Preface

This handbook of research brings together chapters from renowned professionals and academicians from across the globe, on timely and critical topics on social and organizational issues of managing information security. The handbook aims to provide immense scholarly value and contribution to the fields of information technology, security, and management. Despite being a strongly emerging threat to organizational information security, there is evident dearth of research in the area. One of the key objectives of the handbook is to fill the gap in the existing literature on social and softer organizational dimensions of information security by providing the readers one comprehensive source of latest trends, issues, and research in the field. The book provides high-quality research chapters and industrial and practice articles on various topics ranging from employee surveillance to security education and awareness to security usability issues.

A NEW ORDER IN EVOLUTION OF SECURITY THREATS: EMERGENCE OF SOCIAL AND SOFTER ORGANIZATION ISSUES

As organizations are becoming increasingly dependent on technology and information systems for their operations and for sustaining strategic advantages, information security is playing an ever-important role in not only ensuring continuity of operations and protecting informational assets, but also in enabling business. In today's Internet age of interconnected electronic business environments, information security concerns are of paramount significance. At the same time, because of its openness and ubiquity, the Internet is being widely adopted as a cheaper and faster means of provisioning services and goods. Organizations are growing concerned with information security, as it is vital for their existence in protecting customer and corporate information, while managing its supply chain (Olivia, 2003). With the heightened concerns of security and rapid advancements in networking, communication, and mobility, as well as increases in risks and threats, management of information security has become one of the top business priorities within many organizations. It is becoming increasingly evident that the weaker links in an information-security chain are the people, because human nature and social interactions are much easier to manipulate than targeting the complex technological protections of information systems. Concerns and threats regarding human and social factors in organizational security are increasing at an exponential rate and shifting the information security paradigm.

While organizations are increasing spending on countermeasures to protect informational assets, there has been a disproportionate amount of allocation to non-technical countermeasures. Numerous surveys suggest that more than half of security breaches at companies occur due to actions taken by employees either indirectly or directly (Kaplan-Leiserson, 2003). However, organizations are not investing as much on non-technical measures such as security usability issues, compliance issues, motivational

issues, security awareness, and so forth. Accidental or deliberate errors by individuals have adverse impacts through increasing an organization's vulnerability (Dutta & McCrohan, 2002). Practitioners and, increasingly, researchers in the field of information security, are realizing and admitting that information security depends more on peoples' aspects (human, social, and policy) than on technological. Improving organizational information security posture depends more on understanding and changing beliefs, attitudes, and behaviors of employees than on deploying latest technological systems. There are numerous studies that have documented actual and potential losses due to information security abuses by insiders (Burger, 1993; Loch, et. al., 1992; Panettieri, 1995). Beyond focusing on human and social elements, security practices and organizational factors such as policies, management philosophy, and organizational culture also play equally important role in improving information security program's effectiveness. Information security effectiveness is the ability of information security measures to protect against unauthorized or deliberate misuse of IS assets by people (Straub, 1990).

The relative lack of research on the topic of social and organizational aspects of information security in the existing literature on both broader areas of information security and human-computer interaction motivated work on this handbook of research to identify and fill gaps in the research. Despite a good amount of research on technical measures of information security, it is somewhat surprising that human and social factors have not been given sufficient attention, given that appropriate use of information systems involves human and social interactions and users' behavior, both end-users and system managers. This becomes even more important in light of the fact that the study of human-computer interaction has been the one of the most active areas of research within the field of information systems design and user. (Helander et. al., 1997). From a research standpoint, there are several areas that should be explored to better implement information security measures from a social and organizational perspective. Some of the considerations include users' resistance towards secure computing practices (Turnage, 1990), usability designs to lower user resistance (Al-Ghatani & King, 1999; Markus, 1983), ethical legitimacy of user behavior (Gordon, 1994; Gordon, 2000), motivational factors (Franklin et. al, 2007); and organizational policies and structure (Anderson, 1993). There are many key social and organizational issues to information security arising from human error problems such as a lack of adequate security training, lack of awareness about the importance of corporate and customer data, risks associated with insecure behavior, time and schedule pressures, absence of clear knowledge and communications regarding roles, responsibility and accountability, policies regarding use of organizational resources such as phones, e-mail, laptops, ans so forth. Instilling a security culture will entail different socio-cultural aspects that will support technical and other organizational security measures. This will help organizations to understand and increase trust between the different actors concerning information security within its organizational boundaries. Human and social factors in organizational security such as human error on information security are important issues that left unresolved can have adverse effects on industry (Carstens, 2008).

