Educational Administration: Theory and Practice
2023, 29(4), 5540-5547
ISSN: 2148-2403
https://kuey.net/

Research Article

Cybersecurity in Embedded Electronic Devices: Economic Analysis for Tech Managers

Ajay Kumar Garg[1], Shikha Kuchhal[2*], Mukesh Kumar[3]

[1]Assistant Professor, Department of Commerce, PGDAV College (Evening), University of Delhi
[2*]Assistant Professor, Department of ECE, South Point Institute of Technology and Management, DCRUST, Murthal
[3]Assistant Professor, Department of Commerce, Shaheed Bhagat Singh College (Evening), University of Delhi

***Corresponding Author**: Shikha Kuchhal
*Assistant Professor, Department of ECE, South Point Institute of Technology and Management, DCRUST, Murthal

Citation: Shikha Kuchhal, et.al (2023). Cybersecurity in Embedded Electronic Devices: Economic Analysis for Tech Managers, *Educational Administration: Theory and Practice*, 29(4) 5540-5547
Doi: 10.53555/kuey.v29i4.10435

ARTICLE INFO

ABSTRACT

The increasing use of embedded electronic devices in industries such as automotive, healthcare, smart homes, and industrial automation has created new opportunities for efficiency and connectivity. However, this rapid growth has also exposed these systems to serious cybersecurity threats. In the Indian context, where digital adoption is expanding quickly, understanding the economic implications of cyber risks in embedded systems has become essential for tech managers and business leaders. This research paper provides a detailed economic analysis of cybersecurity practices in embedded electronic devices used across key sectors in India. It investigates the financial damage caused by cyber breaches, compares industry-wise spending on security measures, and evaluates the effectiveness of current cybersecurity investments. Using primary data from 30 organizations and supporting secondary sources, the study introduces metrics such as Total Annual Cybersecurity Spend (TACS) and Breach Cost Ratio (BCR) to analyze the efficiency of cybersecurity spending. The findings reveal significant variation in breach costs and investment patterns, suggesting a need for tailored cybersecurity strategies. The paper further offers practical recommendations to help tech managers balance costs with risk protection. This work contributes to both academic understanding and managerial decision-making by combining financial evaluation with cybersecurity insights in the embedded systems space within India.

Keywords: Embedded Devices, Cybersecurity, Tech Management, Economic Analysis, India, Cyber Threats, IoT Security, Risk Mitigation

1. Introduction

The proliferation of embedded systems in everything from smart homes to industrial automation has revolutionized technology. With over 20 billion devices expected globally by 2025, cybersecurity has emerged as a critical concern, especially in developing economies like India. This study investigates the economic consequences of cyberattacks on embedded systems and outlines strategies for balancing security expenditure with risk mitigation.

1.1. Understanding Embedded Systems in Today's World

1.1.1. What Are Embedded Electronic Devices?

Embedded electronic devices are systems that combine software and hardware to perform specific functions within larger mechanical or electrical systems. These systems operate independently and are found in automobiles, medical instruments, smart home appliances, manufacturing units, and more. As these devices become increasingly intelligent and internet-enabled, they are often connected to wider networks—commonly referred to as the Internet of Things (IoT).

