SECTION I: INFORMATION SECURITY AND PRIVACY:
THREATS AND SOLUTIONS

The primary mission of information security is to ensure that information systems and their contents remain impervious to unauthorized access and modification, thereby guaranteeing the confidentiality, integrity and availability of information. Although Information Security can be defined in a number of ways, the most salient is set forth by the government of the United States. The National Institute of Standards and Technology (NIST) defines Information Security based on the 44 United States Code Section 3542(b)(2), which states “Information Security is protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability” (NIST, 2003, p3). The Federal Information Security Management Act (FISMA, P.L. 107-296, Title X, 44 U.S.C. 3532) defines Information Security as “protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction” and goes on to further define Information Security activities as those “carried out in order to identify and address the vulnerabilities of computer system, or computer network” (17 U.S.C. 1201(e), 1202(d)).

The overall goal of information security should be to enable an organization to meet all of its mission critical business objectives by implementing systems, policies and procedures to mitigate IT-related risks to the organization, its partners and customers (NIST, 2004). Information systems face attacks on a daily basis from threats both inside and outside the organization. Insider threats include, but are not limited to poorly trained employees, disgruntled employees, and ignorant employees. Outsider threats include hackers, crackers, phreakers, former employees and forces of nature (Whitman, 2004). Insider threats can be overcome with a combination of stringent formal policies and informal security education awareness and training (SETA) programs. Outsider threats, on the other hand, imply a non-stop cat-and-mouse game between the hackers and the IS security personnel on who outwits the other. More often than not it is the hackers who have the upper hand, as they have nothing to lose, while the organizations have no option but to come up with real-time solutions for each attack from the potential threats or stand to lose the very proprietary information which helps them gain a competitive advantage.

Any information security initiative aims to minimize risk by reducing or eliminating threats to vulnerable organizational information assets. The National Institute of Standards and Technology (NIST, 2003, p. 7) defines risk as “…a combination of: (i) the likelihood that a particular vulnerability in an agency information system will be either intentionally or unintentionally exploited by a particular threat resulting in a loss of confidentiality, integrity, or availability, and (ii) the potential impact or magnitude of harm that a loss of confidentiality, integrity, or availability will have on agency operations (including mission, functions, and public confidence in the agency), an agency’s assets, or individuals (including
privacy) should there be a threat exploitation of information system vulnerabilities,” Risks are often characterized qualitatively as high, medium, or low (NIST, 2003, p 8). The same publication defines threat as “…any circumstance or event with the potential to intentionally or unintentionally exploit a specific vulnerability in an information system resulting in a loss of confidentiality, integrity, or availability,” and vulnerability as “…a flaw or weakness in the design or implementation of an information system (including security procedures and security controls associated with the system) that could be intentionally or unintentionally exploited to adversely affect an agency’s operations (including missions, functions, and public confidence in the agency), an agency’s assets, or individuals (including privacy) through a loss of confidentiality, integrity, or availability” (NIST, 2003, 9). NetIQ (2004) discusses five different types of vulnerabilities that have direct impact on the governance of information security practices. They are: exposed user accounts or defaults, dangerous user behavior, configuration flaws, missing patches and dangerous or unnecessary service. An effective management of these vulnerabilities is critical for three basic reasons. First, an effective vulnerability management helps reducing the severity and growth of incidence. Second, it helps in regulatory compliance. And third and the most important reason can be summed as simply saying, it is a “good business practice” to be proactive in managing the vulnerabilities rather than be reactive by trying to control the damage from an incidence.

That sets the stage for Section I which highlights four different types of threats including credit card frauds, e-mail worms, rootkits, and threats from network administrators, and analyzes their impacts on the organization.

