International Journal of Emerging Research in Computer Science
©IJERCS | Volume 1 | Issue 1 | December 2025 | ISSN: 3139-101X (Online)
Available online at: https://ijercs.com/

Cybersecurity as an Economic Public Good: Challenges for Emerging Economies

Dr. Sangeeta Shashikant Shinde✉
Professor, Department of Economics, Sarhad College of Arts, Commerce and Science, Katraj Pune, SPPU. Maharashtra, India

Received: 06 December 2025 | **Accepted:** 12 December 2025 | **Published:** 15 December 2025

Abstract

The rapid expansion of digital technologies has fundamentally transformed economic systems across the world. In emerging economies, digitalization has accelerated financial inclusion, service delivery, and market integration, but it has also generated new forms of systemic risk in the form of cyber threats. This chapter conceptualizes cybersecurity as an economic public good and examines why market mechanisms alone are insufficient to ensure adequate levels of digital security. Drawing upon economic theory, real-world incidents, and policy experience from emerging economies, the chapter analyses cybersecurity through the lenses of externalities, market failure, coordination problems, and state intervention. It argues that underinvestment in cybersecurity poses serious risks to economic stability, financial systems, and inclusive growth. The chapter concludes by proposing policy measures that emphasize collective action, public–private cooperation, institutional capacity building, and international coordination to strengthen cybersecurity governance in emerging economies.

Keywords: *Cybersecurity, Public Goods, Economic Security, Emerging Economies, Digitalization.*

1. Introduction

Digital technologies have become a central driver of economic transformation. Banking, trade, education, healthcare, and public administration increasingly depend on digital platforms and networked systems. For emerging economies, digitalisation has played a crucial role in expanding access to financial services, improving governance efficiency, and integrating domestic markets with global value chains. Initiatives such as digital payments, online public services, and e-commerce platforms have significantly lowered transaction costs and widened participation in economic activity.

However, the same digital infrastructure that enables economic growth also introduces vulnerabilities. Cyber threats such as ransomware attacks, data breaches, identity theft, and disruptions of critical infrastructure have become frequent and costly. These risks are not confined to individual users or organisations; instead, they often produce

economy-wide consequences. A cyber incident affecting a financial institution, a public service platform, or a digital payments network can undermine trust, disrupt markets, and generate spillover effects across sectors.

In emerging economies, these challenges are intensified by uneven digital literacy, limited institutional capacity, and resource constraints. This chapter argues that cybersecurity should not be treated solely as a private or technical concern, but rather as an economic public good requiring coordinated policy intervention and collective responsibility.

2. Conceptualizing Cybersecurity as an Economic Public Good

In economic theory, public goods are defined by two key characteristics: non-excludability and non-rivalry. Cybersecurity exhibits these characteristics to a considerable extent. Once a secure digital environment is established, all participants in the network benefit from reduced risk, regardless of their individual level of investment. One user's protection does not diminish the security available to others, and it is difficult to exclude non-paying users from the benefits of a secure digital ecosystem.

Cybersecurity also generates significant positive externalities. When banks, payment systems, or government platforms adopt strong security practices, the resulting reduction in systemic risk benefits the broader economy. Conversely, weak security in one part of the network can expose others to harm. The global WannaCry ransomware attack of 2017 illustrates this dynamic clearly. The attack exploited a common software vulnerability and disrupted hospitals, transport systems, and enterprises across multiple countries. Even organizations with relatively strong internal controls were affected because security failures at the network level imposed costs on all users.

From an economic perspective, this leads to underinvestment. Private firms tend to invest in cybersecurity only up to the level that protects their own interests, ignoring the wider social benefits of enhanced security. This divergence between private incentives and social welfare constitutes a classic case of market failure, providing a strong rationale for public intervention (Arrow, 1962; Stiglitz, 1999).

3. Digitalization and Rising Cyber Risks in Emerging Economies

Emerging economies have experienced rapid growth in digital infrastructure and services. Digital payment systems, mobile banking, and e-governance platforms have expanded access to services for previously excluded populations. India's Unified Payments Interface (UPI), for example, has become one of the world's largest real-time payment systems, facilitating billions of transactions annually and supporting financial inclusion.

At the same time, the expansion of digital services has increased exposure to cyber risks. Phishing attacks, digital fraud, and identity theft have grown alongside the user base, particularly affecting first-time and digitally inexperienced users. Regulatory enforcement mechanisms and security awareness have often lagged behind technological adoption, creating vulnerabilities that can be exploited at scale.

The economic implications extend beyond individual losses. Widespread cyber incidents can erode trust in digital systems, slow adoption, and undermine public confidence in innovation-led growth strategies. In this sense, cybersecurity failures threaten not only individual users but also broader development objectives.