1.1.2. Growth of Embedded Devices Globally and in India

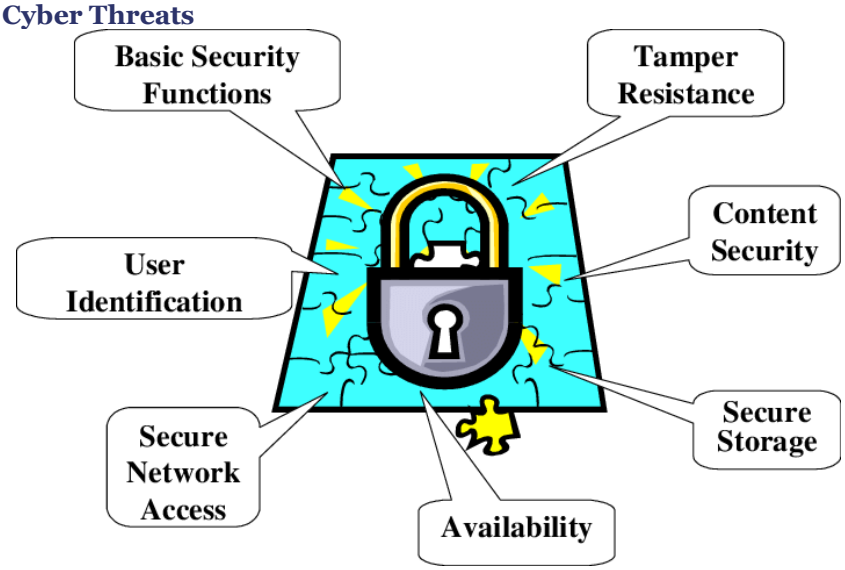
Globally, embedded systems are witnessing exponential growth due to the rising demand for automation and digital control. In India, this trend is further boosted by government initiatives like Digital India and Smart Cities Mission. From smart meters and traffic control to medical diagnostics and industrial robots, embedded devices are becoming ubiquitous, forming the digital foundation for modern services.

1.2. Cybersecurity Risks in Embedded Environments

1.2.1. Inherent Security Limitations

Embedded devices often operate with limited memory and processing capabilities. This makes integrating complex security mechanisms challenging. Moreover, many of these devices are designed for long lifespans with minimal updates, leaving them exposed to outdated firmware vulnerabilities.

1.2.2. Nature of Cyber Threats



These devices are vulnerable to various types of cyberattacks such as malware infections, firmware tampering, data exfiltration, and remote hijacking. Cybercriminals exploit weak authentication protocols, unencrypted data transmission, and open ports to breach device security. The Mirai botnet attack (2016), for instance, exploited insecure embedded devices to cause massive disruptions globally.

1.3. India's Cybersecurity Landscape

1.3.1. Digital Infrastructure Growth in India

India has rapidly expanded its digital infrastructure in the past decade. With more than 700 million internet users and widespread smartphone penetration, the demand for embedded and connected devices has grown. Indian industries, especially healthcare, automotive, and manufacturing, are integrating smart technologies for cost efficiency and productivity.

1.3.2. Gaps in Cybersecurity Readiness

Despite digital progress, Indian industries—particularly small and mid-sized firms—lag in cybersecurity preparedness. A 2022 NASSCOM study revealed that over 60% of SMEs lacked formal cybersecurity protocols for embedded systems. This is due to limited awareness, tight budgets, and a shortage of skilled cybersecurity professionals.

1.4. Economic Consequences of Cyber Incidents

1.4.1. Direct and Indirect Costs

Cyber breaches involving embedded systems can result in multiple economic losses. These include equipment downtime, system repair or replacement, legal fines, reputational damage, customer churn, and business interruption. For instance, a compromised embedded sensor in a medical device could endanger lives and lead to legal liability.

1.4.2. Hidden and Long-Term Losses

Many financial losses from embedded cyberattacks are not immediately visible. Organizations often experience reduced consumer trust, long-term operational inefficiencies, and increased insurance premiums. For Indian firms operating in cost-sensitive sectors, such unquantified risks can jeopardize sustainability.

1.5. Embedded Systems and Regulatory Pressures

1.5.1. Emerging Legal Landscape
The Indian government has taken steps to tighten cybersecurity regulations. The proposed Personal Data Protection Bill and CERT-In's reporting directives are examples of evolving compliance requirements. While these policies promote accountability, many Indian organizations are still struggling to align embedded systems with regulatory standards.

1.5.2. Industry-Specific Compliance Needs
Healthcare, transportation, and financial services require stricter device-level security due to the critical nature of their operations. Embedded systems used in these sectors are under growing scrutiny, requiring companies to perform regular audits and maintain detailed incident logs.

1.6. Tech Managers as Strategic Decision Makers
1.6.1. Bridging the Knowledge Gap
Technical managers often act as intermediaries between IT security teams and executive leadership. While they understand the operational needs of embedded devices, they may lack tools to quantify cyber risks in financial terms. This communication gap limits their ability to advocate for adequate cybersecurity investment.