The first chapter in Section I focuses on the important issue of online credit card fraud and explores ways to protect against it. “A Rule-Based and Game-theoretic Approach to On-Line Credit Card Fraud Detection” is authored by Vishal Vatsa, Shamik Sural, and Arun K. Majumdar. The authors observe that as the use of credit cards increases, so does the possibility of fraud committed by thieves trying to steal credit card information. In this chapter, the authors present a novel approach to dealing with this problem. The model presented in this chapter is based on the assumption that the conflicting motives between an intruder, who is trying to commit fraud, and an intrusion detection system, that is trying to prevent it, can be viewed as a multistage game between two players, each trying to maximize its own payoff. Although the basic ideas of game theory have been applied successfully in many settings, their applications in information security and privacy have been very limited. In applying the game theory, the authors consider the specific application of credit card fraud detection systems and propose a two-tiered architecture having a rule-based component in the first tier and a game-theoretic component in the second tier. The ideas of game-theoretic are used to develop a predictive application in which the intruders are viewed as rational adversaries who would try to behave optimally, and therefore their expected optimal behavior can be determined through game theory.

The focus of the second chapter in this section, “Email Worm Detection Using Data Mining” authored by Mohammad M. Masud, Latifur Khan, and Bhavani Thuraisingham, is application of data mining techniques to detect e-mail worms. The authors explore three different data mining approaches to automatically detect e-mail worms. First, the authors apply either Naïve Bayes (NB) or Support Vector Machine (SVM) on the unreduced dataset, without any feature reduction, and train a classifier. In the second approach, the authors reduce dimensionality using Principal Component Analysis (PCA) and apply NB or SVM on the reduced data and train a classifier. The third approach is to apply a feature-selection technique is called Two-phase Selection (TPS), which is a novel combination of decision tree and greedy selection algorithm. Finally, the trained classifiers are tested on a dataset containing both known and unknown types of worms. The authors’ experiments indicate that the best performance is achieved by TPS, and that the best classifier is SVM. Thus the authors strongly recommend applying SVM with our two-phase selection process for detecting novel email worms in a feature-based paradigm.
The third chapter in Section I is titled: “Information Systems Security: Cases of Network Administrator Threats” by professors Hamid Jahankhani, Shantha Fernando, and Mathews Nkhoma. The authors discuss the importance of network administrators in organizations achieving their desired network security objectives. The authors observe that while information systems network security depends on network designers at the early stages of implementation, in the long term, the network administrators who look after day-to-day network and system functions are the most important, since the initial security level designs can later be changed, improved, or compromised by the network administrators. To illustrate the authors provide two case studies where the influence of network administrators is highlighted.

The last chapter in this section: “Rootkits and What we Know: Assessing U.S. and Korean Knowledge and Perceptions” is authored by professors Kirk P. Arnett, Mark B. Schmidt, Allen C. Johnston, Jongki Kim, and HJ Hwang. The authors present the results of their survey conducted among students of eight Korean and U.S. higher educational institutions regarding their knowledge and experience of various forms of computer malware, in general and rootkits, in particular. A rootkit is a relatively new form of malware that allows its user to gain top level (root) privileges where the rootkit is installed. It is not a virus or a worm but it may deliver a virus or worm. Once installed, if a backdoor mechanism is made available to the attacker, the rootkit will allow the attacker to “own” the machine. The authors believe that rootkit threat levels are not well understood. The authors’ goal is to assess the knowledge levels and perceptions of Korean and U.S. college students regarding rootkits and more traditional malware with an eye toward identifying possible problems or solutions that might surface. Results of the survey indicate that though the two groups are similar in many respects, they exhibit significant differences in self-reported perceptions of rootkit familiarity. U.S. respondents report a higher level of rootkit awareness compared to their Korean counterparts. Perhaps the greater issue here is that the awareness and knowledge of rootkits is limited in both countries. The authors believe that to solve this problem of limited awareness, proactive response must surface and the rootkit awareness curve accelerated to improve worldwide malware protection.

SECTION II: PRIVACY PRESERVATION AND TECHNIQUES

Information privacy is an elusive term to define. Although there are many attempts to articulate a definition for information privacy, the most salient one was first put forth by Westin (Westin, 1967) as a “right of an individual” to determine when, how, and to what extent information about him/her is communicated to others. Information security, on the other hand, has been more successfully defined. The United States’ National Information Assurance Training and Education Center (NIATEC) defines information security as “a system of administrative policies and procedures” for identifying, controlling, and protecting information against unauthorized access to or modification, whether in storage, processing, or transit (NIATEC, 2006). These definitions have profound implications for the way information security and privacy is viewed as a field of study. These definitions imply that an individual has the right and must be able to exercise a substantial degree of control over the data about him/her and its use. However, the exercise of this control is contingent upon the security of systems that collect, store, process, and transmit that information. Hence, the relationship between information security and information privacy can be viewed as synergistic and mutually symbiotic in that, without information security, privacy protection cannot be guaranteed and, without a concerted concern over the protection of privacy, most information security promises can be construed as vain.