The book is aimed towards the primary audience of professionals, scholars, researchers, and academicians working in the fast evolving and growing field of information security. Practitioners and managers working in information technology or information security sectors across all industries would vastly improve their knowledge and understanding of critical human, social, and organizational aspects of information security. The book covers topics both on theoretical (research) aspects of securing information systems and infrastructure from social and organizational perspectives and real-world implications and implementations (practice) of the research.

There are 29 chapters in the handbook that are organized into four sections as follows:

I. Organizational Security
II. Privacy and Social Engineering

III. Security Education and Awareness
IV. Human and Interaction Issues

The first section of the book, titled ***Organizational Security***, hosts 8 chapters on different aspects of organizational issues in information security. The section focuses on issues such as roles and responsibilities in organizational catastrophe contingency planning, soft techniques in understanding and thwarting organizational threats to information security, employee surveillance and monitoring, electronic insurance for security risks, social and cultural development in honesty credit system in organizational settings, role and organization based access management, enterprise information system security life cycle management and information security economics. Brief discussions on objectives and contributions of the chapters in the book are presented next.

Chapter I of the book, "*Responsibilities and Liabilities with Respect to Catastrophes*" by Warren Axelrod, US Trust, USA, examines the impact of catastrophes on information security and suggests who might have responsibility for maintaining an appropriate level of data protection when a catastrophe occurs. The author asserts that catastrophe contingency planning is very different from regular forms of business continuity and disaster recovery planning in terms of size, focus, scope, and content. Catastrophe contingency plans (CCPs) must comprehend a broad range of potential events affecting large numbers of humans and other living creatures, information processing capabilities, information and media, buildings, and infrastructure, and the like, each with its security considerations, and each characterized by its own roles, responsibilities, and liabilities. The chapter encourages the development of more comprehensive and realistic CCPs, that is, plans that delineate roles and responsibilities clearly and liabilities should CCPs go awry.

Chapter II, "*The Complex New World of Information Security*" discusses the latest developments in the shifting threat landscape and their impact on the world of information security. It describes how we are now moving into a "third wave" of cybercrime where sophisticated criminals are applying relatively "soft" techniques that are more pervasive in their execution. The chapter argues that, as a consequence, information security countermeasures based on the latest information intelligence technologies will need to be complemented by softer, more pervasive techniques drawn from disciplines such as process engineering, policy development, behavioral science, psychology, and benefit management. The author, David Porter, Detica Corporation, UK, considers how these countermeasures can be fully realized in today's business environment and concludes by discussing future directions such as the growth in complexity and the rise of the surveillance society. The author hopes that by understanding these new imperatives, information security practitioners will be in a stronger position to protect their organizations from today's threats — and those of tomorrow.

In recent years, many studies have highlighted the unprecedented growth in security threats from multiple and varied sources faced by corporate as well as governmental organizations. People inside the organization with ready access to confidential or proprietary data can easily violate the organization security policy, maliciously or inadvertently, without being caught. In order to protect their reputation and valuable assets, many organizations take the dramatic but necessary step of deploying and operating employee surveillance and monitoring tools within their network perimeters. In **Chapter III**, "*Employee Surveillance Based on Free Text Detection of Keystroke Dynamics*", authors, Ahmed Awad E. Ahmed and Issa Traore of University of Victoria, Canada, discuss employee surveillance schemes from both technological and legal perspectives. They argue that keystroke dynamics could be used to fight effectively against insider threat, and as such it could play an important role in employee surveillance. They present a keystroke recognition scheme based on free text detection that goes beyond the traditional approach of using keystroke dynamics for authentication or employee performance evaluation, and consider us-

ing such information for dynamic user profiling. The generated profiles can be used to identify reliably perpetrators in the event of security breach. Such form of user profiling provides a very effective way of combating insider threat that is less intrusive to individual privacy.

