Preface

In today’s rapidly changing and evolving environment, IT and security executives have to make difficult calculations and decisions about security with limited information. They need to make decisions that are based on analyzing opportunities, risks, and security. In such an environment, information security management and governance issues are at the forefront of any discussions for security organization’s information assets, which includes considerations for managing risks, data, and costs. Organizations worldwide have adopted practical and applied approaches for mitigating risks and managing information security program. Considering complexities of a large-scale, distributed IT environments, security should be proactively planned for and prepared ahead, rather than as used as reactions to changes in the landscape.

Security governance framework should provide alignment of decisions regarding safeguarding information with the strategy, objectives, and culture of an organization (Dallas & Bell, 2004). Also, security governance should include what, who, and how decisions regarding information security (Weill and Woodham, 2002). What decisions should focus on assessment and decisions, who decisions should focus on people, roles, and structures in an organization, including responsibilities and accountability, responsible for business and security accordingly (Korac-Kakabadse & Kakabadse, 2001), and how decisions on processes and technology. Active participation of individuals from across an enterprise in assessments and decision making is also suggested as one of critical success factors of an information security governance (Williams, 2008). Security culture, thereby, emerges as a vital area to inculcate proper user security behavior and responsibility (Schlienger & Teufel, 2002; von Solms, 2000; Nosworthy, 2000). Not realizing that information security is a corporate governance responsibility and that a information security governance structure (organization) is absolutely essential are some of the most common mistakes made by organizations today (von Solms & von Solms, 2004).

Alongside people and cultural factor, lack of security decisions alignment with business strategy has been researched to be the one of the biggest factors in ineffective security governance (Kim and Leem, 2004; Kim and Leem, 2005). Absence of communication of security goals and objectives is also another factor in weak implementation of any security governance initiatives. Measuring and monitoring effectiveness of security governance structure and processes has also been articulated as one of the areas where organizations fail.

Role and importance of information security culture in establishing a successful information security program has never been higher. Technical and procedural controls effectively support information security objectives of an organization through awareness of organizational security culture. Cultural aspects in understanding security goals and enforcing them play vital role in any business setting. In Chapter 1, Investigating the Concept of Information Security Culture, Dr. Daniel Oost and Dr. Eng Chew of University of Technology, Sydney, Australia explore the concept of information security culture and find
that information security culture is a new concept and should not be treated as a panacea for information security problems. They also call for future research on information security culture, staying clear on definition and constituents of information security culture, while providing evidence for such claims. They also suggest that both and complexity and context of the culture be considered while findings and assertions are discussed. They also suggest that research be wary of distinction between behavior and culture from an information security culture standpoint.

In Chapter 2, *Assessing Market Compliance of IT Security Solutions: A Structured Approach Using Diffusion of Innovations Theory*, Dr. Heiko Roßnagel and Dr. Jan Zibuschka from Fraunhofer IAO, Germany present a theory based model for understanding diffusion of IT security solutions. Using Roger’s diffusion of innovations theory, authors suggest a model for holistic ex-ante analysis of the market potential of such systems based on generic factors influencing the diffusion of security solutions. Authors provide introductions to pertinent aspects of diffusion of innovations theory, and present their model that uses theoretical elements as structuring tool in ex-ante analysis. They present case study analyses for three IT security solutions, demonstrating the applicability of their method. They also compare the results yielded by application of their model with the actual market results.

Need for services and frameworks for identity assurance has increased last few years due to propagation of open networks used for identity assertion and trust. Identity assurance is a concept defined as “the degree of confidence” that one party (usually the one receiving identity information about participants) can have about the veracity of the information as well as its closeness in portraying the intended attributes of the participant. With growth of communication over open networks, establishing this confidence has never been more challenging. With recent upsurge in use of open identity management systems, establishing trust with the identity provider is of utmost importance in instilling confidence in the assertions made by them about participant’s identity. Dr. Ivonne Thomas and Dr. Christoph Meinel from Hasso-Plattner-Institute, Germany, in the chapter titled *Identity Assurance in Open Networks* (Chapter 3), provide a state-of-the-art overview of identity assurance frameworks and describe them along important trust factors of identity providers. Authors also call for research into the areas that they identify and highlight as limitations of identity assurance frameworks. To demonstrate suitability of future research, authors present a small case study to enable a service provider to distinguish between different qualities of trust, providing more flexibility in the way identity assurance is achieved in open networks.

