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 10, Issue 1

www.jissec.org

EDITORIAL

The prevailing theme of this issue is the pressing need for organizations to give greater importance to Information Security and to invest in implementing measures to defend themselves from the very real and dynamic threats now increasingly face organizations from all sectors. 2014 has seen some spectacular and mediatic breaches of Information Security which have affected millions of individuals, scores of blue chip companies and even threatened geo-political stability. There is a need for change, and this Journal sees its role as being a champion for this change.

The issue presents two very interesting papers, together with an Industry Report summarizing the findings of a recent cyber-security survey. The first paper, Systems Security Effectiveness in Large versus Small Businesses, by Joseph H. Schuessler, Tarleton State University, USA, and John Windsor and Yu "Andy" Wu from the University of North Texas, USA, aims to raise the degree of management awareness about Information Security by analyzing the relationship between threats and counter-measures using the 'Security Action Cycle'. It extends the Information Systems Security (ISS) construct developed in 2003 in its research, and develops a unique theoretically-based model as a tool for measuring ISS effectiveness, explores the non-recursive (circular) relationship between threats and countermeasures, and also elaborates on the role of industry affiliation and organizational size.

The second paper, Generative Control Theory for Information Security, is by Benoit Raymond of Laval University, Canada and Richard Baskerville from Georgia State University, USA and Curtin University, Australia. It also explores the theme of the threat of increasing information security losses, and explores the importance of information security standards for identifying control gaps and for implementing appropriate and effective information security controls. By analyzing and comparing control sets, the authors present a better understanding of information security controls defined in standards. Their research is innovative, as their analysis of control sets in two prominent information security standards led to the discovery of a new class of controls - generative controls - and also to the proposition of a new classification scheme with simple metrics for analyzing control sets in standards. They named this new theory - 'Generative Control Theory' (GCT).

Finally a summary of 2014 EY Global Information Security Survey (GISS) is presented, which concluded that for the first time in 17 years, external threats are now more likely than internal ones. A three phases for achieving an adequate cyber-security system is propose by EY, together with a description of associated benefits.

I hope that you enjoy reading this issue.

Gurpreet Dhillon, Editor-in-Chief

JISSec
Journal of Information
System Security