An online business organization spends millions of dollars on firewalls, anti-virus, intrusion detection systems, digital signature, and encryption, to ensure minimal security breach. Nonetheless, a new virus or a clever hacker can easily compromise these deterrents, resulting in losses to the tune of millions of dollars annually. To minimize the financial loss, the authors of **Chapter IV**, "*E-Risk Insurance Product Design: A Copula Based Bayesian Belief Network*", propose that online businesses should invest in e-risk insurance products as a complementary alternative, above the network security appliances. In this work, the authors, Arunabha Mukhopadhyay, Indian Institute of Management Calcutta, India; Samir Chatterjee, Claremont Graduate University, USA; Debashis Saha, Indian Institute of Management Calcutta, India; Ambuj Mahanti, Indian Institute of Management Calcutta, India; and Samir K. Sadhukhan, Indian Institute of Management Calcutta, India, develop a Copula aided Bayesian Belief Network (CBBN) model, to assist insurance companies to design e-insurance products. The CBBN model presented in the book does an e-vulnerability assessment (e-VA) and e-risk quantification (e-RQ). Authors first draw a casual diagram (BBN) stating the probable reason for security failure in an organization, assuming the marginal distributions for each of the nodes of the diagram. Using the CBBN model, the joint probability of the constituent nodes of the BBN is computed and the conditional probability of each of the occurrences of the malicious event is arrived at. Authors then assume a loss distribution, and using the principles of collective risk modeling, arrive at the expected severity of the attack. The e-risk insurance companies compute the premium, by charging an extra (i.e., overloading and contingency loading), over the expected severity of attack.

E-commerce mode aggravates information asymmetry so that honesty-credit problems become more serious. **Chapter V**, "*E-Commerce Security and Honesty-Credit*" discusses the honesty-credit issue and honesty-credit system construction in e-commerce. It argues that the honesty-credit issue belongs to e-commerce security problems to some extent since it also destroys information integrity, confidentiality, and availability. The study of honesty-credit issue in e-commerce will help to promote social culture development as well as improve e-commerce security. Basing on analysis of three-game models, the authors, Lao Guoling and Liping Wang, of Shanghai University of Finance and Economics, China, suggest the construction of social honesty-credit system mainly include four aspects: cultivate citizens' sense of honesty-credit, strengthen legislation, build mechanism of third-party authentication, and regulate third-party service industry. At the end of the chapter, the case of Shanghai honesty-credit system construction of is introduced to describe China honesty-credit status.

Chapter VI, "*Towards a Scalable Role and Organization Based Access Control Model with Decentralized Security Administration*" addresses the problems that arise from the fact that traditional role-base access control (RBAC) models do not scale up well for modeling security policies spanning multiple organizations. After reviewing recently proposed Role and Organization Based Access Control (ROBAC) models, the authors, Xinwen Zhang of The College Board, USA; Zhixiong Zhang of Samsung Information System, USA; and Ravi Sandhu of University of Texas at San Antonio and TriCipher Inc., USA, present and formalize an administrative ROBAC model called AROBAC07. Authors used two examples to motivate and demonstrate the usefulness of ROBAC while providing a comparison between AROBAC07 and other administrative RBAC models. The authors show that ROBAC/AROBAC07 can significantly reduce administration complexity for applications involving a large number of organizational units. Finally, an application compartment-based delegation model is introduced in the chapter, which provides a method to construct administrative role hierarchy in AROBAC07. Authors show that the AROBAC07 model provides convenient ways to decentralize administrative tasks for ROBAC systems and scales up well for role-based systems involving a large number of organizational units.

There has been an unprecedented thrust in employing Computers and Communication technologies in all walks of life. The systems enabled by Information Technology are becoming more and more complex resulting in various threats and vulnerabilities. The security properties like confidentiality, integrity, and availability are becoming more and more difficult to protect. In **Chapter VII**, "*Enterprise Information System Security: A Life-Cycle Approach*", a life-cycle approach to achieve and maintain security of enterprises has been proposed. The chapter first examines enterprise information systems and then discusses the need for enterprise information system security and problems associated with security implementation. The authors, Chandan Mazumdar, Mridul S. Barik, and Anirban Sengupta from Jadavpur University, India, consider enterprise information system security as a management issue and detail the information security parameters. Finally, the chapter proposes security engineering life-cycle in detail including Security Requirement Analysis, Security Policy Formulation, Security Infrastructure Advisory Generation, Security Testing and Validation, and Review and Monitoring phases.

