Chapter 6
The Evolving Cyber Threat Landscape in India:
Trends and Implications

Pallavi Kudal
https://orcid.org/0000-0001-9382-804X
Balaji Institute of International Business, Sri Balaji University, Pune, India

Rahul Waghmare
Balaji Institute of International Business, Sri Balaji University, Pune, India

ABSTRACT

India's rapid digital transformation, driven by fintech, e-governance, and smartphone penetration, has created vast opportunities but also heightened cyber risks. A 278% rise in state-sponsored attacks and incidents reported by 83% of organizations makes India one of the most targeted nations. Threats are evolving—from Ransomware-as-a-Service and state-backed espionage to supply chain exploits and disinformation campaigns. Systemic vulnerabilities such as outdated infrastructure, weak regulations, talent shortages, and poor cyber hygiene amplify risks. Businesses suffer financial and reputational losses, governments face threats to critical

DOI: 10.4018/979-8-3373-5992-2.ch006

infrastructure, and citizens encounter identity theft and fraud. Combating these challenges requires stronger public-private partnerships, AI-driven detection, resilient infrastructure, legislative reforms, and widespread cyber literacy. Building cybersecurity talent and awareness is vital to mitigate human-factor risks. India's digital future is promising, but securing it demands collaboration, innovation, and proactive defense is essential.

INTRODUCTION

India is undergoing rapid digital transformation since launch of Digital India Program in the yrear 2015. India is determined to make a digitally empowered society by rapid adoption of fintech solutions, e-governance platforms, and smartphones. Digital transformation is indeed revolutionizing the way individuals and businesses interact with technology. In past decade, fintech has become an integral part of the Indian economy, providing citizens with accessible financial services and facilitating transactions with ease. This boom is evidenced by widespread proliferation of digital payment platforms like Paytm, PhonePe, and Google Pay, which have become the most common way to make payments across the nation. These platforms leverage mobile technology, which has seen unprecedented growth in India, with the country boasting over 1.15 billion mobile subscribers as of December 2024 according to Telecom regulatory Authority of India. Alongwith digital transformation, e-governance, too, is transforming the public administration landscape, offering citizens streamlined access to government services and information. Initiatives like the Aadhaar project and the Digital India campaign aim to enhance transparency and efficiency in governance, further embedding digital practices into everyday life (Sharma, Jamwal, & Agrawal, 2025).

However, this digital revolution brings its own set of challenges. In past few years India has seen steep rise in cyberattacks. Between October 2023 and September 2024, India experienced more than 369 million malware incidents—averaging approximately 702 potential threats each minute. This surge highlights a deeper, systemic challenge, with cybercriminals employing advanced tactics and aggressively targeting any available vulnerabilities (Tripwire, 2024, May 6). In the first half of 2024, India witnessed