Communications of the Association for Information Systems

Volume 20 Paper

December 2007

Management of Information Security: Challenges and Research Directions

Joobin Choobineh
Texas A&M University, JChoobineh@mays.tamu.edu

Gurpreet Dhillon
Virginia Commonwealth University, g.dhillon-alumni@lse.ac.uk

Michael R. Grimaila
Air Force Institute of Technology

Jackie Rees
Purdue University

Recommended Citation
Choobineh, J., Dhillon, G., Grimaila, M., & Rees, J. (2007). Management of Information Security: Challenges and Research Directions. Communications of the Association for Information Systems, 20, pp-pp. https://doi.org/10.17705/1CAIS.02057

Communications of the Association for Information Systems

MANAGEMENT OF INFORMATION SECURITY: CHALLENGES AND RESEARCH DIRECTIONS

Joobin Choobineh
Information and Operations Management
Texas A&M University
JChoobineh@mays.tamu.edu

Gurpreet Dhillon
School of Business
Virginia Commonwealth University

Michael R. Grimaila
Department of Systems and Engineering Management
Air Force Institute of Technology

Jackie Rees
Krannert Graduate School of Management
Purdue University

ABSTRACT

Over the past decade management of information systems security has emerged to be a challenging task. Given the increased dependence of businesses on computer-based systems and networks, vulnerabilities of systems abound. Clearly, exclusive reliance on either the technical or the managerial controls is inadequate. Rather, a multifaceted approach is needed. In this paper, based on a panel presented at the 2007 Americas Conference on Information Systems held in Keystone, Colorado, we provide examples of failures in information security, identify challenges for the management of information systems security, and make a case that these challenges require new theory development via examining reference disciplines. We identify these disciplines, recognize applicable research methodologies, and discuss desirable properties of applicable theories.

Keywords: management of security, research methods, desirable properties of theories

I. INTRODUCTION

Historically, management of information security has mostly relied on technical control measures; however, research has shown that the majority of information security failures occur because of violations of controls by trusted personnel. This suggests that management of information security can only be adequately assured if the emphasis goes beyond technical controls and incorporates business process and organizational issues. Management of information security is primarily concerned with strategic, tactical, and operational issues surrounding the planning, analysis, design, implementation, and maintenance of an organization's information security program. Some of the most salient issues include asset valuation, auditing, business continuity

planning, disaster recovery planning, ethics, organizational communication, policy development, project planning, risk management, security awareness education/training, and various legal issues such as liability and regulatory compliance.

In this paper, we document the discussions and findings that the authors identified during a panel presented at the 2007 Americas Conference on Information Systems held in Keystone, Colorado. The panel was formed after numerous discussions between the authors who recognized that information security management is a relatively immature discipline and that it requires additional academic study. We believe that there is a growing need for research to verify/confirm the management challenges, discover current management deficiencies, identify best practices, devise methodologies, and specify requirements for the management of information security. In this paper, we provide examples of failures in information security, present some of the challenging issues in information security, and discuss emerging issues we have encountered in our experiences to provide motivation and directions for future research.

II. THE MANAGEMENT OF INFORMATION SECURITY

Information security management is the process of administering people, policies, and programs with the objective of assuring continuity of operations while maintaining strategic alignment with the organizational mission [Cazemier et al. 2000]. Ideally, information security management activities should be driven by organizational objectives so that no resources are expended on security without an explicit documented understanding of how it supports the organizational mission. Historically, information security management has been dealt with solely by establishing technical and physical controls. However, the increasing use, value, and dependence on computerized systems to support real world operations have increased the importance of incorporating process and organizational issues in security risk management [Drucker 1999; Blakley et al. 2001]. Information security risk management, the process used to identify the optimal protection strategy when constrained by a limited security budget, has evolved as a required function within organizations which are concerned with their ability to mitigate the effects of a breach of information security [Finne 2000]. Such breaches are referred to as “incidents.” Risk analysis, the first step of the risk management process, requires the identification and documentation of critical organizational resources (e.g., information, people, processes, and technologies) among a huge number of total information resources that are used to support the organizational mission. Determining criticality is not trivial. It requires an estimation of the value the resource provides to the organization based upon how it supports the organization’s strategic objectives [Mercuri 2005]. The scale and complexity of the organization, interdependencies between resources, and the dynamic nature of resource utilization greatly complicate value determination. However, an accurate resource valuation is essential as it directly impacts the quality of the decisions made during risk management [Finne 2000]. The valuation, in conjunction with an estimation of threats, vulnerabilities, and the likelihood (per unit time) of their intersection, is used to determine the potential damage to a resource, given the state of the organizational security capability [Gordon and Loeb 2002]. Collectively, this information provides the ability to rank order and address risks by risk avoidance (e.g., change processes), transference (e.g., outsource), mitigation (e.g., apply control measures), or acceptance (e.g., accept possible losses), commensurate with the value of the resource.

