
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.

Editor-in-Chief
Gurpreet Dhillon
Virginia Commonwealth University,
USA

Managing Editor
Filipe de Sá-Soares
University of Minho, Portugal

ISSN: 1551-0123
Volume 12, Issue 3

www.jissec.org

EDITORIAL

This Issue focuses on the subjects of both recognizing and preparing for security breaches and data theft, and presents the results of studies related to the risk and consequences of facing cyber-attacks and data theft.

The first paper, is entitled “Forensic Analysis Challenges: Shifting from HDD to SSD”, is by Allen Benusa from Ridgewater College, USA, and Shajive Jeganathan and Mark Schmidt from St. Cloud State University, USA. It focuses on the challenges presented by the shift from using hard disk drives (HDD) to solid state drives (SSDs). This is especially pertinent, as, unlike HDDs, SSDs have an intelligent microcontroller that performs read/write operations to the flash storage autonomously from the PC host device. An experiment is carried out on writing and deleting identical data to a HDD and a SSD and the resulting forensic analysis is analyzed.

The second paper, by Steven Simo and Robert Perkins from respectively Mercer University, USA, and the University of West Florida, USA, describes “An Analysis of Data Breach Induced Trauma: An Exploratory Study”. The paper examines the impacts of trust and distrust on consumer intentions regarding the use of credit cards and the sharing of personal information, and analyses a study aimed at determining the trauma induced by data breaches on consumers, and whether this has an impact on levels of trust and distrust and consumer behaviors.

The third paper is an Industry Review entitled “When Biology Meets Cyber-Security” by Mohamed Hassan and Alexios Mylonas from Staffordshire University, UK, and Stilianos Vidalis from the University of Hertfordshire, UK. Similar to living creatures, computers are efficient at recognizing and eliminating danger around them. This paper examines the current cyber security status, whereby computers’ defensive systems are mostly focused on one or two methods – the Artificial Immune System, and AIS and/or Genetic Algorithms approaches.

All three papers discuss how computers and systems are becoming more efficient in defending against data loss, and the subsequent effect on consumer trust and confidence in present day times.

I am sure that you will enjoy reading this Issue.

Gurpreet Dhillon, Editor-in-Chief