4. Vulnerability of Small and Medium Enterprises

Small and medium enterprises (SMEs) form the backbone of most emerging economies, contributing significantly to employment and income generation. However, SMEs often rely on basic digital tools and lack the resources to invest in advanced cybersecurity measures. Unlike large corporations, they typically do not have dedicated security teams, insurance coverage, or robust recovery mechanisms.

Empirical evidence suggests that cyber incidents affecting SMEs frequently lead to temporary shutdowns, financial distress, and loss of customer trust. These effects can cascade through supply chains, disrupt local employment, and reduce regional economic activity. From a macroeconomic perspective, widespread SME vulnerability amplifies the systemic nature of cyber risk and reinforces the argument for collective solutions.

5. Economic Costs of Cyber Insecurity

Cyber insecurity imposes both direct and indirect economic costs. Direct costs include financial losses from fraud, ransom payments, system downtime, and recovery expenses. Indirect costs are often more substantial and persistent, encompassing reputational damage, reduced consumer confidence, and lower levels of investment and innovation.

Studies across banking and e-commerce sectors consistently show that major data breaches are followed by declines in market valuation and customer engagement. In emerging economies, where trust in digital systems is still evolving, such incidents can have disproportionate effects. Reduced trust increases transaction costs and discourages participation in digital markets, undermining efficiency and growth.

6. Cybersecurity and Financial Stability

Cyber risks have increasingly been recognised as a threat to financial stability. Central banks and financial regulators now acknowledge that cyber incidents can disrupt payment and settlement systems, impair interbank confidence, and create systemic shocks comparable to traditional financial risks.

Even temporary disruptions to digital payment infrastructure can have wide-ranging economic consequences, particularly in cash-light economies. As financial systems become more interconnected and technology-dependent, cybersecurity emerges as a core component of macroeconomic stability rather than a peripheral technical issue.

7. Role of the State in Cybersecurity Provision

Given the public good nature of cybersecurity, the role of the state is indispensable. Governments are uniquely positioned to address market failures by setting standards, enforcing compliance, and coordinating

responses across sectors. Public institutions such as national computer emergency response teams, sector-specific regulators, and data protection authorities play a central role in this process.

In India, for instance, frameworks issued by the Reserve Bank of India for banks and payment systems, along with the activities of CERT-In, illustrate how regulatory oversight and institutional coordination can strengthen digital resilience. Mandatory reporting requirements, security audits, and awareness campaigns help internalise externalities and raise overall security standards.

8. Coordination Failures and Information Asymmetry

A persistent challenge in cybersecurity governance is the reluctance of private firms to disclose cyber incidents due to reputational concerns. Under-reporting delays collective response, limits learning, and increases systemic vulnerability. This information asymmetry weakens market efficiency and reinforces the need for regulatory reporting mechanisms and trusted information-sharing platforms.

Public–private partnerships can play a crucial role in overcoming coordination failures by facilitating knowledge exchange, joint preparedness exercises, and shared investment in security infrastructure.

9. Human Capital and Skill Constraints

Many emerging economies face acute shortages of skilled cybersecurity professionals. This skill gap increases reliance on external consultants and raises the cost of security implementation. Limited domestic capacity also constrains the ability of governments to design, monitor, and enforce effective cybersecurity policies.

From an economic perspective, investment in education and training represents a long-term public investment that enhances national resilience and reduces dependence on external expertise.

10. Cybersecurity, Inequality, and Inclusive Growth

Cyber risks do not affect all users equally. Low-income groups, rural populations, senior citizens, and informal workers are often more vulnerable to digital fraud due to limited awareness and access to support mechanisms. Without inclusive cybersecurity policies, digitalisation may exacerbate existing inequalities rather than reduce them.

Treating cybersecurity as a public good ensures that protection is extended across socio-economic groups, supporting inclusive and sustainable growth.

11. Underinvestment and the Free-Rider Problem

Firms frequently invest in cybersecurity only after experiencing a breach, viewing preventive measures as a cost rather than a benefit. However, the social cost of cyber incidents typically exceeds private losses. This behaviour reflects free-rider incentives, a defining feature of public goods, and further justifies collective intervention.

12. Policy Implications and Collective Action

Countries that integrate cybersecurity into national development and financial strategies tend to exhibit stronger digital resilience. Coordinated policy frameworks reduce duplication, improve response times, and enhance accountability. At the international level, cooperation is essential due to the cross-border nature of cyber threats, which share characteristics of a global public good.

12A. Conceptual Framework: Cybersecurity as an Economic Public Good

The conceptual framework below explains cybersecurity from an economic public good perspective, linking digitalisation, market failure, state intervention, and economic outcomes in emerging economies.

Conceptual Flow:

Digitalisation → Increased Cyber Exposure → Market Failure (Externalities & Free-Rider Problem) → Underinvestment in Cybersecurity → Economic Risks (Financial Instability, Trust Deficit, Inequality) → State & Collective Intervention → Strengthened Economic Security

Explanation: - Rapid digitalisation expands economic opportunities but simultaneously increases cyber vulnerabilities. - Individual firms and users underinvest in cybersecurity because benefits are shared across the system. - This results in market failure, leading to systemic economic risks. - Government intervention, regulation, and public–private cooperation correct this failure and enhance economic resilience.

