Chapter 7
The Cyberpsychological Dimensions of Healthcare Cybersecurity Crime Risks

Adina Lundy
https://orcid.org/0000-0001-7564-2110
University of Rhode Island, USA

Darrell Norman Burrell
https://orcid.org/0000-0002-4675-9544
Marymount University, USA & Pellegrino Center for Clinical Bioethics, Georgetown University, USA

Allison Huff
https://orcid.org/0000-0001-6102-8013
College of Medicine-Tucson, University of Arizona, USA

ABSTRACT

This study examines the cyberpsychological dimensions of cybersecurity risks in healthcare, emphasizing how human cognition, emotion, and organizational culture shape vulnerability within digitally transformed care environments. As healthcare integrates electronic health records, AI diagnostics, and telehealth systems, leaders, often trained in clinical or administrative domains, remain largely untrained in human factors psychology, limiting their capacity to address behavioral risk. Cyberattacks increasingly exploit cognitive biases such as urgency, authority, and trust, while clinicians under high cognitive load and ethical pressure frequently bypass protocols perceived as obstructive to patient care. Through an integrative,

DOI: 10.4018/979-8-3373-9918-8.ch007

evidence-based framework grounded in cyberpsychological theory, this research aims to align technical controls with user behavior, leadership awareness, and institutional culture. The goal is to transition healthcare cybersecurity from a reactive, technology-centric model to a proactive, human-centered paradigm that fosters resilience, ethical responsibility, and trust across clinical and digital ecosystems.

INTRODUCTION

The healthcare sector is undergoing a profound transformation driven by the integration of advanced digital technologies, including electronic health records (EHRs), telehealth platforms, wearable biosensors, and artificial intelligence-enabled diagnostic tools (Turuk, 2020; Hermes et al., 2020; Yogev et al., 2023). While these technologies promise significant gains in care efficiency, personalization, and clinical precision, they also expose the healthcare environment to a distinct and escalating category of cyberpsychological risksrisks shaped not only by technological vulnerabilities but also by human cognitive behavior, emotional bias, and institutional culture.

This risk landscape is particularly complex in healthcare because the decision-makers responsible for cybersecurity policy, executives, administrators, and physician-leaders, are typically trained in clinical or operational disciplines, not in human factors psychology or behavioral science. As a result, many cybersecurity interventions are designed with insufficient consideration for how employees actually perceive, interpret, and respond to cyber threats. For instance, while machine learning systems may enhance anomaly detection, their deployment often fails to account for how clinicians interact with alert fatigue or how social engineering tactics exploit emotional urgency and hierarchical deference, factors well documented in cyberpsychological literature (Kioskli et al., 2023; Klimburg-Witjes & Wentland, 2021).

In an environment where time pressure, clinical acuity, and moral responsibility dominate professional behavior, human error becomes a persistent and predictable vector for compromise. The most common breaches stem not from technical exploits but from cognitive and psychological manipulation, phishing emails that mimic trusted sources, fake credential prompts that play on urgency, or subtle behavioral cues that lead to over-disclosure (Barlow et al., 2020). These attacks succeed not merely because systems are misconfigured, but because staff are cognitively overloaded, behaviorally conditioned to bypass controls, and psychologically unprepared to detect deception.

Innovative Wind Energy Solutions for Smart-Sustainable Communities: Vision for Intelligent Energy Management and Climate Resilience in Industry 5.0

Bhupinder Singh, Hind Hammouchand Saurabh Chandra (2025). *AI Technologies for Enhancing Recycling Processes (pp. 491-508).*
www.irma-international.org/chapter/innovative-wind-energy-solutions-for-smart-sustainable-communities/368185