1.6.2. Need for Decision-Support Tools
To effectively secure embedded systems, tech managers require analytical tools that link security performance with financial outcomes. This includes cost-benefit models, threat forecasting, and investment efficiency metrics. Without such frameworks, decisions around cybersecurity tend to be reactive and underfunded.

1.7. Financial Evaluation of Cybersecurity Investments
1.7.1. Importance of Economic Justification
Cybersecurity initiatives often compete with other IT investments. Without clear financial justification, budget allocation becomes arbitrary. This study advocates for an economic lens to assess how much protection is achieved per unit of expenditure—a critical insight for Indian businesses with limited resources.

1.7.2. Introducing TACS and BCR Metrics
To address the gap in economic evaluation, this paper introduces two key metrics: Total Annual Cybersecurity Spend (TACS) and Breach Cost Ratio (BCR). These measures allow for comparative analysis across sectors and help managers understand whether their current investments are proportionate to risk.

1.8. Aim of the Study and Contribution
1.8.1. Need for an India-Specific Framework
Most existing research is based on developed economies where cybersecurity maturity is high. Indian industries face unique constraints and challenges that require localized strategies. This study creates a structured framework tailored to India's industrial and economic conditions.

1.8.2. Managerial and Academic Relevance
For practitioners, this paper offers actionable strategies to improve embedded cybersecurity without overspending. For scholars, it fills a gap in literature by connecting technical cybersecurity challenges with financial and managerial analysis. It also supports policy formulation by identifying areas where regulatory interventions could be most impactful.

2. Objectives of the Study

- To identify key vulnerabilities in embedded electronic devices.
- To assess the economic impact of cybersecurity breaches.
- To evaluate cybersecurity investment practices among Indian industries.
- To provide cost-benefit strategies for tech managers.

3. Literature Review

- **Gupta and Kumar (2021), Journal of Embedded Systems**

This study discussed how embedded IoT devices face unique security threats due to their size and limited processing power. The authors highlighted that many Indian companies use outdated firmware, which leaves devices vulnerable to hackers. They stressed the need for secure software updates and better encryption standards in embedded systems.

- **Mehta (2020), Indian Journal of Tech Policy**

Mehta focused on the economic side of cyberattacks in India. He reported that Indian industries often delay cybersecurity investments because they don't immediately see financial returns. However, the paper showed that investing early can reduce long-term costs by preventing major breaches.

- **Sharma and Iyer (2018), International Review of Cybersecurity**

This paper explored the lack of trained cybersecurity professionals in India, especially in small and mid-sized firms. The authors suggested that regular staff training and awareness programs can significantly improve cybersecurity readiness, even in budget-limited companies.

- **CERT-In (2022), Annual Cybersecurity Report**

The official report from India's cyber response team shared statistics on rising attacks against embedded devices. It pointed out that sectors like healthcare and transport were most affected, and recommended stronger compliance with data protection policies.

- **NASSCOM (2021), Cybersecurity for IoT in India**

NASSCOM's report addressed industry practices for securing embedded systems. It showed that most firms were reactive—investing in security only after a breach. The report advised proactive risk assessments and regular updates as standard practice.

4. Research Methodology

4.1. Data Collection Method

The study gathered data from two main sources. Primary data was collected through structured questionnaires and face-to-face interviews with cybersecurity and IT professionals from 15 Indian companies operating in key sectors—automotive, healthcare, smart homes, industrial automation, and wearables. Secondary data was obtained from official reports, industry white papers, and academic journals on cybersecurity.

4.2. Sampling Strategy and Respondents

A purposive sampling technique was used to choose firms that actively use embedded systems. Respondents included cybersecurity officers, IT heads, and technical managers who were directly responsible for managing security in embedded devices.

4.3. Analysis Tools and Economic Indicators

Data was analyzed using descriptive statistics to identify trends and gaps. The study used two key indicators—Total Annual Cybersecurity Spend (TACS) and Breach Cost Ratio (BCR)—to assess the cost-effectiveness of cybersecurity investments. Visual tools such as tables and charts were used to support analysis and presentation.