12B. Analytical Tables

Table 1: Cybersecurity as a Public Good – Economic Characteristics

Economic Characteristic	Cybersecurity Context	Economic Implication
Non-rivalry	One entity's security benefits others	Shared economic protection
Non-excludability	Difficult to exclude users from network security	Free-rider problem
Positive externalities	Secure systems reduce systemic risk	Market failure

Table 1 explains why cybersecurity fits within the framework of public goods in economic theory. The non-rival nature of cybersecurity implies that one organisation's investment in secure digital systems does not reduce the level of protection available to others operating within the same network. Instead, it enhances overall system safety. Similarly, cybersecurity exhibits non-excludability, as it is difficult to prevent users from benefiting from a secure digital environment once it is established.

These characteristics give rise to positive externalities, where the social benefits of cybersecurity exceed the private benefits captured by individual firms. As a result, market-driven investment tends to fall short of the socially optimal level. This table provides the theoretical foundation for treating cybersecurity as an economic public good and justifies the need for public policy intervention.

Table 2: Market Failure and Cybersecurity in Emerging Economies

Issue	Economic Explanation	Impact
Underinvestment	Firms ignore social benefits	Increased cyber vulnerability
Information asymmetry	Non-disclosure of breaches	Delayed collective response
Coordination failure	Fragmented security efforts	Systemic risk

Table 2 highlights the key dimensions of market failure that affect cybersecurity outcomes in emerging economies. Underinvestment occurs because private firms focus on immediate costs rather than long-term systemic benefits. Information asymmetry arises when organisations conceal cyber incidents to protect their reputation, thereby limiting collective learning and timely response.

Coordination failure further weakens cybersecurity governance, as fragmented efforts by individual actors fail to address interconnected risks. Together, these factors explain why relying solely on market mechanisms is insufficient and why emerging economies face heightened vulnerability in the absence of coordinated regulatory frameworks.

Table 3: Economic Impact of Cyber Insecurity

Level	Type of Impact	Economic Consequence
Micro	Fraud, data loss	Firm-level financial loss
Meso	SME disruptions	Employment & supply chain impact
Macro	Financial instability	Reduced growth & investor trust

Table 3 presents the multi-level economic consequences of cyber insecurity, ranging from firm-level losses to macroeconomic instability. At the micro level, cyber incidents result in direct financial losses, operational disruptions, and reputational damage for individual firms. At the meso level, particularly among small and medium enterprises, cyber disruptions affect employment, local supply chains, and regional economic activity.

At the macro level, large-scale or repeated cyber incidents can undermine financial stability, reduce investor confidence, and slow economic growth. This table underscores the systemic nature of cyber risk and reinforces the argument that cybersecurity should be addressed as an economy-wide concern rather than an isolated technical issue.

Table 4: Role of the State in Cybersecurity Provision

State Function	Policy Instrument	Economic Outcome
Regulation	Cyber laws, compliance norms	Reduced systemic risk
Investment	National cyber infrastructure	Improved resilience
Coordination	Public–private partnerships	Collective security

Table 4 outlines the economic rationale for state involvement in cybersecurity provision. Regulation through cyber laws and compliance standards helps internalise externalities by aligning private incentives with social welfare. Public investment in national cyber infrastructure enhances resilience and reduces systemic vulnerability, particularly in critical sectors such as banking and public services.

Coordination through public–private partnerships enables information sharing, joint preparedness, and efficient allocation of resources. This table demonstrates how state intervention corrects market failures and strengthens collective security, reinforcing cybersecurity's role as a public good essential for economic stability and development.

13. Conclusion

Cybersecurity has evolved into a fundamental economic concern with far-reaching implications for growth, stability, and equity. Viewing cybersecurity through the lens of public goods highlights the limitations of purely market-driven approaches and underscores the importance of collective action. For emerging economies, strengthening cybersecurity governance is essential to safeguarding the gains of digital transformation and ensuring sustainable economic development.

References

[1]. Arrow, K. J. (1962). Economic welfare and the allocation of resources for invention. Princeton University Press.

[2]. OECD. (2020). Cybersecurity policy frameworks. OECD Publishing.

[3]. Stiglitz, J. E. (1999). Knowledge as a global public good. Global Public Goods, 308–325.

[4]. World Bank. (2021). Digital development and cyber risks. World Bank Publications.

Cite this Article:

Dr. Sangeeta Shashikant Shinde, "Cybersecurity as an Economic Public Good: Challenges for Emerging Economies", ***International Journal of Emerging Research in Computer Science****, Volume 1, Issue 1, pp. 32-38, December 2025.*

Journal URL: *https://ijercs.com/*