With fast evolving technological and business landscapes, managing information security has never been more challenging and rewarding. Information security governance has emerged as one of the most effective ways to effectively manage information security while also aiding immensely on corporate governance. There are several frameworks and standards available that can enable companies to incorporate information security governance in their structures, processes, and culture. However, they need to be contextualized for effective management and implementation while ensuring alignment with corporate objectives. In chapter 4, titled *Information Security Governance*, authors, Janne J. Korhonen and Kari Hiekkanen of Aalto University, Finland and Juha Mykkänen of University of Eastern Finland, Finland use design science approach to present a prescriptive reference model for information security governance that aims to incorporate cross-functional information security management throughout the organization and frame it within the overall organizational design.

Chapter 5, *Enterprise Information Security Policies, Standards, and Procedures: A Survey of Available Standards and Guidelines*, surveys enterprise information security policies, standards, and procedures while examining the existing resources, analyzing available options. Authors of the chapter, Syed Irfan Nabi, Ghmlas Saleh AlGhmlas, and Khaled Alghathbar, King Saud University, Riyadh, Saudi Arabia
offer recommendations to decision makers about policies, standards, and procedures to establish effective information security management. Authors evaluate the need, requirements, and audience for different types of security documents and their relationships with one another. This research in the chapter involved identifying the relevant documents and analyzing the various well-known and established international, as well as national, information security standards and guidelines. Authors, based on their research presented in the chapter, recommend appropriate information security standards and guidelines based on the sector to which an organization belongs.

Information Security Management Systems (ISMSs) have emerged as a valid and proven systems for effective management of information security in all levels of organization. These systems offer richer value to Small and Medium-size Enterprises (SMEs), where resource availability and selective deployments are the norm. In Chapter 6 (ISMS Building for SMEs through the Reuse of Knowledge), Luís Enrique Sánchez and Antonio Santos-Olmo of Departament of R+D, Ciudad Real, Spain and Eduardo Fernandez-Medina and Mario Piattini of University of Castilla-La Mancha, Ciudad Real, Spain present strategy to manage and reuse security information in Information System security management. This strategy is framed within a methodology that is designed for integral security management and its information systems maturity, described as “Methodology for Security Management and Maturity in Small and Medium-size Enterprises (MSM2-SME),” and it is defined in a reusable model that authors have called “Reusable Pattern for Security Management (RPSM).” Authors, during the last 10 years, have obtained considerable experience in the establishment of ISMSs, and during this time they have observed that the structure and characteristics of different SMEs as they do security management is more similar than not. Authors have leveraged this finding to construct patterns for ISMSs which can be reused and refined.

Social networking sites (SNSs) have gain significant attention in last few years. With a diverse demographics participating in the SNSs, users have traditionally entrusted SNSs with confidential and personal information. While users have some control over their information, the implications surrounding security and privacy are real and severe. SNSs have used a wide variety of systems to mitigate risks from information sharing on these sites, but the threats are fast evolving. In chapter 7 (Information Security and Management in Social Network), authors Ajit Balakrishnan and Alkesh Patel describe issues related with privacy and social spamming, and show the measures to handle them by semi-automatic ways. They also navigate through construction of user reputation system and its applicability in social network.

Effective access management is a growing concern for most organizations. Authentication plays a central role in managing access to information in an organization. Stronger authentication on one hand tends to improve security due to complex (and hard to guess) passwords, but at same time, they are difficult to recall, which encourages users to write down the password, thereby undermining security or impacts availability and productivity due to forgotten passwords. Due to importance of authentication mechanism in ensuring integrity and confidentiality of information, there are many newer and innovative methods emerging to supplement or replace passwords. As an unique alternative to secure passwords, Marcia Gibson, Marc Conrad, and Carsten Maple of University of Bedfordshire, Luton, United Kingdom and Karen Renaud of University of Glasgow, Glasgow, United Kingdom present a novel scheme - a musical password in Chapter 8, titled Music is the Key: Using our Enduring Memory for Songs to Help Users Log On. Their method - Musipass – is designed for user authentication to Web resources and proposes to replace passwords. The chapter presents one the most promising and innovative authentication mechanisms proposed for replacing passwords for user authentication.

Chapter 9, Information System Integrated Security, presents a comprehensive and integrated view on the security of Information System that includes considering hardware, software, human factor, data,
and the impact of real world. Author, Milena Tvrdíková of VSB-Technical University Ostrava, Czech Republic, asserts that the security of Information Systems cannot be solved only by management of Information Technologies alone, because they are just part of a larger and more integrated system. The chapter presents an integrated approach to the security of Information System, while providing recommendations for managing the security of Information System.