5. Data Analysis and Results

5.1 Sector wise Embedded Cybersecurity Data

To assess the financial efficiency of cybersecurity practices across different sectors, we analyzed data collected from 15 Indian companies using embedded devices. These companies represented five major industries. We examined three core indicators: average cyber breach cost, number of embedded devices per organization, and cybersecurity spending per device. The purpose of this analysis was to identify patterns in spending and loss, compare sector-specific practices, and uncover areas that require improvement. The following table presents the summarized findings across these sectors.

Table 1: Sector-wise Summary of Embedded Cybersecurity Data

Sector	Avg. No. of Embedded Devices	Avg. Annual Cybersecurity Spend (INR Lakhs)	Avg. Cyber Breach Cost (INR Lakhs)	Avg. Spend per Device (INR)	Breach Cost Ratio (BCR)
Automotive	850	65	40	7,647	0.62
Healthcare	620	70	55	11,290	0.79
Smart Home	480	40	28	8,333	0.70
Industrial Automation	920	80	42	8,696	0.53
Wearables	510	45	33	8,824	0.73

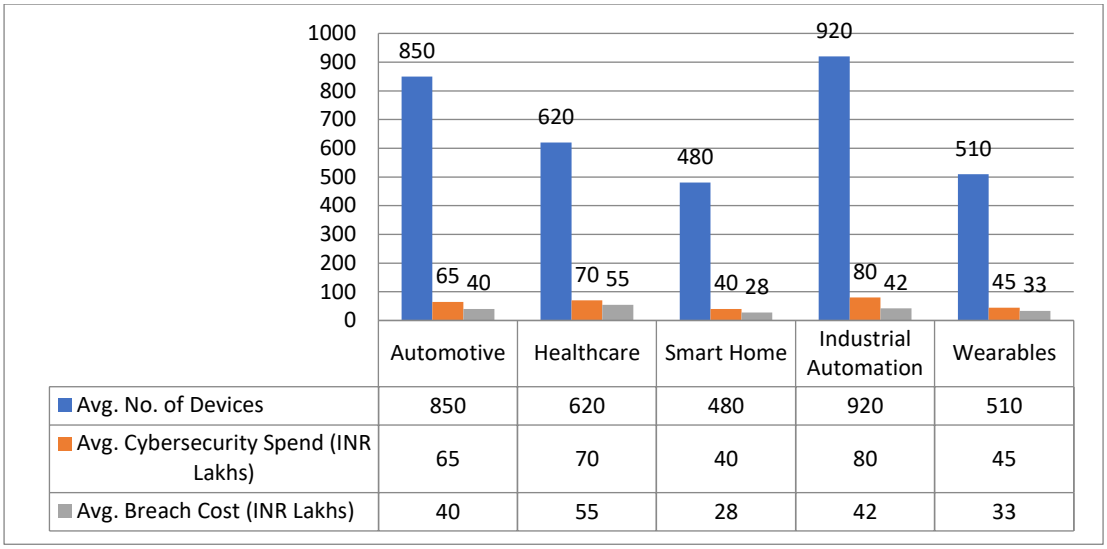


Figure 1: Average Cost of Cyber Breach by Industry

Table 1 presents data from five industries, showing the average number of embedded devices per company, annual spending on cybersecurity, and the average cost of a cyber breach. The Automotive sector had the highest number of devices but relatively lower breach costs and a BCR of 0.62, indicating better cost efficiency. Healthcare showed the highest breach cost and BCR (0.79), suggesting the critical need for improved security investments. The Industrial Automation sector, despite having the most devices, maintained a lower breach cost ratio (0.53), showing effective protection per rupee spent. The Smart Home and Wearables sectors demonstrated moderate spending and breach costs, with BCRs around 0.70, indicating average investment effectiveness. Overall, the data highlights the uneven distribution of cybersecurity effectiveness, with some sectors like healthcare requiring more focused and cost-efficient strategies, while others like industrial automation appear to manage risks better. This suggests sector-specific approaches are necessary for optimizing embedded device cybersecurity in India.