Most companies would agree that securing their information assets is worth some investment. It is thus plausible to assume that low levels of IT security investment indicate that only a small portion of the firm's business is IT asset value driven. It could also point to a misaligned corporate investment policy. Conversely, some firms may be investing more than is warranted, given the value of their information asset holdings, thereby wasting shareholder resources. The question then becomes: What level of IT security investment is enough? Several models exist to help companies set their IT spending in general and Information Security spending in particular. The leading model out there is the Information Technology Portfolio Management (ITPM) model, which is a financial portfolio management theory applied to the information technology realm to optimize IT spending based on a number of factors like business value, efficiency, and cost reduction among others. Despite current vigorous research at esteemed institutions like the Center for Information Systems Research (CISR) at MIT and at the Free University of Amsterdam, ITPM is still in its infancy and the field would benefit from alternative models. In **Chapter VIII**, "*An Alternative Model of Information Security Investment*", the author, Peter O. Orondo, president, Acclaim Consulting Group Inc., USA, proposes an alternative model of IT security spending that firms may readily apply when setting their Information Security budgets. The model is analytical and begins by developing a model for the business value of information. It then develops a model for the cost of an information security breach. Finally, the author presents a relationship between the value model and the cost model.

The second Section, ***Privacy and Social Engineering***, of the book contains 7 chapters on privacy issues and social engineering threats and countermeasures. The chapters in this section cover policy-based privacy management, a country-specific privacy issues in banking sector, framework for defending against phishing attacks, context-dependent countermeasure against social engineering attacks, latest privacy enhancing technologies, social engineering taxonomy and countermeasures; and security challenges with social networking sites.

The growth of the Internet is increasing the deployment of e-services in areas as e-commerce, e-learning, and e-health. In parallel, the providers and consumers of such services are realizing the need for privacy. The use of P3P privacy policies on Web sites is an example of this growing concern for privacy. Managing privacy using privacy policies is a promising approach. In this approach, an e-service provider and an e-service consumer each have separate privacy policies. Before an e-service is engaged, the provider's policy must be "compatible" with the consumer's policy. However, beyond compatibility, the policies may face pitfalls arising from improper specification, misapplication, and improper maintenance (e.g. failing to keep a personal privacy policy up-to-date). This can result in the loss of privacy and even lead to serious safety issues in certain cases. **Chapter IX**, "*Avoiding Pitfalls in Policy-Based Privacy Management*," by George O. M. Yee and Larry Korba of National Research Council, Canada, gives examples of how such pitfalls can arise and suggests ways to avoid these pitfalls.

Enabling customers to influence the way they are represented in a bank's databases is one of the major personalization, responsiveness, and privacy issues in banking. **Chapter X**, "*Privacy and Banking in Australia*," draws on the results from a qualitative study of the ways in which Australians think of privacy, security, and money. The authors, Supriya Singh, RMIT University, Australia; Margaret Jackson, RMIT University, Australia; and Jenine Beekhuyzen, Griffith University, Australia, find that changes in life stages, residence, and relationships motivate people to share additional personal information with their bank, in order to receive personalized services. The authors suggest ways in which privacy rights management can help customers better represent themselves in a flexible manner reflecting the changes in their lives.

Phishing scams pose a serious threat to end-users and commercial institutions alike. E-mail continues to be the favorite vehicle to perpetrate such scams mainly due to its widespread use combined with the ability to easily spoof them. Several approaches, both generic and specialized, have been proposed to address this growing problem. However, phishing techniques, growing in ingenuity as well as sophistication, render these solutions weak. To overcome these limitations, authors, Madhusudhanan Chandrasekaran, State University of New York, Buffalo, USA, and Shambhu Upadhyaya, State University of New York, Buffalo, USA, propose a multistage framework – the first stage aims at detecting phishing based on their semantic and structural properties and the second stage proposes a proactive technique based on a challenge-response technique to establish the authenticity of a Web site. The authors in **Chapter XI**, "*A Multistage Framework to Defend Against Phishing Attacks*", use live e-mail data to demonstrate that their approach is able to detect a wider range of phishing attacks than existing schemes.

In recent years, the security research community has been very active in proposing different techniques and algorithms to face the proliferating security vulnerabilities. However, social engineering remains an alarming threat to most secured networks. Security administrators are certainly aware of the significance of the human factor irrespective of the strength of the applied technological measures. The human factor is still a difficult-to-surround notion and a difficult to quantify concept. It is rarely considered in the early stages of the development life cycle of software, assuming traditional security considerations have been taken into account. In **Chapter XII**, "*A New Approach to Reducing Social Engineering Impact*", the authors, Ghita Kouadri Mostéfaoui, Oxford University Computing Laboratory, UK, and Patrick Brézillon, LIP6, University Paris 6, France, discuss the added-value of *context* as a way to deal with social engineering. Based on a case study describing a typical attack, the authors provide a first attempt to model this parameter.