Proper day-to-day and strategic management of information security operations are among critical success factors in achieving organizational goals. Pipkin [2000] identifies a cyclic, five-phase process to conceptualize the information security management process: inspection, protection, detection, reaction, and reflection. The inspection phase requires the identification, valuation, and assignment of ownership of information assets critical to the organization; the protection phase requires the assignment of the control measures to protect critical information assets commensurate with their value; the detection phase requires the development of robust detection capabilities to insure that any breach of the organization is detected in a timely manner; the reaction phase requires that the organization has developed the resources and capabilities to quickly respond, contain, investigate, and remediate breaches; and the reflection phase requires

effective post-incident documentation, reporting, and accountability to assure institutional learning. Pipkin asserts that assuring organizational security requires consideration of all the five phases. Neglecting any one of the five phases can expose the organization to excessive losses when they inevitably experience an information incident. Unfortunately, as will be shown in the next section, organizations are not aware of, choose not to, or are not capable of implementing these phases in an effective and efficient manner.

III. EXAMPLES OF FAILURES IN INFORMATION SYSTEM SECURITY MANAGEMENT

In this section, we present two examples. The first is an example of an actual incident. The second is hypothetical, though with a high likelihood of occurrence. These examples represent a small sample of the types of problems that can occur when managing an organizational information security program. First, consider the May 2005 information security breach of CardSystems Solutions, Inc. (CSSI), a small credit card transaction processing company, located in Tucson, Arizona, that employed approximately 115 people [Consumer Affairs 2005; FTC Complaint 2006]. CSSI provided credit card transaction processing products and services to approximately 119,000 different merchants, enabling them to accept American Express, Discover, MasterCard, and VISA credit cards and debit cards as payment [House 2005]. At the time of the incident, CSSI was processing over 210 million transactions for approximately $15 billion dollars per year. The breach was not detected by CSSI but instead by MasterCard, who had received complaints from affiliate banks that CSSI was the source of a potential fraud. A forensic investigation of the CSSI incident revealed that a database containing credit card information had been compromised nine months prior to the detection of the incident, which resulted in the theft of more than 40 million credit card records [Mimoso 2006]. This was quite remarkable, because CSSI had retained the credit card records in direct violation of the VISA Cardholder Information Security Program and their contractual agreements with VISA, MasterCard, American Express, and Discover. While at the time few details were released about the incident, it was revealed that CSSI information systems had been breached via its Internet facing Web server using a well-known security exploit called a Structured Query Language injection attack [Mimoso 2006]. The inability for CSSI to properly implement protection, detection, and reaction serves as a textbook example of the spectacular damage that can occur due to improper information security management. The fallout from the incident prompted congressional hearings; resulted in legal and regulatory actions; revealed problems related to accountability, auditing, due diligence, and notification; and demonstrated the consequences of failing to properly maintain an effective information security program.