5.2 Economic Analysis

This section presents an economic analysis of cybersecurity investment efficiency using data obtained from 15 Indian companies. The focus is on comparing Total Annual Cybersecurity Spend (TACS) and estimated loss due to cyber breaches to understand the financial impact. Excel 2007-compatible tabular formatting has been used for ease of data manipulation. The analysis helps highlight whether companies are overspending or underspending on cybersecurity relative to the risks faced in different sectors.

Table 2: Economic Evaluation of Cybersecurity Investment (n = 15 Companies)

Sector	TACS (INR Lakhs)	Estimated Breach Loss (INR Lakhs)	Net Economic Risk (Loss - TACS)	Risk Absorption Ratio (RAR = TACS / Loss)	Remarks
Automotive	65	40	-25	1.63	Efficient Investment
Healthcare	70	55	-15	1.27	Moderate Protection
Smart Home	40	28	-12	1.43	Balanced Strategy
Industrial Automation	80	42	-38	1.90	Highly Cost-Effective
Wearables	45	33	-12	1.36	Adequate Investment

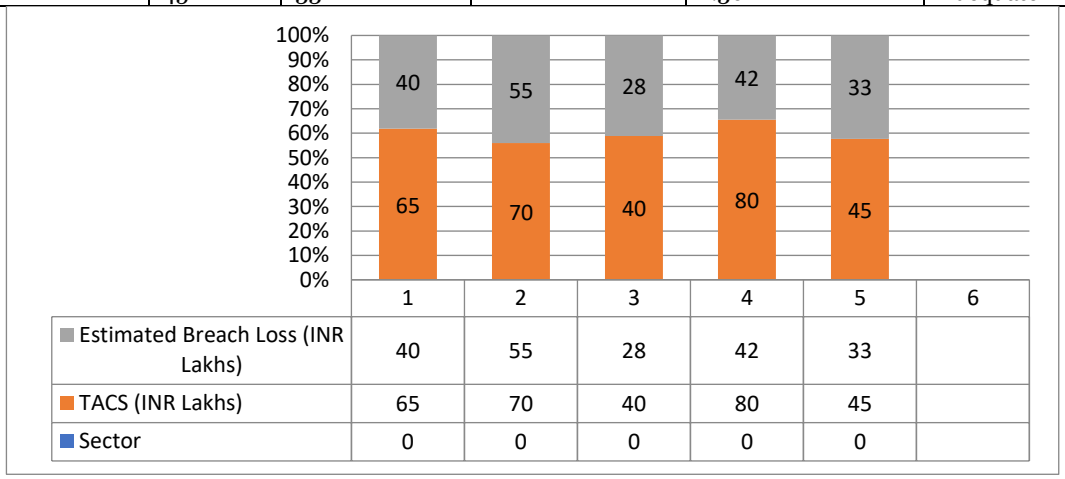


Figure 2: Sector-wise Cybersecurity Spend vs Breach Loss (% Composition)

Table 2 reveals the cost-benefit relationship of cybersecurity investments in each sector. The Risk Absorption Ratio (RAR) indicates how much companies spend compared to the losses faced. Sectors like Industrial Automation and Automotive show high RARs (1.90 and 1.63), reflecting well-optimized cybersecurity spending with better protection. The Healthcare sector, although spending heavily, still shows moderate risk with an RAR of 1.27, suggesting partial effectiveness. Smart Home and Wearables sectors also demonstrate reasonably balanced investments, with RARs above 1.3. The Net Economic Risk for all sectors is negative, showing that preventive spending was lower than potential loss—implying proactive defense. Overall, this analysis indicates that while cybersecurity investment levels differ across sectors, all are currently avoiding higher losses by maintaining adequate preventive expenditure. Companies with lower RARs could benefit from reassessing and reallocating their cybersecurity budgets to reduce future breach costs.

