Chapter 7
Organizational Readiness for Artificial Intelligence (AI) in Network Security

B. Avery Greene
https://orcid.org/0009-0007-0849-3945
Capitol Technology University, USA

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

ABSTRACT

This chapter explores the essential organizational and cultural prerequisites for successfully integrating Artificial Intelligence (AI) into network security. This research employs a qualitative methodology, including a comprehensive literature review, to analyze internal needs and address ethical considerations such as bias, privacy, and fairness. This study examines the impact of organizational culture on the acceptance and effectiveness of AI-based solutions. It emphasizes the significance of end-user trust in AI-driven security alerts. The findings highlight the necessity of organizational readiness and cultural adaptation for the effective implementation of AI in network security, concluding that a comprehensive approach is essential for maximizing AI's potential in enhancing security measures. This research will benefit cybersecurity professionals, organizational leaders, and policymakers seeking to understand and navigate the complexities of AI integration in network security.

DOI: 10.4018/979-8-3693-8562-3.ch007

INTRODUCTION

It is not known how organizational readiness and cultural adaptation impact the successful integration of Artificial Intelligence (AI) in network security frameworks in the United States. The increasing impact of AI in network security is a direct response to the developing and complex nature of cyber threats (Kaur et al., 2023). As organizations become more digitally integrated, the need for advanced AI-driven security systems becomes crucial (Lee et al., 2023). As given by Mohammed (2023), integrating AI into existing network security frameworks presents unique challenges, necessitating significant organizational readiness and cultural and operational adaptation (Mohamed, 2023). In an era where cyber threats evolve unprecedentedly, integrating AI into network security transitions from an option to a necessity (Mohamed, 2023). The Mohammed (2023) research ties to the information presented by Sharton (2021), which focusses on the radical surge in cyberattacks, chiefly ransomware, throughout the move of remote work amidst the COVID-19 pandemic.

The reported 150% increase in ransomware incidents and the succeeding 300% upsurge in ransom payments emphasize the intensified susceptibility and the intensifying relentlessness of cyber threats faced by individuals and organizations (Sharton, 2021). Accordingly, these statistics support Mohamed's assertion that implementing AI-driven security solutions is no longer non-compulsory, perilous if ignored, and must successfully offset and mitigate these radical cyber threats.

Also, connected to the information presented by Sharton (2021), is the Hiscox Cyber Readiness Report, which surveyed over 5,000 organizations of diverse sizes across eight countries, specifies an unceasing rise in cyberattacks for the fourth consecutive year (Hiscox, 2023). A considerable increase in attacks targeting small businesses with fewer than ten employees rose from 23% to 36% in the past three years, highlighting cybercriminals' increasing focus on exploiting vulnerabilities within IT infrastructures (Hiscox, 2023). With the financial toll of cybercrime projected to attain $6 trillion annually by 2023 (Agenda, 2023), it is vital for organizations to strengthen their digital defenses (Hiscox, 2023; Peter et al., 2020). At this critical intersection, AI exists as a vital resource, poised to augment detection capabilities, simplify response times, and protect digital assets from various cyber threats (Sharma, 2023).

This chapter is an in-depth qualitative investigation that dives into the organizational and cultural requirements necessary for the optimal integration of AI into network security via a literature review. It sheds light on the difficulties and problems that companies confront with digital transformation (DT) by analyzing the internal demands and concerns around AI, including but not limited to, critical ethical issues such as prejudice, privacy, and justice. It also looks at how organizational culture and context influence the acceptability and efficacy of AI-based monitoring sys-