Privacy-enhancing technologies (PETs), which constitute a wide array of technical means for protecting users' privacy, have gained considerable momentum in both academia and industry. However, existing surveys of PETs fail to delineate what sorts of privacy the described technologies enhance, which makes it difficult to differentiate between the various PETs. Moreover, those surveys could not consider very recent important developments with regard to PET solutions. In **Chapter XIII**, "*Privacy-Enhancing Technologies*," authors, Yang Wang, University of California, Irvine, USA and Alfred Kobsa, University of California, Irvine, USA, provide an analytical framework to differentiate various PETs. This analytical framework consists of high-level privacy principles and concrete privacy concerns. The authors use this framework to evaluate representative up-to-date PETs, specifically with regard to the privacy concerns they address, and how they address them (i.e., what privacy principles they follow). Based on findings of the evaluation, authors also outline several future research directions.

Chapter XIV, "*Social Engineering and its Countermeasures*," introduces and defines social engineering, a recognized threat to the security of information systems. The chapter introduces a taxonomy for classifying social engineering attacks along four dimensions: (1) who or what the targets are, (2) what media are used, (3) how the attacks fit in an attack cycle and (4) what are the techniques used to execute

the attacks. Additionally, the author, Douglas P. Twitchell, Illinois State University, USA, discusses current social engineering countermeasures and how to map attack types to these countermeasures. Use of the taxonomy should help security professionals and researchers understand social engineering attacks, and implementation of the discussed current and future countermeasures should help professionals reduce the risks associated with social engineering attacks. Finally, the chapter ends with a discussion of future trends and technologies for defending against social engineering attacks.

Social networking has become one of the most popular applications on the Internet since the burst of the dot-com bubble. Apart from being a haven for teenagers and online marketers, social networking sites are increasingly adopted by the corporate community. The trend makes viable many new business models and applications. The popularity of these sites has altered the way society interacts, but it has also greatly heightened the threats of cyber crime. Safety and crime issues aside, the massive amount of user-generated content in the Web 2.0-enabled social networking sites are becoming fertile grounds for all kinds of malware such as viruses and Trojan horses. Furthermore, these sites pose great challenges on how to protect copyrighted works as they are havens for digital content sharing. Society must learn to balance the benefits of social networking with its drawbacks as the phenomenon is an inescapable global trend. Author, Tom S. Chan, Southern New Hampshire University, USA, presents opportunities and security challenges that social networking sites pose in **Chapter XV**, "*Social Networking Site: Opportunities and Security Challenges*".

The third section of the book, ***Security Education and Awareness***, contains 7 chapters on information security and assurance education and research issues. The section has chapters on design and implementation issues in information security curriculum and education and on research issues in emerging fields in information security.

Fraudulent e-mails, known as phishing attacks, have brought chaos across the digital world causing billions of dollars of damage. These attacks are known for their ability to exploit the human aspect of a computer system by pretending to originate from a source trusted by the victim. While technology defenses have been setup for protection, people are still succumbing to these attacks at alarming rates. Therefore, educational techniques must be implemented to strengthen the human factor of security. Authors, James W. Ragucci, Syracuse University, USA, and Stefan A. Robila, Montclair State University, USA, in **Chapter XVI**, "*Designing Antiphising Education*", propose the use of a phishing IQ test that when used in classroom setting can help users build experience needed to identify phishing e-mail during their daily routine.

Chapter XVII, "*Theories Used in Information Security Research: Survey and Agenda*," discusses the recent theories used in information security research studies. The authors Serkan Ada, Raj Sharman, and Manish Gupta, of State University of New York, Buffalo, USA, introduce the importance of the information security research and why it has become so important recently. Following the introduction, "theory" is defined and the importance of the theories in information security research is mentioned. The chapter then goes on to discuss recently used theories (socio-technical systems theory, activity theory, distributed cognition theory, general deterrence theory, grounded theory, social cognitive theory), while presenting basic information about these theories as well as applications from the literature. Other recently used theories are also summarized. The chapter finally ends with concluding remarks on the theories and recommendations to the researchers in the information security area.

Information assurance education is an interdisciplinary endeavor that when taken only as a holistic and inclusive educational activity it can be successful. Authors, Samuel P. Liles and Reza Kamali, of Purdue University Calumet, USA, suggest in **Chapter XVIII**, "*Information Assurance and Security Curriculum Meeting the SIGITE Guidelines*," that during the design and implementation of a curriculum that is set to meet standards set by outside agencies, the educational institution must use a flexible and

repeatable process. Building a curriculum on top of a strong foundation will empower and facilitate success. Authors suggest that meeting outside agencies' requirements, such as accrediting agencies, will close, if not eliminate any credibility gaps within an institution.