Even organizations that maintain a strong and effective security capability can suffer significant mission impact and loss if they do not explicitly document their information security risk management information [Fung et al. 2003; Grimaila and Fortson 2007]. Consider a hypothetical scenario that demonstrates the consequences that can occur when documentation aspects of information security management are not properly implemented. In this scenario, a deployed military organization is conducting an active military operation on foreign soil. One element of the operation requires the periodic delivery of supplies between facilities located in different parts of the country via ground vehicles. The commander of the logistics unit uses a logistics management program that stores the convoy routes and schedules in a network connected database. The local database is overloaded, so a system administrator decides to relocate the logistics database to a database server located in another organizational unit without documenting the change. As often occurs, access to the network is provided to a coalition partner to facilitate information sharing on an unrelated operation. Unfortunately, the coalition partner does not enforce stringent access control policies to the network. As a result, an adversary breaches the coalition partner's system and uses it as a conduit to gain access to, and breach, the database server containing convoy routes and schedules. A short time later, the incident is detected and the adversary's access to the database is terminated. An Incident Response Team (IRT) is dispatched to investigate the breach. It finds the cause for the breach and begins to remediate the system. A key responsibility of the IRT is to notify organizations that have information stored on the system that their information might have been compromised. The

problem is that no explicit documentation exists which identifies all of the information owners who have information stored in the database. Over the next few days, the IRT reconstructs a list of information owners to notify them of the breach and to gain an understanding of the loss due to the unavailability of the system during remediation. Before the IRT can complete their investigation and notify the affected parties, one of the convoys whose schedule was listed in the database is ambushed, leading to a significant loss of life and loss of supplies. While the scenario presented is hypothetical, it reveals the consequences that can result from failing to implement a strict change management process, failing to sufficiently restrict access to partners, and failing to properly protect critical information resources.

These examples illustrate the damage that can occur from information breaches and demonstrate opportunities for improvements in information security management. In the first case, if CSSI had properly implemented a vulnerability assessment and patching process, developed an intrusion detection capability, and/or periodically audited their information systems, they may have prevented (or mitigated) the breach. In the second case, if there were a mechanism to document information dependencies and insure that all information consumers who critically depended upon information were notified immediately when a breach occurs, the commander would have rerouted the convoy and prevented the ambush. In many cases, proven policies, procedures, and practices exist that can significantly mitigate or eliminate risks. However, organizations are often indifferent to, incapable of, or simply choose not to implement the required protective measures. The reasons why organizations fail to implement such measures when available appear to be extremely complex and require substantial research. In order to provide the rationale for the kinds of research that are needed, a deeper understanding of the challenges in the management of information security is required.

IV. CHALLENGING ISSUES IN MANAGEMENT OF INFORMATION SECURITY

The management of information security faces three major challenges. First, even after decades of research in the theory and practice of IS security, its management is usually considered as an afterthought. Second, largely because security is considered as an afterthought, the problem of development duality creeps in. Third, conceptualizations of information security have largely been atheoretical. We believe that a focus on these three challenges will help in defining and addressing many of the problems in managing information security, as evidenced in the case examples in the previous section.

IS SECURITY AS AN AFTERTHOUGHT

The problem of information security being considered as an afterthought dates back to the era of checklists. Once a system has been implemented, it was a norm to follow a checklist to address whether any of the security ‘holes’ remained unplugged. While the information security community has recognized the inadequacy of checklists as a means to address security concerns, the checklist culture has, however, prevailed. Therein resides the problem of information security being considered as an afterthought. The lack of recognition of the importance of accounting for security during system and product development has resulted in little or no budget allocation for security. The result is that, if there is any security, it tends to be “bolted-in” rather than “baked-in.”

Checklist culture in the era of risk analysis has perhaps done the most disservice to the information system and information security communities relative to the purist use of risk analysis. The purpose of risk analysis has always been defined as the product of the probability of occurrence of events and their cost. In order for risk analysis to be useful, it is important to identify assets that need to be protected, since any calculation of probability of occurrence of a negative event is in the context of assets that need to be protected. However, checklist culture forces one to identify and classify criticality of assets based on some predetermined list. At the same time, the classification of assets is largely vendor driven, without any consideration of the context of use. This results in risk analysis being applied to assets that have never been

compromised. Conventional wisdom from probability theory tells us that probability of occurrence of events can only be accurately calculated if there is data on occurrence of such events in the past. However, the prevalent checklist culture forbids this from happening. In the case of CSSI, this is what probably occurred. While the business was more interested in ensuring state of the art interfaces, security considerations emerged to be rather minimal, since many of the controls were checked, albeit based on old requirements.

