JISSec 8(1) 2012

Journal of Information System Security

www.jissec.org

Editorial

As I was putting together this issue of the journal, I remembered my first encounter with information security research. This was in 1988. While in my mind I seem to have a rather clear understanding of what constituted information security, but there is significant confusion in terms of definitions. Shall we refer to the field as "information systems security", "computer security", "cyber security" or simply "information security". More often than not these terms have been used interchangeably. Yet, the confusion persists. So, we decided that it would be useful to explore the nature and scope of what information security might be. We invite a discussion on this topic area. And we shall engage in exposition on the subject matter in one of the subsequent issues.

In this issue of the *Journal of IS Security* we have three very interesting papers. The first is authored by Daniel Phelps and his colleagues – Information system security: self-efficacy and implementation effectiveness. In this paper the authors demonstrate the impact information training has on the effectiveness of information system security implementation. The construct of self-efficacy is used to present a causal link to the correlations.

The second paper is by Michael Whitman and Herbert Mattford. The authors revisit the threats to information security. The paper presents an update of a study conducted10 years ago and highlights the changes therein. As the authors note, the lessons presented in this study hark back at the obvious - (1) become more informed of the potential for security breaches … (2) increase their awareness in key areas, … and (3) recognize that their overall level of concern for security may underestimate the potential risk inherent in the highly connected environment in which they operate.

The third paper is by Puneet Prakash. The paper, "Risk-based Valuation of Investments in Information Security- A Combination Approach" The paper argues that the price that the market charges a firm to bear the risk associated with its information systems forms a benchmark for investment in information security. At this price, the firm is indifferent between investing in security and transferring information systems security's risk to an outside bearer, most often insurers. Given the argument, the author argues that hence the actuarial techniques can be used to value information security investments. In conducting the argument the authors use

a combination of value-at-risk concept and the actuarial frequency-severity analysis, which are used to calculate risk premiums and expected loss.

I hope you find this issue of the journal interesting. I look forward to engaging in “secure’ conversations in the subsequent issues.

Gurpreet Dhillon, PhD
Editor in Chief
Virginia Commonwealth University