Surveillance is an important and critical aspect of compliance and threat monitoring. In today’s complex and high traffic environments, continuous monitoring and response, with cost management, is a daunting task due to highly evolving contexts with time and location based sensitivities. Complete automatic detection, without human intervention and decision-making, from results produced by these surveillance systems, is not possible. Introduction of human element to verify alarms generated by surveillance systems and to respond to alarms is not only necessary but required for assurance of the process. This entails impact on performance. In Chapter 10, Dr. Peter Goldschmidt, of The University of Western Australia, Australia, discusses support and assurance of surveillance monitoring outcomes and processes. The aim of this chapter, Surveillance Communities of Practice: Supporting Aspects of Information Assurance for Safeguards and Compliance Monitoring, is to manage and operationalize information assurance real time alarm identification and verification, by tracking the parameters monitored by the existing information assurance monitoring infrastructure and operating work systems, and then leveraging that data/knowledge to create useful and actionable information. The ultimate objective of this research is to expedite decision making process to enable accurate and rapid operational execution.

The prospects of cloud-based computing are highly promising. Companies have a lot to gain by adopting cloud based services and products to not only enhance their own capabilities while focusing on their core competencies, but also allowing for agility and scalability while effectively managing costs. The trend towards this phenomenon is strong and encouraging. It has been researched and found that while there are proven benefits to cloud computing there are inherent risks that are inadequately, at best, managed by existing safeguards. Particularly concerns around risks and compliance cannot be ignored and haven’t found an established strategies or frameworks for effective management. Chapter 11, titled Not Every Cloud Brings Rain: Legal Risks on the Horizon, authored by Dr. Sylvia Kierkegaard of International Association of IT Lawyers, Denmark, provides an introduction and discusses different kinds of legal risks associated with cloud computing. Dr. Kierkegaard asserts “Cloud computing opens numerous legal, privacy and security implications, such as copyright, data loss, destruction of data, identity theft, third-party contractual limitations, e-discovery, risk/insurance allocation and jurisdictional issues.” The chapter presents special coverage on the international data transfer between the EU and non-EU states.

In current organizational environment where collaboration and partnerships with strategic service providers are key to sustaining competitive advantages, organizational processes are managed by individuals from within company as well as from outside including a varied sources of companies such as contractors, employees of partners, etc. This raises unique challenges in maintaining integrity and confidentiality of enterprise information without hampering collaboration and information sharing. Standards such as ISO27001 do provision for work agreements and contracts to serve as basis of trust and ensuring security of information, but actual implementation and enforcement is left to companies to decide. To address this challenging situation, chapter 12, Securing the Extended Enterprise: A Method for Analyzing External Insider Threat, presents a method to identify external insiders and to categorize them as a threat or as a possible mitigation. The results of the method can be further used to help companies design third-party agreements to include and address non-measurable IT security agreements. The authors of the chapter, Virginia N. L. Franqueira, André van Cleeff, Pascal van Eck, and Roel Wieringa
of University of Twente, Enschede, The Netherlands, illustrate the above-mentioned method using a manufacturer-retailer example, while giving an overview of the external insider threat and showing challenges involved with external insiders.

Management of different aspects of information security is an overwhelming challenge. Effective management usually entails use of a standard framework or structure for ensuring success and continuous monitoring of overall performance. Some of the most common standard security management systems include ISO 27001, BS 25999, and ISO 20000. Each organization can evaluate strengths and weaknesses of each of these available and widely adopted standard based on their own unique requirements and environmental impositions. Guiding through the process of selection and eventual adoption of a standard and its structures is a significant undertaking for most organizations. In chapter 13, Information Security Management Systems Cybernetics, Dr. Wolfgang Boehmer of Technische Universität Darmstadt, Germany presents standard management systems as they relate to prescribed policies while suggesting valuable potential applications. Dr. Boehmer also presents a field study that highlights the advantages of management systems in practice, while demonstrating how a formal description of an information security management system can be created by means of discrete-event systems theory and how an objective function for management systems can be defined.