Checklists have also been prevalent in the evaluation of information security. While the ease of use and convenience in deployment of controls listed in the checklists cannot be disputed, there are concerns about lack of considerations for the context and the business processes within which the checklists are applied. Clearly there is a need to go beyond checklists and define information security requirements in terms of what may be required by the organization. This will help in considering information security as an enabler of business rather than a requirement that needs to be fulfilled.

Had CSSI proactively evaluated their business environment and followed guidelines for archiving records, the breach would not have occurred. There is no doubt that good information security management can be achieved by proactively focusing on the quality of business processes rather than fulfilling requirements drawn for some checklist.

DEVELOPMENT DUALITY AND INFORMATION SECURITY

Development duality is a phenomenon where systems and security design are undertaken in parallel rather than in an integrated manner. This largely occurs when systems developers fail to recognize the security requirements at the onset of the development process.

In the literature, it has been argued that development duality can be overcome if security considerations are addressed at the logical design phase of systems development [Baskerville 1988] . This may be true, but one can argue that the real remedy of development duality is correctness of systems specification. In an ideal world, a correctly specified system should exactly model the real world. Therefore, requirements analysis is perhaps the most important stage of systems development, which provides input to the system specifications. Normally programmers tend to write code based on the requirements. This is where problems emerge. While it may make sense to take the complete set of requirements for developing the system, there is a significant semantic gap. It is therefore prudent to develop requirements for security policy that are based on the user requirements. This would be the first step in formally defining a high level security specification. A formal specification along with proper usability considerations feeds into the actual design of a system. Finally the actual code is written. By following a sequenced approach of this kind, it is possible to overcome development duality. Any failure to do so results in a semantic gap, which impacts the overall correctness in specification and hence the security of the system (see Fig 1).

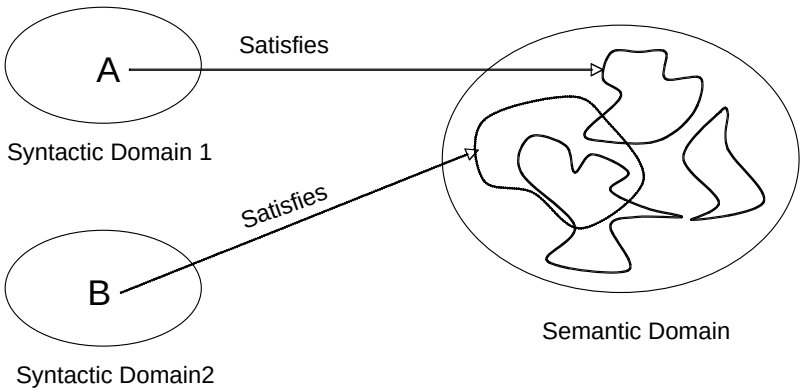

Figure 1. Correctness in Specification [based on Wing 1990]

Correctness in system specification is an important information security property. It prevents development duality from creeping into systems design. While specifying systems, the syntactic domain (the logical structure of the program) needs to satisfy the semantic domain (the abstraction of reality). Many times, however, the syntactic domain may only appear to satisfy the semantic domain, as in the case represented in Figure 1. While syntactic domain "A" correctly satisfies what needs to be formalized within a universe of discourse, syntactic domain "B" does not. It just satisfies part of the semantic domain. Clearly, this leads to misspecification with ensuing errors [see Wing 1990].

ATHEORETIC NATURE OF IS SECURITY METHODS AND TOOLS

A theory is a logical explanation of interactions of a set of phenomena that are capable of predicting future occurrences or observations of the same kind. Over the past several decades, the field of information security management has suffered because of a lack of theoretical conceptualizations. While many researchers have offered interesting insights, there are as yet no well-established principles that define "good" information security management. There are multiple factors which conspire to make any research effort difficult. First, organizations are as unique as human beings are. As a consequence, results collected and generalized from one organization in a given domain do not always translate well into other domains or for other organizations. Second, organizations are organic, dynamic entities that change over time. This fact can often undermine or invalidate an otherwise sound security architecture if it is not adaptive. Finally, the best policies, procedures, and practices will have little or no value if they are not followed. Many organizations have developed great guidance but fail to periodically audit their implementation and operational use. Even worse is when the consequences of committing a policy violation are not enforced, which is analogous to police never patrolling the highway for speeders. When this occurs, an organization may falsely believe that it is secure while its intellectual properties, trade secretes, and other assets are vulnerable and subject to be compromised. These factors have prevented IS security research from being cumulative.

These three challenges provide a significant number of opportunities for the researchers to leave their imprint upon the burgeoning stream of research on information security management.

V. RESEARCH OPPORTUNITIES

As a subfield of information systems discipline, information security management is still in its infancy. Practitioners and academics are clamoring for greater understanding of the problems presented by information security and assurance activities and more acutely, solutions to those problems. Therefore, there are tremendous opportunities for new and current researchers to make a significant impact on the field.

An ongoing area of inquiry is the relationship between information security risk management practices and other areas of risk management within the firm, or enterprise-wide risk management. For example, should there be a relationship between the activities undertaken in managing information-related risks and financial or legal risks? Given the increasing role of state and federal legislation regarding sensitive data losses in organizations, the need for alignment between legal and information risk management processes seems clear. However, there seems to be little in the way of organizational theory that would characterize this relationship. In practice, very few firms appear to position information security and assurance processes as part of the overall enterprise risk-management activities. Whether or not this is ideal is an open question.

Certainly, the risk-management approach to information security provides for the characterization of the rewards, or benefits of using sensitive data and information for decision making. However, in order to better balance this risk-reward equation, we need to better understand the nature of the risks involved and the activities undertaken to manage those risks. (We assume for the purposes of this paper that the rewards are well documented and appreciated.) Several researchers have tried to examine the risk assessment process itself, particularly in terms of the

common challenges faced by managers in approaching and executing the process [Baskerville and Portougal 2003; Sun, Srivastava, and Mock, 2006]. The attitudes, technologies, behaviors, and other phenomena are incorporated into the risks and activities under consideration. In order to fully appreciate these risks and the management of them, we need to step back and carefully examine the theories available within the reference disciplines of economics, strategic management, organizational behavior, psychology, and other potential sources for application to the security management problem.

REFERENCE DISCIPLINES AND EXAMPLES OF RESEARCH

Many reference discipline theories and/or frameworks that have been used or explored in the security context. These include economics, strategic management, psychology, deterrence theory, theory of planned behavior, resource based view (RBV) of the firm, rational choice theory, high reliability theory, normal accident theory, social control theory, agency theory, game theory, complexity theory, and cognitive dissonance theory. Certainly others are plausible.

Researchers have been delving into economic theories as they apply to managing the risks inherent in information management. Ross Anderson is often credited for initializing this stream of research [Anderson 2001; Gordon 2006]. Gordon and Loeb [Gordon and Loeb 2002] published the first economic analysis for rational investments in information security controls, making some headway against the Fear, Uncertainty, and Doubt (FUD) practice which is still common in the actual practice of security management. Other researchers, for example, August and Tunca [2006] examined network software security, particularly patching behaviors, within a game-theoretic environment. Managing intrusion detection systems from the firm value perspective was the focus of other research [Cavusoglu, Mishra, and Raghunathan 2005]. Gal-Or and Ghose [2005] also used game theory to study the effects of information sharing among firms for managing information security risks. We need to encourage further exploration of this domain as economics clearly is a strong motivating force in the actions and responses of firms, as well as attackers.

There is also a need to explore and assimilate theories from the strategic management literature. There exists a long history of theories, such as the behavioral theory of the firm [March and Simon 1958; Cyert and March 1963] and the resource-based view (RBV) of the firm [Wernerfelt 1984], that seek to explain firm behavior which will be vital to better understanding the security requirements and potentially effective responses of firms in managing their information risk.