Advances in technology are causing new privacy concerns. According a survey by U.S. Department of Commerce, an increasing number of Americans are going online and engaging in several online activities, including online purchases and conducting banking online. The growth in Internet usage and
e-commerce has offered businesses and governmental agencies the opportunity to collect and analyze information in ways never previously imagined. “Enormous amounts of consumer data have long been available through offline sources such as credit card transactions, phone orders, warranty cards, applications and a host of other traditional methods. What the digital revolution has done is increase the efficiency and effectiveness with which such information can be collected and put to use” (Adkinson, Eisenach, & Lenard, 2002). The significance of privacy has not been lost to the information security and ethics research and practitioners’ communities as was revealed in Nemati and Barko (Nemati et al., 2001) of the major industry predictions that are expected to be key issues in the future (Nemati et al., 2001). Chiefly among them are concerns over the security of what is collected and the privacy violations of what is discovered ((Margulis, 1977), (Mason, 1986), (Culnan, 1993), (Smith, 1993), and (Milberg, S. J., Smith, & Kallman, 1995)). About 80 percent of survey respondents expect data mining and consumer privacy to be significant issues (Nemati et al., 2001).

Technologies such as data warehousing have allowed business organizations to collect massive amounts of data which could then be passed through data mining tools and techniques that intelligently and automatically sift through that data to discover meaningful and previously hidden information. If this new information is not used properly, it can create privacy concerns. People feel violated when their privacy is invaded. Privacy invasions lead directly to lost sales. The solution is to make privacy a corporate priority throughout all levels of the organization. The bottom line is that privacy preservation must be viewed as a business issue, not a compliance issue.

This important issue of privacy is the focus of Section II where different techniques such as privacy-preserving data mining, privacy-preserving clustering, privacy-preserving transactions protocol using mobile agents, and autonomous user privacy control are highlighted and the possibilities of using quantum computing to solve information privacy issues are explored.

The first chapter in Section II is titled, “Privacy-Preserving Data Mining and the Need for Confluence of Research and Practice” and is coauthored by professors Lixin Fu, Hamid Nemati, and Fereidoon Sadri. In this chapter, privacy-preserving data mining (PPDM) is defined as data mining techniques developed to protect the privacy of sensitive data while allowing useful information to be discovered from the data. In this chapter, the authors observe that the practice of privacy-preserving data mining, as mandated by the regulatory agencies, currently cannot keep up with the pace of advances in technologies supporting data mining. This incongruence in the research and the practice of privacy-preserving data mining makes it imperative that a comprehensive research agenda be charted relevant to practice and as a reference basis for future related legislation activities.

The second research chapter in this section is titled “A Dimensionality Reduction-Based Transformation to Support Business Collaboration” and is authored by Stanley R. M. Oliveira and Osmar R. Zaíane. In this chapter, the authors argue that while the benefits of data sharing for the purpose of data mining are immense, so are the concerns over the privacy violations resulting from such data sharing. Rather than simply preventing data sharing to enhance privacy, the authors present a solution designed to meet privacy requirements while guaranteeing valid data clustering results. The chapter introduces an innovative method called dimensionality reduction-based transformation (DRBT) that preserves privacy in a shared data environment.

