# Exploring the Strategic Cybersecurity Defense Information Technology Managers Should Implement to Reduce Healthcare Data Breaches

Maurice Mawel
mauricemawel@yahoo.com
U.S. Department of State (DoS)
Washington, DC – U.S.

Samuel Sambasivam
Samuel.sambassivam@woodbury.edu
Computer Science Data Analytics
Woodbury University
Burbank, CA 91504

## Abstract

The principal investigator (PI) conducted the research study to explore the strategic cybersecurity defense IT Managers should implement to reduce healthcare data breaches. The PI conducted a systematic literature review and selected articles that addressed healthcare data security breaches, information disclosure, cybersecurity in healthcare, and IT Managers' lack of leadership competence. Also, various annotations from contextual, seminal, grey, and recent literature were used to find the research problem: The strategic cybersecurity defense IT Managers should implement to reduce healthcare data breaches has not been established. The PI collected secondary data from the Office of Civil Rights (OCR)/Department of Health and Human Services (HHS). The analysis, results, and findings are provided below in Part 9. Nevertheless, the routine interaction during health information exchange (HIE) on an interoperable network and the behavior of care providers and third parties who use computers and mobile devices to exchange patient data is an opportunity for cybercriminals to install malware or launch a ransomware attack to exploit potential vulnerabilities whether to steal sensitive data or compromise the network systems. Therefore, strategic cyber defense or an innovative security model would mitigate the threat. An exploratory design is used, and an epistemological approach supports the research method and design. The study is significant, and it will contribute to the body of knowledge the PI suggested for future research and provide major recommendations.

**Keywords:** Health information exchange, Innovative security models, Interoperability, and Ransomware attack.

A full and updated version of this abstract appears in https://isedj.org