As with health and safety or legal compliance, management can hardly expect employees to comply with corporate information security policies, adopt security standards, and follow security procedures if they don't even know of their existence. Information security awareness is therefore an essential component of effective information security management systems, supporting and enhancing the technical and procedural information security controls and contributing to the corporation's overall governance. Author, Gary Hinson, IsecT Ltd, New Zealand, suggests in **Chapter XIX**, "*Information Security Awareness*," that in order to instill a genuine security culture throughout the organization, the awareness issue goes well beyond simply informing employees of their security obligations. To overcome the inevitable change in resistance or inertia, employees have to be both informed and motivated to modify their behaviors; "think security and act securely". The chapter explains the challenges and details information security awareness approaches that work, using quotations from others in the field to illustrate the points made.

Security training and awareness is often overlooked or not given sufficient focus in many organizations despite being a critical component of a layered defense. Organizations often purchase expensive hardware and software to help secure their organization, but fail to allocate resources to train employees who will install and configure the product. Similarly, organizations will devote many hours developing polices and procedures to protect sensitive information, but fail to allocate the appropriate resources to ensure awareness of those policies and procedures. Authors, Nick Pullman, Citigroup, USA, and Kevin Streff, Dakota State University, USA, in **Chapter XX**, "*Creating a Security Education, Training, and Awareness Program*," discusses how to design, create, and implement a formal security education, training, and awareness (SETA) program as a component of a layered defense strategy.

Chapter XXI, "*Information Security Within an E-Learning Environment*," introduces information security within the educational environments that utilize electronic resources. The education environment experienced a paradigm shift over the past number of years, due to the rapid growth in technology. This growth has made it possible for the education environment to utilize electronic services to enhance education methods. However, it is vital that all education environments (traditional or new ones) ensure that all resources (lecturers, students, and data) are properly protected against any possible security threats. Authors of **Chapter XXI**, E. Kritzinger, University of South Africa, Pretoria, South Africa, and S. H von Solms, Rand Afrikaans University, Johannesburg, South Africa, highlight the importance of securing information within the electronic environment. The authors present key aspects that must be addressed and implemented to ensure information security. The chapter also identifies four information security pillars that could assist top management to enhance overall information security management.

Authors, Donald Murphy from a northeast U.S. financial services firm and Manish Gupta, State University of New York, Buffalo, USA, and H. R. Rao, State University of New York, Buffalo, USA, present five emerging areas in information security that are poised to bring the radical benefits to the information security practice and research in **Chapter XXII**, "*Research Notes on Emerging Areas of Conflict in Security*". Authors have selected these five areas based on extensive literature review and emerging trends in information technology and security. This is a theoretical discourse, which considers a number of research issues and paradigms and explores the relevance of some interesting research areas that have far-reaching implications for IS research. The chapter stimulates discussions about the five covered research areas and in doing so provides a call for information security researchers to be more aware of the research methodological options available to them. For each area, the chapter provides background and existing research along side rationale on why the area is becoming important and vital in the field of information security research. The chapter introduces five key areas of information security research that are gaining recognition and credibility to significantly aid information security practice.

The last section of the book, ***Human and Interaction Issues***, deals with human, behavioral and psychological aspects of managing an information security program and practices. The section hosts chapters on different issues on the topics of linguistic steganography, password aspects, security issues with interactive systems, role of gender and social influence on security vulnerabilities, shill bidding detection, privacy, and security in large public displays and emotional trust factors.

Chapter XXIII, "*The Human Attack in Linguistic Steganography*" develops a linguistically robust encryption system, LUNABEL, which converts a message into syntactically and semantically innocuous text. Drawing upon linguistic criteria, LUNABEL uses word replacement, with substitution classes based on traditional linguistic features (syntactic categories and subcategories), as well as features under-exploited in earlier works: semantic criteria, graphotactic structure, and inflectional class. The original message is further hidden through the use of cover texts—within these, LUNABEL retains all function words and targets specific classes of content words for replacement, creating text which preserves the syntactic structure and semantic context of the original cover text. LUNABEL takes advantage of cover text styles which are not expected to be necessarily comprehensible to the general public, making any semantic anomalies more opaque. Authors, C. Orhan Orgun, University of California, Davis, and Vineeta Chand, University of California, Davis, suggest that this line of work has the promise of creating encrypted texts that are less detectable to human readers than earlier steganographic efforts.