The use of mobile agents in e-commerce to achieve privacy is the crux of the third chapter in Section II. The third chapter is titled, “Privacy-Preserving Transactions Protocol Using Mobile Agents with Mutual Authentication”, and is coauthored by Song Han, Vidyasagar Potdar, Elizabeth Chang, and Tharam Dillon. This chapter introduces a new transaction protocol using mobile agents in electronic commerce. This protocol is developed based on the assumption that a privacy-preserving e-commerce transaction requires that both the customer and the provider to become committed in protecting the privacy of the customer. This approach is based on mutually-authenticated transactions achieved by using mobile agents.
The focus of the fourth chapter in this section, “Dynamic Control Mechanisms for User Privacy Enhancement” authored by Amr Ali Eldin, is to allow end users to exert automatic and manual control over their private information. The authors propose a consent decision-making mechanism, the Sharing Evaluation Model (ShEM), for this purpose. The authors developed an enhanced fuzzy logic approach for the automatic decision-making process. The proposed mechanism has been prototyped and integrated in a UMTS location-based services testbed platform called Mobile Information and Entertainment Services (MIES) on a university campus. The service was implemented and used by two groups of users in real time. A survey of users’ responses on the privacy functionality has been carried out and analyzed as well. Users’ response on the privacy functionality was positive. Additionally, results obtained showed that a combination of both manual and automatic privacy control modes in one approach is more likely to be accepted than only a complete automatic or a complete manual privacy control.

The fifth chapter in Section II deals with the intriguing new idea of quantum computation and discusses its implications for information security, privacy research, and practice. “A Projection of the Future Effects of Quantum Computation on Information Privacy” by Geoff Skinner and Elizabeth Chang presents quantum computation as a digital/computing environment that utilizes quantum mechanical principles and technologies in its operation to process data. In traditional computers, data is represented as a series of binary bits, and computational processes are achieved by manipulation of these bits. However, in quantum computers, the processing engine is a quantum computational environment, and data is represented as a series of “qubits,” where data can be either 0 or 1 or it can simultaneously hold two or more functional values. This has profound implications on how data is processed, including encryption and authentication. The authors point out that although the area of quantum computation is still in its infancy, and a truly functional quantum computer has not been implemented, it is anticipated that within the next decade it may be feasible. The authors provide an overview of the key issues in information privacy that will be impacted with the expected evolution and realization of quantum computation and provide guidelines for researchers in information security and privacy seeking to exploit the opportunities provided by it.

SECTION III: AUTHENTICATION TECHNIQUES

Authentication is the process of attempting to verify the digital identity of the sender of a communication by obtaining his/her identification credentials such as name and password and validating those credentials against some authority (OWASP, 2008). If the credentials are valid, the user is considered an authenticated identity. Authentication tools provide the ability to ensure that a message came from who it claims to have come from. All authentication schemes are based on the possession of some secret information known only to the user and possibly (but not necessarily) to the authentication system itself. Communications with other parties use this secret in a way that allows the recipient to verify that the user possesses the secret, but that does not divulge the secret itself. This means that the secret itself cannot be shared, since to do so would allow the recipient to impersonate the user on subsequent interactions with other parties. One of the major differences between authentication systems lies in how to prove you know the secret without telling it (Wells, 1996).

Authentication is defined as a “Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual’s authorization to receive specific categories of information” (CNSS, 2003. p 5). In order for a system to achieve security, it should require that all users identify themselves before they can perform any other system actions. Once the identification is achieved, authorization should be the next step. Authorization is process of granting permission to a subject to access a particular object. Authentication is the process of establishing the validity of the
user attempting to gain access, and is thus a basic component of access control, in which unauthorized access to the resources, programs, processes, systems are controlled. Access control can be achieved by using a combination of methods for authenticating the user. The primary methods of user authentication are: access passwords, access tokens, something the user owns which can be based on a combination of software or hardware that allows authorized access to that system (e.g., smart cards and smart card readers), the use of biometrics (something the user is, such as a fingerprint, palm print or voice print), access location (such as a particular workstation), user profiling (such as expected or acceptable behavior), and data authentication, to verify that the integrity of data has not been compromised (CNSS, 2003).

Authentication is important as it forms the basis for authorization (determining whether a privilege will be granted to a particular user or process), privacy (keeping information from becoming known to non-participants), and non-repudiation (not being able to deny having done something that was authorized to be done based on the authentication) (Wells, 1996).

The vital topic of authentication receives well-deserved attention in Section III with chapters that focus on the design of authentication systems, use of the two-factor interlock authentication protocol to defeat phishing attacks, and use of watermarking to increase the authentication capabilities of existing mechanisms.

The focus of the first research chapter in Section III is on the design of authentication systems. This chapter, titled “On the Design of an Authentication System Based on Keystroke Dynamics Using a Pre-defined Input Text” is authored by Dieter Bartmann, Idir Bakdi, and Michael Achatz. The authors realize the difficulty in the design of authentication systems based on keystrokes dynamics, which are highly influenced by fluctuation of the individual typing behavior. This paper presents an asymmetrical method to overcome this difficulty. The paper presents the empirical results of an extensive field test study.

The second chapter in this section deals with a very timely issue of Internet phishing and how to defeat it. “Defeating Active Phishing Attacks for Web-Based Transactions” is authored by Xin Luo and Teik Guan Tan. Internet phishing is a term first used in 1996 by hackers who were trying to steal account information from AOL account holders. These hackers would collect personal and account information fraudulently by pretending to represent legitimate entities. In this chapter, the authors observe that up to now the best defense against Internet phishing has been the use of two-factor authentication systems and argue that this solution, while effective, is not fool-proof and provides no defense against man-in-the-middle, or active phishing. The authors provide evidence that active phishing attacks have crippled the growth of Web-based transactional systems and observe that even with vigilant users and prudent applications, no solutions seem to have addressed the attacks comprehensively. The authors propose a new two-factor interlock authentication protocol (TIAP), adapted from the interlock protocol with two-factor authentication, which is able to defend successfully against active phishing attacks. Through the use of simulating a series of attacks against this protocol, the authors assess the robustness of the TIAP protocol and demonstrate how each attack can be defeated.

The last chapter in Section III provides a very interesting watermarking approach to increase authentication mechanisms. “A Content-Based Watermarking Scheme for Image Authentication Using Discrete Wavelet Transform Inter-Coefficient Relations” is authored by Latha Parameswaran, and K. Anbumani. The authors observe that the proliferation of multimedia on the Internet has led to the need for developing authentication mechanisms and proposes a new blind watermarking scheme based on the contents of the image in the discrete wavelet transform domain for image authentication. Watermarking is a method in which an image or a digital pattern is embedded or sometimes hidden in an electronic document in order to enhance its authenticity. The approach presented in this chapter is based on a “discrete wavelet transformation” method in which the relationship between neighboring wavelet coefficients in each band of the second level decomposition is considered to construct the content-based watermark. The watermark is embedded in the first level mid frequency band, of the discrete wavelet transformed image. The
received image is authenticated by extracting the watermark and determining the level of authenticity. This scheme is capable of tolerating content-preserving modifications and detecting content-changing modifications. Experimental results prove the efficiency of the scheme.

SECTION IV: SECURITY AND PRIVACY MANAGEMENT

Privacy is a set of expectations, with or without a legal basis, existing within certain relationships (for example: consumer / service provider) regarding the collection, control, use, transfer, storage and disclosure of information. Privacy management is quickly becoming a core business concern across most industries. Privacy management is no longer about just staying within the letter of the latest law or regulation. Privacy policies and procedures that cover all of the organization’s online and offline operations must be put in place. Regulatory complexity will grow as privacy concerns surface in scattered pieces of legislation. Companies need to respond quickly and comprehensively. They must recognize that privacy is a core business issue.

Privacy concerns are real and have profound and undeniable implications on people’s attitude and behavior (Sullivan, 2002). The importance of preserving customers’ privacy becomes evident when we study the following information: In its 1998 report, the World Trade Organization projected that the worldwide Electronic Commerce would reach a staggering $220 billion. A year later, Wharton Forum on E-commerce revised that WTO projection down to $133 billion. What accounted for this unkept promise of phenomenal growth? Census Bureau, in its February 2004 report stated that “Consumer privacy apprehensions continue to plague the Web and hinder its growth.” In a report by Forrester Research it is stated that privacy fears will hold back roughly $15 billion in e-commerce revenue. In May 2005, Jupiter Research reported that privacy and security concerns could cost online sellers almost $25 billion by 2006. Whether justifiable or not, consumers have concerns about their privacy and these concerns have been reflected in their behavior. The chief privacy officer of Royal Bank of Canada said “Our research shows that 80% of our customers would walk away if we mishandled their personal information.”

Privacy considerations will become more important to customers interacting electronically with businesses. As a result, privacy will become an import business driver. People (Customers) feel ‘violated’ when their privacy is invaded. They respond to it differently, despite the intensity of their feelings. Given this divergent and varied reaction to privacy violation, a lot of companies still do not appreciate the depth of consumer feelings and the need to revamp their information practices, as well as their infrastructure for dealing with privacy. Privacy is no longer about just staying within the letter of the latest law or regulation. As sweeping changes in attitudes of people their privacy will fuel an intense political debate and put once-routine business and corporate practices under the microscope. Two components of this revolution will concern business the most, rising consumer fears and a growing patchwork of regulations. Both are already underway. Regulatory complexity will grow as privacy concerns surface in scattered pieces of legislation. Companies need to respond quickly and comprehensively. They must recognize that privacy should be a core business issue. Privacy policies and procedures that cover all operations must be enacted. Privacy Preserving Identity Management should be viewed as a business issue, not a compliance issue.

Privacy implies many things to the organization. It means risk management, compliance, gaining a competitive advantage over competitors and forming a trust-building vehicle with customers. Managing privacy involves more than simply creating and posting a privacy policy. If an organization posts a policy and then does not verify that the policy is being followed in actual practice, the privacy policy can become more of a liability than an asset. Responsibly managing privacy involves a comprehensive
process of assessing an organization’s data use needs, putting in place appropriate privacy practices, posting a privacy policy that reflects those practices and establishing processes that allow management to verify compliance with the stated policy.

The chapters in Section IV are dedicated to ethical issues and privacy management and discuss the role of privacy in the age of eCRM, the role of privacy risk in its acceptance and the effect of increased knowledge on privacy concerns and e-commerce personalization preferences.

The first research chapter in Section IV looks at privacy and security issues in Electronic Customer Relationship Management (e-CRM). This chapter is titled, “Privacy and Security in the Age of Electronic Customer Relationship Management” and is coauthored by Nicholas Romano, Jr. and Jerry Fjermestad. This chapter presents a value exchange model of privacy and security for electronic customer relationship management. The value exchange model requires that customer preferences for privacy and security and the enterprise requirement to sell goods and services be balanced. The model is an integration of the customer sphere of privacy, the sphere of security, and the privacy/security sphere of implementation.

The second research chapter in this section presents an empirical study of the impact of privacy risk in the acceptance of information technology. The chapter is titled, “The Impact of Privacy Risk Harm (RH) and Risk Likelihood (RL) on IT Acceptance”, and is authored by Joseph A. Cazier, E. Vance Wilson, and B. Dawn Medlin. The authors speculate that risk and concerns over privacy violations impact the adoption of technology. Technology acceptance model (TAM) is extended to include perceptual measures of privacy risk harm and privacy risk likelihood. The result of their study confirms the notion that privacy risks play an important role in the use of information technology.

The final research chapter in Section IV presents a provocative idea that ignorance about privacy risks can be bliss. The chapter is titled “Ignorance is Bliss: The Effect of Increased Knowledge on Privacy Concerns and Internet Shopping Site Personalization Preferences” and is authored by Thomas P. Van Dyke. The author observes that while people claim that privacy matters to them, they often do things while browsing that are risky in terms of privacy and posit that this seeming inconsistency between professed privacy concerns and risky behavior on the Internet may be more a consequence of ignorance rather than irrationality. An experiment to determine if people understood the privacy violation risks of technology, would that knowledge alter their level of privacy concern and their preferences concerning e-commerce Web site personalization. Results indicate that increased awareness of information gathering technology resulted in significantly higher levels of privacy concern and significantly reduced preferences for Web site personalization.

SECTION V: WEB SECURITY AND PRIVACY ISSUES AND TECHNOLOGIES

The W3C defines a Web service as “a software system designed to support interoperable machine-to-machine interaction over a network. It has an interface described in a machine-processable format (specifically WSDL). Other systems interact with the Web service in a manner prescribed by its description using SOAP-messages, typically conveyed using HTTP with an XML serialization in conjunction with other Web-related standards.” (W3C, 2004)

A Web service is simply an application that exposes a function that is accessible using standard Internet technologies and that adheres to Web services standards. Web services promote platform independence as they can be developed for and deployed onto any platform using any programming language. Web services use the Web Services Description Language (WSDL) to specify a service contract. A consumer of a Web service uses a service registry called Universal Description, Discovery and Integration (UDDI) to dynamically discover and locate the description for a Web service. Web service is one of the Web
2.0 technologies that organizations are embracing to drive up their bottom lines. In a McKinsey global survey conducted in January 2007, more than 80% of the respondents indicated that they were either currently using or planning to use Web services in the near future (McKinsey, 2007).

The W3C defines Semantic Web as a methodology that provides a common framework that allows data to be shared and reused across application, enterprise, and community boundaries. (W3C, 2004). The Semantic Web is a web of data. The Semantic Web is about two things. It is about common formats for integration and combination of data drawn from diverse sources, where on the original Web mainly concentrated on the interchange of documents. It is also about language for recording how the data relates to real world objects. That allows a person, or a machine, to start off in one database, and then move through an unending set of databases which are connected not by wires but by being about the same thing. The Semantic Web will bring structure to the meaningful content of Web pages, creating an environment where software agents roaming from page to page can readily carry out sophisticated tasks for users. The Semantic Web is not a separate Web but an extension of the current one, in which information is given well-defined meaning, better enabling computers and people to work in cooperation (Berners-Lee, 2007).

Together Web services and Semantic Web have the potential to transform the way computer-to-computer and people-to-computer communications take place. This forms the perfect backdrop for Section V which articulates the trustworthiness of Web services, privacy and trust management for the semantic web, and an ontology of information security.

The focus of the first chapter in this section is on the security of Web services. This chapter is titled, “Trustworthy Web Services: An Experience-Based Model for Trustworthiness Evaluation” and is co-authored by Stephen J. H. Yang, Blue C. W. Lan, James S. F. Hsieh, and Jen-Yao Chung. Web Services technology is defined as a set of software tools designed to support the interoperability of services over a network. This paradigm requires that the service provider and the service requester each follow a set of protocols. In this chapter, authors observe that although Web services technology has made seamless integration of different software possible, the trustworthiness of the component software remains problematic. This is due to the fact that to achieve a secure transaction in a Web services environment, the service requester needs to make an informed decision regarding the trustworthiness of the service provider. They present an experience-based method to evaluate the trustworthiness of the service provider. This approach is based on the understanding of trust experience and trust requirements of the service provider and the service requester. The use of ontology to specify past experience of services and the trustworthy requirements of the requester is presented.

The second chapter in Section V is titled, “Administering the Semantic Web: Confidentiality, Privacy and Trust Management” and is co-authored by Bhavani Thuraisingham, Natasha Tsybulnik, and Ashraf Alanam. In this chapter, the authors introduce the Semantic Web as a collection of technologies to support information interoperability. They point out that in order to achieve secure, confidential, and private information interoperability, a set of administration policies needs to be defined. Administration policies of the Semantic Web have been described, and techniques for enforcing these policies are outlined. Specifically, the authors discuss an approach for ensuring confidentiality, privacy, and trust for the Semantic Web.

In the third chapter in this section “An Ontology of Information Security”, authors Almut Herzog, Nahid Shaharbary, and Claudiu Duma present a publicly available, OWL-based ontology of information security which models assets, threats, vulnerabilities and countermeasures and their relations. The authors’ goal is to present an ontology that provides a general overview over the domain of information security, contains detailed domain vocabulary and is thus capable of answering queries about specific, technical security problems and solutions, and supports machine reasoning. The authors designed their
ontology according to established ontology design principles and best practices to ensure that it is collaboratively developed and acceptable to the security and ontology community. All the core concepts are subclassed or instantiated to provide the domain vocabulary of information security. Relations connect concepts. Axioms, implemented as OWL restrictions, model constraints on relations and are used to express, for example, which countermeasure protects which asset and which security goal. Inference and the query language SPARQL allow additional views on the ontology. They can show countermeasures that protect the confidentiality of data, countermeasures that detect integrity violations, threats that can compromise the availability of a host etc. Inference also assists in finding countermeasures for a given threat. The authors propose that their work can be used as online learning material for human users, as a framework for comparing security products, security attacks or security vulnerabilities, as a publicly available knowledge base for rule-based reasoning with semantic web applications and as a starting point and framework for further extensions and refinements.

SECTION VI: EVALUATING INFORMATION SECURITY AND PRIVACY: WHERE ARE WE GOING FROM HERE?

The requirement to measure information security performance is driven by regulatory, financial, and organizational reasons. A number of existing laws, rules, and regulations cite information performance measurement, in general, and information security performance measurement in particular, as a requirement. These laws include the Clinger-Cohen Act, the Government Performance and Results Act (GPRA), the Government Paperwork Elimination Act (GPEA), and the Federal Information Security Management Act (FISMA) (NIST, 2008).

The key components of effective information security are strong upper-level management support, existence of information security policies and procedures backed by the authority necessary to enforce compliance, quantifiable performance measures that are designed to capture and provide meaningful performance data, and results-oriented performance measures analysis (NIST, 2008).

Evaluating information security is critical since it has the potential to shed light on the state of security within the organization, the level of threats facing the organization, the readiness of the organization to deal with incidents, the adequateness of the organization’s disaster recovery and business continuity plans, and the effectiveness of protection of information assets of the organization.

The goal of Section VI is to bring the key issue of information security evaluation to the limelight by discussing the effectiveness of information security using a theoretical model and investigates a simulation model of information systems security.

The focus of the first research chapter in Section VI is in measuring the effectiveness of information security activities. The chapter is titled “Information Security Effectiveness: Conceptualization and Validation of a Theory” and is authored by Kenneth J. Knapp, Thomas E. Marshall, R. Kelly Rainer, Jr., and F. Nelson Ford. The chapter presents a sequential qualitative-quantitative methodological approach to propose and test a theoretical model of information security effectiveness. The proposed model includes four variables through which top management can positively influence security effectiveness: user training, security culture, policy relevance, and policy enforcement. The chapter links the finding of the study to existing top management support literature, general deterrence theory research, and the theoretical notion of the dilemma of the supervisor.

The second chapter in this section “A Simulation Model of IS Security” is authored by Norman Pendegraft and Mark Rounds. The purpose of this research chapter is to develop a model sufficiently robust to provide management insight into the merits of alternative responses. In this chapter, the authors
offer a simulation model for simulating interactions between an information system (IS), its users, and a population of attackers. The model incorporates plausible interactions between the rate of attacks, the value of the IS, user sensitivity to security, user specific response curve to security and the level of security. These interactions are incorporated into a reservoir / flow model using the IThink simulation software. The model depends on four fundamental constructs: VALUE, USAGE, ATTACKS, and SECURITY. The authors perceive VALUE construct as a reservoir, USAGE and ATTACKS as flows, and SECURITY as a control parameter representing the management decision. Results suggest that the marginal value of additional security may be positive or negative as can the time rate of change of system value. This implies that IT security policy makers should be aware of where they are in the state space before setting IT security policy.

CONCLUSION AND FINAL THOUGHTS

Until recently, information security and privacy were exclusively discussed in terms of mitigating risks associated with data and the organizational and technical infrastructure that supported it. With the emergence of the new paradigm in information technology, the role of information security and privacy has evolved. As information technology and the Internet become more and more ubiquitous and pervasive in our daily lives, a more thorough understanding of issues and concerns over the information security and privacy is becoming one of the hottest trends in the whirlwind of research and practice of information technology. This is chiefly due to the recognition that whilst advances in information technology have made it possible for generation, collection, storage, processing and transmission of data at a staggering rate from various sources by government, organizations and other groups for a variety of purposes, concerns over security of what is collected and the potential harm from personal privacy violations resulting from their unethical uses have also skyrocketed. Therefore, understanding of pertinent issues in information security and privacy vis-à-vis technical, theoretical, managerial and regulatory aspects of generation, collection, storage, processing, transmission and ultimately use of information are becoming increasingly important to researchers and industry practitioners alike. Information security and privacy has been viewed as one of the foremost areas of concern and interest by academic researchers and industry practitioners from diverse fields such as engineering, computer science, information systems, and management. Recent studies of major areas of interest for IT researchers and professionals point to information security and privacy as one of the most pertinent.

REFERENCES


American Institute of Certified Public Accountants (AICPA) information security tops the list of ten most important IT priorities, 2007. Accessed from: http://infotech.aicpa.org/Resources.