Identity theft is one of the major upcoming threats in cybercrime, which could be defined as an unlawful activity where the identity of an existing person is used as a target without that person’s consent. There are obvious direct financial losses, e.g. the amounts directly extracted by criminals from the accounts etc, but also indirect costs for businesses, governments, and consumers in terms of loss of reputation. In Chapter 14, Fraud and Identity Theft Issues, authors Ranaganayakulu Dhanalakshmi and Chenniappan Chellappan of Anna University, India present contemporary issues and challenges with fraud and identity theft prevention while proving an overview of different modes of launching identity theft. The chapter presents methods of fraud and identity theft while evaluating the impact on consumers and businesses. The chapter discusses defense mechanisms for phishing attacks and presents a content based statistical filter for thwarting phishing emails.

In recent years, with a spurt in growth of legal and regulatory requirements surrounding protecting consumer interests, companies have embraced information security governance as part of corporate governance for meeting their due diligence efforts. Several security governance frameworks and models have come to commercial successful adoption at millions of companies across globe. Use of a governance framework allows companies to leverage some of the best practices in the industry while following standard based systems for monitoring and enforcement. Chapter 15, Information Security Governance and Standard Based Management Systems, by Margareth Stoll and Ruth Breu of University of Innsbruck, Austria, presents an effective and efficient method to implement information security governance and compliance. The presented holistic information security governance model integrates standard based management systems with different information security governance frameworks while meeting the requirements of the international ISO/IEC 27001 information security management standard. The model has been implemented in various organizations, and the chapter discusses the case studies results as well.

Implementation of effective security solutions requires availability of and interaction amongst several solution elements, each element of which a component can be posed as a potential weakness, thereby threatening effectiveness and objectives of the complete security coverage and system. Chapter 16, A Construct Grid Approach to Security Classification and Analysis, presents a method to map solutions to problems while identifying gaps and weaknesses. The authors of the chapter, Michael Van Hilst and Eduardo B. Fernandez of Florida Atlantic University, Boca Raton, Florida, USA, call the suggested
A method constructs a grid, which divides the conceptual problem space along multiple dimensions, where each dimension is defined as a continuum with identifiable regions of concern. The chapter also provides examples of several dimensions and the types of concerns used to define the regions of concern.

Employee motivations and behaviour significantly impact implementation of security measures in an organization. There are a lot of factors that influence employee behaviour towards security practices and their own intention to proactively safeguard company’s information assets. The development of a security culture in an organization that promotes positive compliance and security behaviour from employees is utmost critical to success of any information security program. Chapter 17, *Towards an Organizational Culture Framework for Information Security Practices*, analyses the important relationship between organizational culture and its role in successful implementation of information security system. Authors, Joo Soon Lim, Shanton Chang, Atif Ahmad, and Sean Maynard of the University of Melbourne, Australia, identify eight organizational culture characteristics that any security practice can be successfully implemented within. The chapter presents research and practical implications of the findings and future research areas are discussed.

Despite the fact that need for IT security architecture has never been higher in recent years, there is a lack of comprehensive and proven models or frameworks for security architecture development. Literature on applied and practical aspects of the architectural design is even more lacking. Architecture for Information Security that is modular and flexible allows for changes in it as landscape for threats, and risks change over time. This not only allows for more organizations to adapt such architectural blueprint, but also allows them to effectively mitigate new risks that emerge over time. Development of an architecture that is based on industry best practices, as well as well understood and deployed standards such as ISO27001, further adds validity to the components of the architecture while allowing companies to fit their objectives and requirements with the architecture. Shyh-Chang Liu and Tsang-Hung Wu of I-Shou University, Taiwan, Republic of China, in chapter 18, *Establishment of Enterprise Secured Information Architecture*, present a unique solution to enhance the overall security of IT environment by designing and incorporating information flows (including the strategy flow, risk management flow and logistic flow) based on the company’s own integrated operational modes.

Ines Brosso of Mackenzie Presbyterian University, Brazil and Alessandro La Neve of Centro Universitário da FEI, Brazil, present a system for information security management based on adaptive security policy using user’s behavior analysis in Information Technology. Chapter 19, titled *Information Security Management Based on Adaptive Security Policy using User Behavior Analysis*, presents a system that analyzes user behavior based on information accessed about different systemic components such as hardware, software, time, policies, et cetera. The output of the system provides different levels of trust that can be assigned to each user, which can determine if the user can be trusted or not. The dynamic nature of the system continuously gathers information from environment and performs updated assessments for the trust levels, in an effort to keep current with changes in environment and in user behavior.