The traditional approach to security has been the use of passwords. They provide the system with a barrier to access that was quite safe in the analogical world. The digital era provided the means to easily try thousands of passwords in a short period of time and now the password schema is no longer safe. Now it suffers of the password's contradiction: the fact that it requires both simplicity and complexity to be usable and safe. Being so, new technologies are required that can preserve the ease of use, but can provide stronger authentication processes. Authors, Sérgio Tenreiro de Magalhães, Faculdade de Ciências Sociais da Universidade Católica Portuguesa, University of Westminster, UK; Kenneth Revett, Departamento de Sistemas de Informação da Universidade do Minho, Portugal; Henrique M. D. Santos, Departamento de Sistemas de Informação da Universidade do Minho, Portugal; Leonel Duarte dos Santos, Departamento de Sistemas de Informação da Universidade do Minho, Portugal; André Oliveira, Departamento de Sistemas de Informação da Universidade do Minho, Portugal; and César Ariza, Bogomovil Ltda, Columbia, in **Chapter XXIV**, "*Using Technology to Overcome the Password's Contradiction*," present the latest advances in three technologies that can be used, unaided or together, to improve the safety of user/password schemas without significant changes in the protected information system architecture, despite the human factors that traditionally reduce the security of those systems. The chapter presents technologies such as Keystroke Dynamics, Graphical Authentication, and Pointer Dynamic.

Reducing the likelihood of human error in the use of interactive systems is increasingly important. Human errors could not only hinder the correct use and operation, they can also compromise the safety and security of such systems. Hence the need for formal methods to analyze and verify the correctness of interactive systems, particularly with regards to human interaction. **Chapter XXV**, "*Formal Analysis of Security in Interactive Systems*," examines the use of formal modeling and analysis of security properties of interactive systems. The chapter introduces some basic concepts in security and human-computer interaction, followed by formal modeling of human cognitive behavior and analysis of such systems. Authors, Antonio Cerone, United Nations University, China, and Siraj A. Shaikh, United Nations University, China, highlight the use of model checking to drive the system development to design secure user actions and sequences of actions. Authors also analyze the patterns of user behavior that may lead to security violation. Finally, particular areas of security protocol design where human interaction plays a key role are discussed.

It is estimated that over 1 billion people now have access to the Internet. This unprecedented access and use of Internet by individuals around the world, however, is accompanied by malicious and mis-

chievous activities online. With the traditional crimes such as fraud, identity theft, and harassment now being committed with the use of the Internet, and networked home computers being exploited to carry out attacks such as denial of service, spamming, phishing, and virus/worm propagation, it has become important to investigate security and privacy issues as they pertain to individual Internet users. To date very little is known about what characteristics of Internet users affect their computing and online behaviors as they relate to security online. While some attention has been paid to understand the security issues affecting corporations, research investigating security issues as they relate to home users is still in infancy. Drawing from disciplines such as criminology, sociology, consumer fraud, and information security, **Chapter XXVI**, "*Internet Crime: How Vulnerable Are You? Do Gender, Social Influence and Education Play a Role in Vulnerability?*" seeks to find the role of computing skills and computer training, social influence, and gender on person's vulnerability to Internet crimes. Authors of the chapter 26, Tejaswini Herath, State University of New York, Buffalo, USA; H. R. Rao, State University of New York, Buffalo, USA, and Shambhu Upadhyaya, State University of New York, Buffalo, USA, assert that the findings of the study presented in the chapter are significant and shed light in this important area of Internet crime contributing to the information security literature.

Shill bidding is where spurious bids are introduced into an auction to drive up the final price for the seller, thereby defrauding legitimate bidders. While shilling is recognized as a problem, presently there is little or no established means of defense against shills. **Chapter XXVII**, "*Detecting Shill Bidding in Online English Auctions*," presents an algorithm to detect the presence of shill bidding in online auctions. The authors, Jarrod Trevathan, James Cook University, Australia, and Wayne Read, James Cook University, Australia, show that the algorithm observes bidding patterns over a series of auctions, providing each bidder a score indicating the likelihood of his/her potential involvement in shill behavior. The algorithm has been tested on data obtained from a series of realistic simulated auctions, and commercial online auctions. The algorithm is able to prune the search space required to detect which bidders are likely to be shills. This has significant practical and legal implications for commercial online auctions where shilling is considered a major threat. This chapter presents a framework for a feasible solution, which acts as a detection mechanism and a deterrent.