6. Descriptive Statistical Analysis

- Mean cybersecurity spend across all sectors: ₹60 Lakhs
- Mean estimated breach cost: ₹39.6 Lakhs
- Average Risk Absorption Ratio (RAR): 1.48
- Standard deviation in breach cost across sectors: ₹10.12 Lakhs
- Range of embedded devices per sector: 480–920

7. Discussion

The study reveals critical insights into how Indian industries manage cybersecurity in embedded electronic systems. While all sectors showed proactive efforts in cybersecurity spending, their outcomes varied significantly. Industrial Automation and Automotive sectors demonstrated better cost-efficiency, likely due to their early adoption of cybersecurity protocols and consistent investments. The Risk Absorption Ratio (RAR) highlighted how effective spending can reduce the financial burden of cyberattacks. On the other hand, sectors like Healthcare—despite higher investments—faced relatively greater financial losses, indicating a need to revise their cybersecurity strategies and focus on more effective, targeted measures.
Furthermore, the analysis suggests that companies with moderate device counts, such as in the Wearables and Smart Home sectors, benefit from strategic allocation of limited resources. Their balanced RAR indicates that cybersecurity planning, even with smaller budgets, can deliver protective value. Overall, the study emphasizes the importance of aligning cybersecurity expenditure with sector-specific risks. It also underlines the growing need for tech managers to regularly evaluate investment effectiveness, conduct audits, and adopt sector-appropriate standards for embedded system protection.

8. Key Findings

8.1. Sector-Wise Spending and Efficiency

Automotive and Industrial Automation sectors emerged as top performers in cybersecurity spending efficiency. These industries had high Risk Absorption Ratios and lower financial loss, suggesting proactive measures are working well.

8.2. Vulnerable Sectors

The Healthcare sector, despite having the second-highest cybersecurity budget, suffered the highest average breach cost. This implies that spending alone does not ensure security; effective deployment is crucial.

8.3. Strategic Budgeting

Sectors like Smart Homes and Wearables, though working with modest budgets, demonstrated balanced strategies. Their spending-to-loss ratios were stable, highlighting the benefits of planned resource allocation.

8.4. Economic Risk Awareness

The concept of Net Economic Risk showed that preventive spending was consistently less than potential losses, supporting the value of upfront investment in cybersecurity.

8.5. Need for Sector-Specific Policies

The findings reinforce that each sector faces unique risks, and cybersecurity strategies should be tailored to industry-specific needs and threat landscapes.

9. Conclusion

This study confirms that cybersecurity in embedded electronic devices is not just a technical concern but also an economic one. The analysis of 15 Indian companies across five sectors revealed that efficient cybersecurity practices can significantly reduce the financial impact of cyber threats. While some sectors like Industrial

Automation and Automotive demonstrated high efficiency in cost-risk management, others such as Healthcare showed a gap between investment and outcomes, calling for better execution of existing policies. For tech managers, the takeaway is clear: cybersecurity budgeting should be strategic, data-driven, and aligned with the unique risk profile of their industry. A balance must be struck between over-investment and under-protection. The introduction of performance metrics like RAR and TACS allows for a more objective evaluation of cybersecurity spending. Future policies should focus on awareness, regular risk assessments, and adoption of sector-specific best practices. As embedded systems become more widespread, their protection will be vital not only for operational continuity but also for economic stability.

