JISSec
Journal of Information System Security

Journal of Information System Security is a publication of the Information Institute. The JISSec mission is to significantly expand the domain of information system security research to a wide and eclectic audience of academics, consultants and executives who are involved in the management of security and generally maintaining the integrity of the business operations.

ISSN: 1551-0123
Volume 17, Issue 1

www.jissec.org

EDITORIAL

The first two papers of this Issue present solutions for both root cause analysis of information security incidents and secure user authentication, while the third contribution presents a case study which reinforces the importance of compliance in preventing information security breaches and the theft of personal data.

The first paper, entitled "Root Cause Analysis Quality Model for Corporate Security Breaches", is by Garry L. White and Jaymeen Shah from the USA. It explores issues that dilute the effectiveness of Root Cause Analysis (RCA) within an organization and proposes a quality model for integrated RCA thinking to identify the root cause(s) of information security incidents. Based on three key issues, this model lays the foundation for further theoretical development research to address these issues and to test the RCA framework with regards to corporate information security breaches.

In the second paper, "Secure matches of E-Mail to the Postal Addresses System", the author Carlos Gonzalez, from Mexico, presents a new and simple technology designed to support the secure authentication of a user which is applied in a system which securely matches e-mail addresses with postal addresses for a retail provider. This authentication technique has implications for the design of other applications that require user authentication and is of considerable interest for e-commerce retail companies, such as Amazon and e-Bay.

The case study is entitled "A Case Study of the Capital One Data Breach: Why didn't compliance requirements help prevent it?", and is by Nelson Novaes Neto, Stuart Madnick, Anchises Moraes G. de Paula, and Natasha Malara Borges, mainly from Brazil. This case study of a major data breach in 2019 at Capital One, one of the largest financial institutions in the U.S., highlights the key question of why firms' protection initiatives and compliance standards have not been sufficient to anticipate the leak of billions of data points in recent years. The authors attempt to understand whether more rigorous compliance would have helped prevent the data breach incident at Capital One, by mapping out exploited vulnerabilities and by identifying the already-existent NIST framework compliance requirements.

I sincerely hope that you will enjoy reading this Issue which is of such topical interest.

Gurpreet Dhillon, Editor-in-Chief