Finally, there is a strong need to continue the survey of the psychology, sociology, and criminal justice literatures in terms of organizing and better understanding not only the criminal element of information risk but also the individual and employee role in information risk management. Some of the earliest work in the field [Straub and Collins 1990; Straub and Nance 1990; Goodhue and Straub 1991; Harrington 1996; Straub and Welke 1998] draws theoretical grounding from these disciplines. Further progress in this area has been made by Dhillon and Torkzadeh [2006], with the use of value focused thinking for strategizing about information security objectives. The strategy literature has significantly been influenced by sociology, so it seems prudent to delve into the sociological paradigms to inform information security theory development. Some initial guidelines have been provided by Dhillon and Backhouse [2001]. As more emphasis is placed on employees and other insiders being the “weakest link,” particularly as there is more interest from attackers on social engineering types of attacks, we will need much additional research into how to better manage this segment of the information security chain.

There is a substantial need to scrutinize current “best practices.” Best practices are often created using a “one size fits all” mentality which fails to account for organizational differences. These practices need to be assessed in terms of the theories catalogued above and then tested, both analytically and empirically as relevant. We also need to consider what linkages, if any, exist between security activities and corporate strategy, enterprise risk management, business intelligence, and knowledge management. For example, could security ever lead to a competitive advantage for firms outside the security product and service space? There also exists a need to

focus on the pressing issue of quickly securing the integration of new technologies into the organization, particularly wireless and mobile technologies. We also need to consider supply chain and virtual organizations.

Information security and assurance policies are the "vehicle" for managing the identified risks to the organization. However, there is a great deal of unknown regarding the proper management and use of security policies. More specifically, are there ideal designs for security policies in organizations? Are there tested guidelines for developing and implementing security policies that are tied to theory? When do we retire security policies? A few researchers are looking into this issue [Doherty and Fulford 2005]. Again, an inherently interdisciplinary approach is required.

Insider threat is another interesting problem that requires more research. While there have been great strides for protecting systems from outside threats, only modest work has been conducted on defending against the malicious insider [Gordon, Loeb, Lucyshyn, and Richardson 2005]. Are certain organizations more susceptible to insider threat? Are certain types of employees more susceptible to succumbing to temptation, opportunity, and so on? How can managers, security practitioners, and human resource professionals design and implement more effective programs to better manage this threat?

Additional research is also needed to explore successful security programs. Why are certain firms able to effectively implement and execute business continuity plans, which encompass various aspects of information security, whereas other firms struggle to do so in the face of various incidents affecting information assets? Why have organizations resisted implementing new technologies or improving procedures when it is so clear in hindsight, if not beforehand, that disastrous consequences are nearly inevitable? For example, the CSSI incident, where data was not deleted in violation of protocol, raises questions of why procedures were not followed. Was it purely a matter of economics? Overly optimistic thinking? Systems complexity overwhelming the information processing capabilities of managers? Lack of education and training?

POSITIONING OF RESEARCH METHODOLOGIES

Various methodologies can be and have been applied in conducting research in this field. Among others, these include analytics, empirical, lab experiments, and simulation. In addition, there still is a strong need for theory clarification and aggregation. The field is not mature enough to exclude any particular methodological approaches. There is definitely an opportunity to build theory here, and we explicitly invite our colleagues versed in qualitative techniques to add assistance here.

There are a growing number of analytical papers from the economics of information systems community. As mentioned earlier, a number of papers using game theory have been published in this arena, for example, August and Tunca [2006], Gal-Or and Ghose [2005], and Cavusoglu et al. [2005]. These papers are vital as they are attempting to link firm financial issues to security-related topics. These papers are important not only for understanding the economic phenomena surrounding information security in organizations but also for providing motivation for corporate funding for ongoing research. More analytical research with respect to quantitative managerial model analysis needs to be executed. Decision support in terms of statistical analysis, machine learning, and heuristics are all vital for today's managers working in a dynamic and complex environment. Hamill and colleagues adopted a value-focused thinking approach [Hamill, Deckro, and Kloeber 2005] for evaluating and assessing information assurance strategies. Genetic algorithms were used to match software vulnerabilities to specific security technology profiles [Gupta, Rees, Chaturvedi, and Chi 2006]. A risk-management approach to security investments has also been tried [Yue, Cakanyildirim, Ryu, and Liu 2007].