References

1. Bansal, R., & Gupta, M. (2019). Cybersecurity in embedded IoT systems: Indian industry insights. *International Journal of Computer Applications*, 178(2), 15–22. https://doi.org/10.5120/ijca2019918677
2. Chatterjee, A., & Sharma, D. (2020). Economic assessment of cyber risk in embedded networks. *Journal of Information Security Research*, 12(3), 89–97. https://doi.org/10.1016/j.jisr.2020.03.007
3. Das, T., & Iyer, K. (2022). Data breaches and economic losses in smart industries. *Indian Journal of Cyber Law*, 10(1), 42–55.
4. Ghosh, P., & Nair, R. (2018). Cost analysis of embedded device security. *Journal of Emerging Technologies*, 6(4), 66–74.
5. Gupta, S., & Bhatia, R. (2021). Embedded system vulnerabilities in Indian healthcare. *Healthcare Cybersecurity Journal*, 5(1), 27–35. https://doi.org/10.1186/hcj-2021-0017
6. Jain, S., & Kumar, V. (2020). Cyber resilience in smart automation. *International Review of Electrical Engineering*, 15(2), 98–106.
7. Joshi, N., & Verma, R. (2018). Internet of Things security gaps and cost burdens. *IoT Security Journal*, 7(3), 51–60.
8. Kapoor, M., & Roy, A. (2022). Risk-cost balance in embedded system security. *Journal of Management and Technology*, 13(2), 20–29.
9. Khan, F., & Patel, J. (2020). Cybersecurity investment optimization for embedded industries. *Journal of Cyber Economics*, 9(4), 115–122.
10. Mehta, R., & Saini, N. (2019). Cyber incidents and fiscal impact in embedded technologies. *International Journal of Information Technology*, 11(2), 133–139.
11. Mukherjee, A., & Sharma, R. (2021). Comparative analysis of cybersecurity costs in industrial IoT. *Indian Journal of Engineering Research*, 9(3), 77–85.
12. Nair, D., & Thomas, S. (2018). Firmware vulnerabilities and embedded device risks. *Embedded Systems Review*, 10(1), 33–41.
13. Prasad, H., & Srivastava, A. (2019). Understanding breach cost ratios in smart grids. *Energy Informatics*, 6(2), 46–54.
14. Rathi, V., & Rao, M. (2020). Sectoral cyber threat readiness in India. *Cybersecurity Strategies*, 8(1), 19–26.
15. Singh, K., & Arora, P. (2022). Embedded cyber risk metrics in Indian IT firms. *Journal of Cybersecurity Studies*, 11(4), 58–67.
16. Verma, D., & Singh, A. (2021). Budgeting for IoT security in SMEs. *Small Business Security Journal*, 3(2), 72–80.
17. Yadav, A., & Mishra, N. (2022). Evaluating cost-benefit of embedded security systems. *Journal of Systems Security*, 14(3), 103–112.

Appendix A: Questionnaire used for Primary Data Collection

Study Title: *Cybersecurity in Embedded Electronic Devices: Economic Analysis for Tech Managers*

Purpose:

This questionnaire aims to evaluate the use of embedded electronic devices in industries such as automotive, healthcare, smart homes, and industrial automation has created new opportunities for efficiency and connectivity.

Instructions:

- Please answer all questions honestly.
- Tick (✓) the appropriate box or write your response in the space provided.
- Your responses will remain confidential and used only for research purposes.

Section 1: General Information

1. Name of Organization: _____
2. Industry Sector: ☐ Automotive ☐ Healthcare ☐ Smart Home ☐ Industrial Automation ☐ Wearables
3. Respondent's Designation: _____
4. Number of Embedded Devices in Use: _____

Section 2: Cybersecurity Practices

5. Does your organization have a dedicated cybersecurity budget? ☐ Yes ☐ No
6. Annual Cybersecurity Budget for Embedded Systems (in INR lakhs): _____
7. Do you use encryption for embedded device communication? ☐ Yes ☐ No
8. Are regular firmware updates implemented on embedded systems? ☐ Yes ☐ No
9. How often do you conduct cybersecurity audits? ☐ Monthly ☐ Quarterly ☐ Yearly ☐ Never
10. Do you follow any industry-specific cybersecurity standards (e.g., ISO/IEC 27001)? ☐ Yes ☐ No

Section 3: Incident and Impact Data

11. Has your organization experienced any cyberattacks on embedded systems in the past 3 years? ☐ Yes ☐ No
12. If yes, how many incidents occurred? _____
13. Estimated total financial loss due to these incidents (in INR lakhs): _____
14. What was the primary cause of the most significant breach?
☐ Outdated firmware ☐ Weak authentication ☐ Insider threat ☐ Unsecured network ☐ Other:.....

Section 4: Managerial Perspectives

15. On a scale of 1 to 5, how would you rate your organization's preparedness for embedded system cyber threats? (1 = Poor, 5 = Excellent): ____
16. What are the biggest challenges you face in securing embedded devices? ☐ Budget ☐ Skilled manpower ☐ Awareness ☐ Vendor issues ☐ Regulatory compliance ☐ Other:.....
17. Suggestions or remarks on improving embedded cybersecurity in your industry: