e.g., Jindal Steel & Power Ltd.) show better equity returns than those with higher spending.

Conclusion:

Cybersecurity expenditure does not significantly affect ROE.

Decision:

H_0 accepted, H_2 rejected.

7. CONCLUSION

This study looked at the relationship between cybersecurity spending and financial performance in a few Indian steel businesses as determined by Return on Equity (ROE) and Return on Assets (ROA). The results show that there is no discernible positive correlation between cybersecurity spending and ROA or ROE. While businesses with modest cybersecurity expenditure, like Jindal Steel & Power Ltd., attained comparatively improved

financial efficiency, companies with higher anticipated cybersecurity spending, like Tata Steel and JSW Steel, did not consistently show superior asset or equity returns. This suggests that rather than being a direct source of short-term profitability, cybersecurity spending mostly serves as an investment focused on risk mitigation and stability.

Overall, the study finds that factors including asset utilization, cost management, capital structure, and market circumstances have a greater impact on financial performance in the steel business than does the amount of money spent on cybersecurity. Nonetheless, investing in cybersecurity is still crucial for safeguarding digital infrastructure, maintaining business continuity, and averting possible financial and reputational damages. To better capture the long-term and indirect financial advantages of cybersecurity investment, future study may include econometric analysis, longer time-series data, and firm-level cybersecurity disclosures.

8. REFERENCES

1. Al-Amosh, H., & Khatib, S. F. A. (2024). The relationship between cybersecurity disclosure and financial performance. ResearchGate.
2. Arcelor Mittal Nippon Steel India Ltd. (2025). Annual financial statements 2024–25. AM/NS India.
3. Bharadwaj, A. S., Bharadwaj, S. G., & Konsynski, B. R. (1999). Information technology effects on firm performance as measured by Tobin's q. Management Science, 45(7), 1008–1024. https://doi.org/10.1287/mnsc.45.7.1008
4. EOXS. (2025). The importance of cybersecurity in steel manufacturing. EOXS Blog.
5. Equity master. (2025). Company financial analysis and balance sheet data. Equitymaster Research.
6. Ernst & Young Global Limited. (2023). Cybersecurity in mining and metals: Managing the risk. EY India.
7. Fortune Business Insights. (2025). Industrial cybersecurity market size, share & industry analysis, 2032. Fortune Business Insights.
8. Gordon, L. A., Loeb, M. P., & Sohail, T. (2010). Market value of voluntary disclosures concerning information security. MIS Quarterly, 34(3), 567–594.
9. IBM Security. (2024). Cost of a data breach report 2024: The industrial sector. IBM Corporation.
10. Investopedia. (2024). Return on assets (ROA) and profitability in manufacturing. Investopedia.
11. Jindal Steel & Power Limited. (2024). Annual report 2023–24. JSPL.
12. JSW Steel Limited. (2025). Annual report 2024–25. JSW Steel Ltd.
13. Kumar, R. (2023). Financial performance of selected companies of iron and steel industry in India. International Journal of Management.
14. Masoud, N., & Al-Utaibi, S. (2022). Cybersecurity risk disclosure and firm value. Journal of Corporate Accounting.

15. Money control. (2025). Financial performance and ratio analysis of Indian steel companies. Money control.
16. National Institute of Standards and Technology. (2020). Framework for improving critical infrastructure cybersecurity. U.S. Department of Commerce.
17. Ponemon Institute. (2023). The state of industrial cybersecurity. Ponemon Institute Research.
18. Romanosky, S. (2020). Examining the costs and causes of cyber incidents. Journal of Cybersecurity.
19. Smart-Investing. (2025). Return on assets (ROA) ratios of Indian steel companies. Smart-Investing.in.
20. Steel Authority of India Limited. (2025). Annual report 2024–25. SAIL.
21. SUERF. (2023). Cybersecurity and financial stability: A public good perspective. The European Money and Finance Forum.
22. Tata Steel Limited. (2025). Annual report 2024–25. Tata Steel Ltd.
23. Value Investing.io. (2025). Financial ratios database for Indian listed companies. Value Investing.io.