

Association for Information Systems

AIS Electronic Library (AISeL)

NEAIS 2023 Proceedings

New England Chapter of Association for
Information Systems

10-28-2023

Factors Influencing Data Breaches in Healthcare Organizations: A Comprehensive Analysis

Kaushik Ghosh

Suffolk University, kghosh@suffolk.edu

Kholekile L. Gwebu

University of New Hampshire, khole.gwebu@unh.edu

Follow this and additional works at: <https://aisel.aisnet.org/neais2023>

Recommended Citation

Ghosh, Kaushik and Gwebu, Kholekile L., "Factors Influencing Data Breaches in Healthcare Organizations: A Comprehensive Analysis" (2023). *NEAIS 2023 Proceedings*. 4.

<https://aisel.aisnet.org/neais2023/4>

This material is brought to you by the New England Chapter of Association for Information Systems at AIS Electronic Library (AISeL). It has been accepted for inclusion in NEAIS 2023 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

Factors Influencing Data Breaches in Healthcare Organizations: A Comprehensive Analysis

Research-in-Progress

Kaushik Ghosh
Suffolk University
kghosh@suffolk.edu

Kholekile L. Gwebu
University of New Hampshire
Khole.gwebu@unh.edu

ABSTRACT

Data breaches pose significant risks to patient privacy and security, especially in healthcare organizations. Despite the valuable insights provided by prior studies, a notable gap exists regarding the examination of technological and organizational factors that contribute to breaches. This study employs the Technology, Organization, and Environment (TOE) framework to provide insights into how data security in healthcare organizations can be enhanced. The TOE framework enables a thorough examination of the relationships between technical infrastructure, organizational variables, and the external environment, offering a holistic view of potential data security vulnerabilities. Within this framework, this study specifically explores the interplay between technological infrastructure, human resource management, and security protocols, with the goal of better understanding the variables that contribute to data breaches in the healthcare industry.

The preliminary findings indicate a notable trend wherein breached healthcare organizations exhibit a higher employment of full-time equivalent (FTE) programmers and network administrators, suggesting a potential vulnerability stemming from system complexity or heightened susceptibility points. Yet, distinctions in other staffing categories, overall FTEs, and hospital size were not significant. When observing security software, these compromised organizations reflected reduced usage of comprehensive security tools like antivirus, data loss prevention, encryption, and user authentication mechanisms. This emphasizes the centrality of a fortified technological infrastructure in alignment with the TOE framework. Interestingly, a pronounced reliance on firewall software was identified among breached institutions, potentially indicating an overemphasis on this singular defense mechanism. The research also found an absence of a marked difference in the adoption of biometric technologies between breached and secure organizations. This revelation underscores that biometric adoption in isolation may not drastically alter breach likelihood, accentuating the importance of other TOE dimensions such as robust user training and regulatory compliance. Furthermore, apart from a decreased usage of Thin Clients, the overall computer system configuration did not present significant variations, suggesting that the mere deployment type or volume of systems may not directly correlate with breach probabilities. In line with this, breached organizations displayed reduced employment of diverse server types, aligning with the TOE framework's technological dimension, which proposes that server diversity may augment system resilience. Nonetheless, it's imperative to recognize that the type of server alone isn't the lone breach determinant, reiterating the holistic necessity of considering all facets of the TOE framework, inclusive of encompassing security protocols and external determinants.

Keywords

Healthcare data breaches, Data security, Security protocols, Risk mitigation strategies, Technology, Organization, and Environment (TOE) framework