International Journal of Science, Strategic Management and Technology
Volume **02** Issue **03** March-**2026** | ISSN: **3108-1762 (Online)** | Impact Factor: 3.8
An International, Peer-Reviewed, Open Access Scholarly Journal Indexed in recognized academic databases

Product Resilience and Accountability in the Era of Ransomware:A Risk-Aware Software Product Management Perspective for Indian Enterprises

Swagatika Samal
Assistant Professor
T. John College, Bengaluru, India

Jeyarani Milton
Assistant Professor
T. John College, Bengaluru, India

https://doi.org/10.55041/ijsmt.v2i3.193

Cite this Article: Milton, J. (2026). Product Resilience and Accountability in the Era of Ransomware:A Risk-Aware Software Product Management Perspective for Indian Enterprises. International Journal of Science, Strategic Management and Technology, *02*(03). https://doi.org/10.55041/ijsmt.v2i3.193

Abstract

Ransomware attacks have emerged as a persistent and economically damaging threat to enterprises operating in increasingly digital and interconnected environments. Indian organizations, particularly those relying on software-intensive business processes, face heightened exposure due to rapid digital transformation, cloud adoption, and limited cyber risk awareness. While existing ransomware research largely concentrates on technical detection and prevention mechanisms, relatively little attention has been paid to ransomware as a product-level risk influencing software design decisions, accountability, and long-term resilience.

This study proposes a **risk-aware software product management perspective** for addressing ransomware threats in Indian enterprises. Using a secondary data-driven approach, the research synthesizes insights from industry reports, national cyber advisories, and documented ransomware incidents to identify key risk drivers and economic consequences. The study introduces a conceptual framework that maps ransomware risks to product management decisions across the software lifecycle, emphasizing resilience, accountability, and cost-sensitive prioritization.

The findings highlight that ransomware resilience is not merely a security feature but a strategic product capability with measurable economic implications. By embedding risk-awareness into product planning and design, software product managers can improve organizational preparedness, justify security investments, and contribute to the stability of India's digital ecosystem. The study aligns with national objectives of building trustworthy, resilient, and accountable digital products.

Keywords

Ransomware Attacks, Software Product Management, Product Resilience, Cybersecurity Risk, Economic Impact, Indian Enterprises

1. Introduction

Ransomware has evolved from opportunistic malware into a structured cybercrime model targeting enterprises across critical sectors. In India, the rapid digitization of business processes, expansion of software platforms, and increasing dependence on data-driven services have significantly expanded the attack surface for ransomware actors. Enterprises affected by ransomware frequently experience prolonged downtime, financial losses, reputational damage, and regulatory challenges.

Traditional approaches to ransomware mitigation emphasize technical controls such as malware detection, endpoint protection, and backup systems. While essential, these measures often overlook the strategic role of software product management in shaping resilience, usability, and accountability. Product managers are required to balance security requirements with cost constraints, user experience, and time-to-market pressures, making ransomware risk a complex product-level challenge.

This paper argues that ransomware should be treated as a **product resilience and accountability problem**, rather than solely a technical security issue. The objective of this study is to propose a conceptual framework that integrates ransomware risk considerations into software product management decisions, with a specific focus on Indian enterprises.

2. Related Work

Ransomware research has predominantly focused on malware behavior analysis, cryptographic mechanisms, and detection techniques. Surveys and empirical studies highlight the growing sophistication of ransomware families and their evolving attack strategies. Parallel research on cybersecurity economics examines breach costs, insurance models, and organizational losses, though these studies often remain high-level and context-agnostic.

From a software product management perspective, security is frequently addressed as a compliance requirement rather than a value-creating capability. Limited work exists that connects ransomware risks to product design trade-offs, lifecycle decisions, and accountability metrics. This gap is particularly evident in emerging economies, where enterprises operate under tighter budgetary and regulatory constraints.

This study contributes to the literature by linking ransomware risk awareness with software product management practices, offering a structured lens to evaluate resilience and accountability in product strategy.

3. Risk-Aware Product Management Framework

This study adopts a qualitative, secondary data-driven methodology. Publicly available industry reports, ransomware incident analyses, and cybersecurity advisories were reviewed to identify recurring risk patterns and economic consequences relevant to software products. The proposed framework aligns ransomware risks with key stages of the software product lifecycle.

The framework identifies four core dimensions of product-level ransomware risk:

1. **Design-Time Risk** – architectural choices, dependency management, and security-by-design considerations
2. **Operational Risk** – exposure arising from deployment environments, configuration practices, and access control.
3. **Economic Risk** – costs related to downtime, recovery, customer attrition, and regulatory exposure.
4. **Accountability Risk** – challenges related to governance, auditability, and responsibility for incident response.

By mapping these dimensions to product management decisions, the framework enables structured evaluation of resilience features and investment priorities.

4. Discussion: Implications for Software Product Management

The proposed framework offers practical implications for software product managers. First, it enables proactive

identification of ransomware-related risks during product planning rather than post-incident remediation. Second, it supports economically informed prioritization of resilience features such as automated recovery, secure defaults, and monitoring capabilities.

Third, the framework strengthens accountability by linking product decisions to measurable risk and cost outcomes. For Indian enterprises, particularly small and medium organizations, this approach supports cost-effective cybersecurity strategies aligned with business objectives. At a broader level, integrating ransomware resilience into product management contributes to the reliability of India's digital infrastructure.

5. Conclusion and Future Work

This paper presents a risk-aware software product management perspective for addressing ransomware threats in Indian enterprises. By reframing ransomware as a product resilience and accountability challenge, the study highlights the strategic role of product managers in cybersecurity decision-making.

Future work will focus on empirical validation through case studies and surveys involving product managers and security professionals. The framework can also be extended to inform policy discussions and industry best practices for building resilient digital products.

References

1.Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M., Levi, M., Moore, T., & Savage,S. (2013).Measuring the cost of cybercrime. *The Economics of Information Security and Privacy*, 265–300.
2.European Union Agency for Cybersecurity. (2023).*ENISA threat landscape 2023*. Publications Office of the European Union.
3.Gordon, L. A., Loeb, M. P., & Zhou, L. (2016).The impact of information security breaches: Has there been a downward shift in costs? *Journal of Computer Security, 24*(1), 1–26.
4.IBM Security. (2023).*Cost of a data breach report 2023*. IBM Corporation.
5.Verizon. (2023).*Data breach investigations report*. Verizon Enterprise.