Chapter 8
Advancing Cybersecurity: Strategic Insights Into Multifactor Authentication

Sharon L. Burton
https://orcid.org/0000-0003-1653-9783
Capitol Technology University, USA

ABSTRACT

This research investigates the efficacy and challenges of Multifactor Authentication (MFA) in enhancing cybersecurity within organizational settings. Employing a qualitative design, this study integrates a comprehensive literature review with case studies to examine the deployment and impact of MFA technologies. Key findings reveal that over 57% of global businesses have adopted MFA, significantly reducing unauthorized access and breaches by 99.9% when correctly implemented. However, challenges such as user resistance, implementation costs, and the complexity of MFA systems persist, affecting overall effectiveness and adoption rates. This research concludes that while MFA substantially improves security, its success hinges on strategic deployment and user compliance. The significance of this research lies in its potential to guide organizations in refining their cybersecurity measures and in informing policy on secure authentication practices, ultimately contributing to enhanced organizational and data security in an increasingly digital world.

INTRODUCTION, PROBLEM, AND INDUSTRY CHALLENGES

The rapid adoption of mobile handheld devices in the workplace has shifted their role from luxury items for tech enthusiasts to essential tools for the modern workforce. These devices enhance productivity and operational efficiency but also pose significant security risks. Strong user authentication is critical to safeguard

DOI: 10.4018/979-8-3693-8562-3.ch008

against unauthorized access, especially in lost or stolen devices, and is vital for protecting organizational data. To address these security concerns, as given by Aburbeian and Fernández-Veiga (2024), multifactor authentication (MFA) plays a crucial role by requiring multiple forms of verification from different categories of credentials: knowledge-based (e.g., passwords), possession-based (e.g., tokens), and inherent characteristics (e.g., biometrics). In other words, MFA is a security process that verifies a user's identity by requiring multiple forms of verification, each from a different category of credentials (Bonderud, 2022). See Figure 1. This approach ensures that access to an account or completion of a transaction involves several independent methods of authentication, enhancing overall security. This thorough tactic pointedly lessens the risk of unapproved access, ascertaining MFA as a vital component of contemporary cybersecurity practices (Sun et al., 2024). Understanding the strengths and limitations of MFA is essential for its effective integration into an organization's security strategy. As of 2019, the third annual Global Password Security Report notes that approximately 57% of businesses globally have adopted MFA (LastPass Security Report, 2019). This statistic reflects a significant increase from previous years, highlighting the growing recognition of MFA's importance in securing digital assets (LastPass Security Report, 2019). Larger organizations, principally organizations with a workforce exceeding 10,000 employees, show even higher adoption rates, with around 87% utilizing MFA to protect their systems (Özşahan, 2023). The adoption rate of MFA for medium size organizations (26-100 employees) is 34% (Özşahan, 2023). The adoption rate for MFA for small organizations (25 employees or less) is 27% (Özşahan, 2023).

Figure 1. What is multi-factor authentication?