Credit fraud is one of the fastest emerging threats in electronic commerce domain, which affects both consumers and businesses alike. While e-commerce is thriving due to its convenience and choices that it offers consumers and businesses, it also poses untraditional risks that are undermining the trust and validity of the channel. Banks are increasingly investing in detection and prevention technologies and procedures for mitigating risks from credit card fraud. However, with recent data breaches are most high profile transaction processors, the use of credit card information (without having to have physical possession of the card) via Internet to make fraudulent charges are increasing at an alarming rate. The techniques for effective detection and deterrence have never been more needed for security of the elec-
tronic commerce channel. Chapter 20, Detecting Credit Fraud in E-Business System: An Information Security Perspective on the Banking Sector in UK, investigates the current debate regarding the credit fraud and vulnerabilities in online banking and discusses some possible remedial actions to detect and prevent credit fraud. Authors, Md Delwar Hussain Mahdi of Applied Research Centre for Business and Information Technology (ARCBIT), London, UK and Karim Mohammed Rezaul of Glyndŵr University, Wrexham, UK, conduct a comprehensive study of online banking and e-business, paying special attention to credit fraud detection. They find that there are specific channels of credit fraud that are increasing, while imposing significant barrier to growth of e-business in the banking sector.

Use of cyber attacks and threats are increasingly gaining attention from terrorism experts. Recently, threats in cyber space have been highlighted as upcoming and most challenging channel of launching cyber terrorism attacks. Given the interconnectedness of the communications media and reliance of them for business and national defense alike, cyber terrorism has taken a central position in cyber terrorism discussions. Christopher Beggs of Security Infrastructure Solutions, Australia and Matthew Warren of Deakin University, Australia in Chapter 21, Safeguarding Australia from Cyber-Terrorism: A SCADA Risk Framework, suggest that cyber-terrorism capabilities are an integral, imperative, yet under-researched component in establishing and enhancing cyber-terrorism risk assessment models for SCADA systems. In their chapter, they propose a cyber-terrorism SCADA risk framework that has been adopted and validated by SCADA industry practitioners. The chapter presents a high level managerial framework designed to measure and protect SCADA systems from the threat of cyber-terrorism within Australia. The chapter presents the findings and results of an industry focus group in support of the developed framework for SCADA industry acceptance.

Yurdaer N. Doganata of IBM T. J. Watson Research, USA discusses the importance and challenges of detecting compliance failures in unmanaged business processes in Chapter 22, Detecting Compliance Failures in Unmanaged Processes. The chapter also explains the process of creating and verifying internal controls as a requirement of enterprise risk management framework while investigating use and effectiveness of automated auditing tools to detect compliance failures against internal control points in unmanaged business processes. The chapter also analyzes risk exposure of a business process due to compliance failure and the factors that affect the exposure.

Chapter 23, Loss of Data: Reflective Case Studies, by Ian Rosewall and Matthew Warren, Deakin University, Australia presents a number of real life case studies: Wikileaks, Ministry of Defence - Burton Report (UK), and disclosure issues within the Victorian Police (Australia). The chapter discusses organizational loss of data, prevention approaches, enforcement policies, and need to know versus need to share policies in a modern working environment. The chapter focuses on the impact of “Generation F - the Facebook Generation” and their attitudes to security, while discussing the issues surrounding the compliance /non compliance with enforcement policies and the dilemma facing current work practices of need to know versus need to share.

The primary audience for the book is professionals, scholars, researchers, and academicians working in this field that is fast evolving and growing as an area of information assurance. Practitioners and managers working in Information Technology or information security area across all industries would vastly improve their knowledge and understanding of critical human and social aspects of information security. Auditors and lawyers from organizations from across industries will also find this book as a very helpful resource. Often the managers are overwhelmed with solutions and technologies for information security while squandering a lot of resources on trying to understand what would work for them and what not. While there are a few publications in the area, the proposal of this edited book is quite unique and
different from current offerings. By keeping the focus of the chapters to the practices and solutions that are practical and implementable, it will add huge value to the extant literature while helping organizations around the world understand and effectively improve their overall security posture. Based on the contributors’ collective experience in information security and allied domains, they are highly confident that the focus and approach of this book is nothing like the ones already published. The editors anticipate huge response from information security community due to practicality and applicability of issues and solutions that are included in the book.

Manish Gupta  
*State University of New York, Buffalo, USA*

John Walp  
*M&T Bank Corporation, USA*

Raj Sharman  
*State University of New York, Buffalo, USA*

**REFERENCES**


