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.

Editor-in-Chief
Gurpreet Dhillon
The University of North Carolina,
Greensboro, USA

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

ISSN: 1551-0123
Volume 13, Issue 2

www.jissec.org

EDITORIAL

This Issue reproduces two papers that were presented at the 2016 Security Conference in Lisbon and one from the Las Vegas Security Conference. Two of the papers examine the prevalence of security breaches and malware attacks via social media, identifying their *modus operand,* providing solutions for academia, practitioners and security professionals. The third investigates the crime of degree milling.

The first paper, entitled "Flash in the Dark: Illuminating the Landscape of Actionscript Web Security Trends and Threats", is by Meera Sridhar, Mounica Chirva, Benjamin Ferrell, Kevin W. Hamlen, and Dhiraj Karamchandani from the USA. It analyses the myriad malware attacks on Adobe's ActionScript Flash platform over the past six years, as this powers multimedia features for a significant percentage of all web sites nowadays. The results of these analyses provide researchers, web developers, and security analysts a better sense of how to protect users of these technologies.

The second paper, "Do Data Breaches Affect Our Beliefs? - Investigating Reputation Risk in Social Media", by Griselda Sinanaj and Frederick Beyer from the University of Göttingen, Sweden, examines the economic and organisational consequences of data breach incidents, as there is limited knowledge about their impact. More specifically, it examines the impact of data breaches on social media and measures the repercussion on reputation, which was found to be directly linked to the news media exposure of the breach incident and on the breach history of each firm.

The third paper is entitled "Cybercrime Dilemma in Distance Education", and is by Nattakant Utakrit from King Mongkut's University of Technology in Thailand. It recounts the findings of a study that investigates the scandals of degree mills, or diploma mills, which involves buying or selling bogus degrees. The study found that this newly emergent online academic fraud is more strategic, mainly targeting overseas buyers. It concluded that enhancing the ethical approach to education, self-awareness training, and strengthening national and international law and associated penalties are essential for mitigating these crimes.

All three papers discuss the need for professionals to be vigilant and attentive to the cited new trends in cyberattacks. In the case of degree mills, the role of governments in tightening laws and applying much more severe penalties is paramount.

I hope that this Issue makes profitable reading.

Gurpreet Dhillon, Editor-in-Chief