Editorial: Recent advances in security management

Sangkyun Kim

Department of Industrial Engineering,
Kangwon National University,
Chuncheonsi, Gangwondo, Republic of Korea
E-mail: saviour@kangwon.ac.kr

Information has become a vital resource for successful management of enterprise. The successful management of security technology and policy in a corporation is indispensable to its continuous growth. The goal of security management in a corporation is the continuous safeguarding of business processes and knowledge. This special issue aims to solve the difficult problems that a corporation easily faces in business environments when he tries to solve information security issues by providing practical and various research results. This special issue provides a variety and wealth of contributions in the management of security technology and policy for industrial information management.

The first paper, entitled 'Linking information engineering and security engineering with a problem-solving perspective', is authored by Sangkyun Kim. In this paper, the future directions of research which liaisons between information engineering and security engineering are provided. This study helps practitioners to understand what kinds of methodologies are used in their organisation and find a suitable methodology which solves the brain-teasing problems of corporate security.

The second paper, entitled 'Exploring the relationships between IT capabilities and information security management', is co-authored by Shuchin Ernest Chang and Shiou-Yu Chen. This paper explores the relationship between information technology (IT) capabilities and information security management (ISM). The validated model and the results of this study provide a reference for enterprise managers and decision makers to develop favorable tactics for achieving their goal of ISM.

The third paper, entitled 'Securing intellectual assets: integrating the knowledge and innovation dimensions', is authored by Kevin C. Desouza. This paper provides an integrated process framework for the management of intellectual assets. The proposed framework is used to describe salient security management challenges faced when managing intellectual assets. Many executives involved in security management programs were interviewed to elicit key security management challenges faced by organisations when addressing intellectual assets.

The fourth paper, entitled 'Security model applied to electronic records management: experiences and results in the nuclear sector', is co-authored by Pedro Solana and Daniel Pérez. This paper describes the design and implementation of a security model applied to the records management in the nuclear energy sector. This paper could be used as a guideline which helps other organisations to manage their records securely by providing the security model for operation and transmission of the acquired knowledge on the basis of their practical experiences.

The fifth paper, entitled ‘An integrated approach to the optimal selection of security tools using analytic hierarchy process and goal programming’, is co-authored by Vu H. Nguyen, Sangmun Shin and Yongsun Choi. In this paper, an enhanced methodology for supporting the decision maker in selecting the appropriate security tools for information systems in organisations is proposed. This paper provides security criteria hierarchy as the decision criteria. The competitiveness score of each security tool and the relative weights among different types of security tools are also provided. Finally, a systematic model which determines the optimal solutions for the security tools is implemented.

The sixth paper, entitled ‘IS practitioners’ views on core factors of effective IT governance for Taiwan SMEs’, is co-authored by Fengyi Lin, Shuching Chou and Wei-Kang Wang. This paper explores the core factors for effective IT governance and introduces a new framework. With the results of this paper, management could manage the corporate information security systems properly and effectively in support of the firm’s business objectives.

The seventh paper, entitled ‘Auditing methodology on legal compliance of enterprise information systems’, is authored by Sangkyun Kim. This paper proposes an IT compliance auditing methodology which consists of an auditing target, checklist, process model, evaluation indices and reference model. The methodology proposed in this paper helps IT staffs, managements and auditors to improve the level of IT compliance of enterprise information systems and manage an auditing project effectively.

The eighth paper, entitled ‘Ethical issues for internet use policy: balancing employer and employee perspectives, is authored by Sharman Lichtenstein. In this paper, the ethical issues that must be addressed when developing an organisational internet use policy (IUP) are explored. This paper draws on a conceptual analysis and an interpretive study of some organisations in Australia and North America. This paper highlights the need to balance the employer and employee perspectives when setting an IUP.

The ninth paper, entitled ‘Investigating effects of security incident awareness on information risk perception’, is co-authored by Antonio P. Volpentesta, Salvatore Ammirato and Roberto Palmieri. This paper describes an empirical investigation about the relationship between what is known about information security incidents which occurred within an organisation and the actual perception of information risk. Hypotheses about the influence of two awareness factors on risk perceived by information security managers are formulated and tested through ANOVA techniques.

The final paper, entitled ‘Technology-push and need-pull roles in information system security diffusion’, is co-authored by Quey-Jen Yeh and Arthur Jung-Ting Chang. This paper analyses managers’ security concerns on the basis of two forces of technology-push and need-pull which are traditionally applied to technology diffusion. The empirical findings show that the organisations are less likely to adopt new security measures unless compelled to do so by industry or security gaps, or if they are large enough and technically prepared for security innovations.

Finally, the guest editor of this special issue wishes to thank the authors for their contributions including those whose papers were not included in this issue. Furthermore, special thanks are due to the reviewers who provided invaluable evaluation and fruitful comments.