Chapter 5
Enhancing Business Transformation Through Cybersecurity Frameworks in IoT Ecosystems:
Strategies for Risk Mitigation and Consumer Trust

Mercy Nyasha Magoso
http://orcid.org/0009-0007-9461-5098
Great Zimbabwe University, Zimbabwe

Clainos Chidoko
http://orcid.org/0000-0003-4530-7500
Great Zimbabwe University, Zimbabwe

Inos Chibidi
http://orcid.org/0009-0009-4201-1625
Great Zimbabwe University, Zimbabwe

Njodzi Ranganai
http://orcid.org/0000-0003-0451-1417
Great Zimbabwe University, Zimbabwe

ABSTRACT

The rapid growth of the Internet of Things (IoT) brings both opportunities and cybersecurity challenges for businesses. This chapter examines the integration of

DOI: 10.4018/979-8-3373-3441-7.ch005

Copyright © 2026, IGI Global Scientific Publishing. Copying or distributing in print or electronic forms without written permission of IGI Global Scientific Publishing is prohibited. Use of this chapter to train generative artificial intelligence (AI) technologies is expressly prohibited. The publisher reserves all rights to license its use for generative AI training and machine learning model development.

cybersecurity frameworks within IoT ecosystems, highlighting their role in mitigating risks. It discusses frameworks like the NIST Cybersecurity Framework and ISO/IEC 27001 as essential tools for addressing vulnerabilities. Through qualitative analysis of case studies, the chapter assesses how organizations utilize these frameworks to identify risks, develop management strategies, and enhance security awareness. Findings reveal that adopting cybersecurity frameworks improves risk management and boosts consumer trust, enhancing operational resilience. The chapter concludes with recommendations for tailored frameworks, employee training, transparent consumer communication, and regular vulnerability assessments.

INTRODUCTION

The Internet of Things (IoT) has transitioned from a technological frontier to a foundational pillar of global business transformation. By weaving a digital fabric of sensors, actuators, and data analytics into the physical world, IoT ecosystems are unlocking unprecedented efficiencies, creating novel business models, and reshaping the interface between corporations and consumers. However, this hyper-connectivity introduces a commensurate expansion of the cyber-attack surface, making robust security not merely a technical requirement but a strategic imperative for sustainable growth and market acceptance. This chapter explores how the adoption of structured cybersecurity frameworks can mitigate these risks, enabling organizations to harness the full transformative potential of IoT while building and maintaining essential consumer trust.

The scale of IoT's integration into the global economy is staggering. By 2025, Gartner projects the total IoT market, encompassing hardware, software, and services, will reach US $821 billion, driven by a 16% compound annual growth rate from 2020 (Jinxuan et. al, 2020). This ecosystem will include over 2.6 billion enterprise-grade IoT machines in service, a 31% increase from 2020 levels (Jinxuan et. al, 2020). From a value-creation perspective, the McKinsey Global Institute estimates that IoT could generate up to US $11.1 trillion in annual economic impact by 2025, revolutionizing sectors from manufacturing and healthcare to urban infrastructure (Patel et al., 2017). Cellular connectivity, a key enabler, is also accelerating, with IDC forecasting 3.6 billion cellular-connected IoT lines by 2025, spurred by innovations like 5G and eSIM technology that expand the reach and viability of connected solutions (Shafique et al., 2020).

Despite this immense potential, the journey of digital transformation is fraught with peril. Cybersecurity risk has emerged as the single greatest inhibitor to scaling IoT initiatives. A 2022 McKinsey survey of 208 executives revealed that 54% of companies now cite cyber-risk as the primary barrier to broader IoT adoption, a sig-

34 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/enhancing-business-transformation-through-cybersecurity-frameworks-in-iot-ecosystems/408620

Related Content

Security Principles in Smart and Agile Cybersecurity for IoT and IIoT Environments

Abdullah S. Alshraa, Loui Al Sardy, Mahdi Dibaeiand Reinhard German (2024). *Smart and Agile Cybersecurity for IoT and IIoT Environments (pp. 1-26).*
www.irma-international.org/chapter/security-principles-in-smart-and-agile-cybersecurity-for-iot-and-iiot-environments/351053

Identifying the Components of a Smart Health Ecosystem for Asthma Patients: A Systematic Literature Review and Conceptual Framework

Gloria Ejehiohen Iyawa, Asiya Khan, Sesinam Dagadu, Kristine Mae Magtuboand Rupert Calvin Sievert (2019). *The IoT and the Next Revolutions Automating the World (pp. 122-132).*
www.irma-international.org/chapter/identifying-the-components-of-a-smart-health-ecosystem-for-asthma-patients/234026

Cloud Computing, Smart Technology, and Library Automation

Lavoris Martin (2020). *Emerging Trends and Impacts of the Internet of Things in Libraries (pp. 105-123).*
www.irma-international.org/chapter/cloud-computing-smart-technology-and-library-automation/255387

Individual Privacy and Security in Virtual Worlds

Malu Roldanand Alan Rea (2011). *Security in Virtual Worlds, 3D Webs, and Immersive Environments: Models for Development, Interaction, and Management (pp. 1-19).*
www.irma-international.org/chapter/individual-privacy-security-virtual-worlds/49514

Digital Transformation and Tourist Experiences

Yunus Topsakal, Onur Icozand Orhan Icoz (2022). *Handbook of Research on Digital Communications, Internet of Things, and the Future of Cultural Tourism (pp. 19-41).*
www.irma-international.org/chapter/digital-transformation-and-tourist-experiences/295495