In **Chapter XXVIII**, "*Information Security at Large Public Displays*," authors Carsten Röcker, University of California, San Diego, USA; Carsten Magerkurth, SAP Research, Switzerland and Steve Hinske, Institute for Pervasive Computing, Switzerland, present a novel concepts for personalized privacy support on large public displays. In a first step, two formative evaluations are conducted in order to analyze the requirements of potential users regarding the protection of private information on large public displays. The insights gained in these evaluations are used to design a system that automatically adapts the information visible on public displays according to the current social situation and the individual privacy preferences of the user working on the display. In a third evaluation, the developed system is evaluated regarding its appropriateness for daily usage and its usefulness to protect privacy. The results of the evaluation showed that users are in general willing to trust system-based protection mechanisms, provided that they are well implemented. In this context, the proposed combination of pre-defined privacy profiles and context-adapted information visualization proved to be a good trade-off between usability and adequate privacy protection.

In **Chapter XXIX**, "*The Sense of Security and Trust*," the sense of security, identified with the Japanese term, Anshin, is identified as an important contributor to emotional trust. This viewpoint, put forth by the authors of the chapter, Yuko Murayama, Iwate Prefectural University, Japan; Carl Hauser, Washington State University, USA; Natsuko Hikage, Iwate Prefectural University, Japan and Basabi Chakraborty, Iwate Prefectural University, Japan, suggests that designers should consider the subjective sense of security as well as objective security measures in designing systems and their user interfaces. A

survey of users reveals both the personal and the environmental factors contributing to the users' sense of security when using the Internet. A more encompassing view of Anshin as including safety, reliability, and other non-functional properties of systems may provide additional insights for system design.

Manish Gupta & Raj Sharman
State University of New York at Buffalo, USA

REFERENCES

Al-Ghatani, S. S., & King, M. (1999). Attitudes, satisfaction and usage: Factors contributing to each in the acceptance of information technology. *Behaviour & Information Technology, 18*, 277-297.

Anderson, R. (1993). Why cryptosystems fail. In *Proc. ACM CCS'93*, pages 215–227, Fairfax, VA, Nov. 1993.

Burger, K. (1993). The new age of anxiety. *Insurance and Technology, 18*(10), 48–54.

Carstens, D. S. (2008). Human and Social Aspects of Password Authentication. *Social and Human Elements of Information Security: Emerging Trends and Countermeasures.* Eds: Manish Gupta and Raj Sharman. IGI Global, Hershey, PA. 2008

Dutta, A., & McCrohan, K. (2002). Management's role in information security in a cyber economy. *California Management Review, 45*(1), 67-88.

Franklin, J., Paxson, V., Perrig, A., & Savage, S. (2007). An inquiry into the nature and causes of the wealth of Internet miscreants. In *Proc. ACM CCS'07*, Alexandria, VA, Oct./Nov. 2007.

Gordon, S. (1994). The generic virus writer. In Proc. Intl. Virus Bulletin Conf., pages 121-138, Jersey, Channel Islands, 1994.

Gordon, S. (2000). Virus writers - The end of the innocence? In *10th Annual Virus Bulletin Conference (VB2000)*, Orlando, FL, Sept. 2000.

Helander, M. G., Landauer, T. K., & Prabhu, P. V. (Eds.). (1997). *Handbook of human-computer interaction*. Amsterdam: Elsevier.

Kaplan-Leiserson, E. (2003). People and plans: Training's role in homeland and workplace security. *T+D, 57* (9).

Loch, K. D., Carr, H. H., & Warkentin, M. E. (1992). Threats to information systems: Today's reality, yesterday's understanding. *MIS Quarterly, 17*(2), 173–186.

Markus, M. L. (1983). Power, politics, and MIS implementation. *Communications of the ACM, 26*, 430–444.

Olivia, R. (2003). Will your information survive? *Marketing Management, 12*(1). Business Source Elite Database 10613846.

Panettieri, J. C. (1995). Information Week/Ernst and Young security survey. *Information Week, 555*, 32–37.

Straub, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research, 1*(3), 255–276.

Turnage, J. J. (1990). The challenge of new workplace technology for psychology. *American Psychologist*, *45*, 171–178.