There is certainly a need for continued empirical work. We have seen a number of event studies published within the domain. However, many unanswered and conflicting results call for further and deeper research into this area. There is a growing interest in adoption and diffusion studies

of technologies, policies, and certifications. These studies should be encouraged, as they could have important policy implications for researchers and practitioners.

There have been few lab experiments performed via the experimental economics tradition. Depending on the framing of the research question, students may be sufficient proxies for employees and certainly for average home users. Certainly, in-depth field research, while difficult, expensive, and time-consuming, is needed. Another possibility is to incorporate "nonobvious" data sources. Are there security implications for organizations through employee use of FaceBook and MySpace? What about blogging or Second Life? Certainly, discussion boards and blogs have been of concern from a marketing and brand perspective, hence the creation of reputation management services. The Department of Defense has recognized these risks. On May 11, 2007, U.S. Army Commander General B.B. Bell signed a directive prohibiting access to 13 popular culture sites for operational security reasons [Associated Press 2007]. Are competitors able to locate more information about organizations on the Web than is prudent? What research opportunities do these media present to researchers, especially those working with large data sets or in knowledge discovery settings?

Finally, simulation has an important role to play. As we become more and more adept at agent-based simulation methods, these methods should find a role in scenario planning, validation and verification.

DESIRABLE PROPERTIES OF INFORMATION SECURITY THEORIES

The previous discussion emphasized the urgent need to identify existing applicable theories in the various reference disciplines as well as formulating security-specific theories in order to inform current and future research. Any theory identified or formulated needs to adhere to the following criteria:

- *Consistency.* Consistency refers to the property where all premises hold in the model. That is, the model proves that the theory is consistent. Usually any arbitrary model of a theory is sufficient to prove its consistency. However, in practice, it makes sense to find more natural models of the theory, meaning that we examine various models and assess if they conform to the mental models of a theory. This helps in safeguarding against not so obvious inconsistencies (e.g., inconsistencies because the background knowledge remains implicit).

- *Soundness*. Any theory presupposes assumptions grounded on the substantive field. One of the major challenges in developing a theory is to define the assumptions that need to be included. This requires a deep understanding of the field. Soundness refers to the ability to ground assumptions in the literature such that implicitly the theory makes sense.

- *Falsifiability*. A theory is scientific only if it is falsifiable [Popper 1959]. The attempt therefore is to find a model (or framework) in which the definitions hold and the assumptions (or a theorem) are false.

- *Satisfiability/Contingency*. The notion of satisfiability is one where the models or frameworks are true for the definitions and the assumptions. In such cases the empirical claims can be either corroborated or refuted.

- *Experience Explication*. An information security theory ought not to be just an opinion as to how security might exist in an organization. Rather it should be an attempt at formulating the meaning of its existence. This would be done by explicating the content of some very definitive experiences. Such experiences would obviously have to be logically classified and interpreted. The argument of such a theory would not be arbitrary, but it would derive its validity from the aggregate of experiences. Such a theory should invoke or suggest occurrence of parallel experiences, which in many ways would be an empirical

test of the truth of a theory. If a theory is unable to identify some sort of an explication of experiences, then at best the theory may be considered irrelevant or it may be rejected.

A careful consideration of these criteria facilitates systematic development of theory that helps in explaining and predicting occurrences. Such a theory is needed for information security.

IV. CONCLUSIONS

Modern organizations are heavily dependent on their computerized information systems for their low-level day-to-day operations, high-level strategic decision-making process, and all the administration functions in between these two. Given this dependency, organizations have become increasingly vulnerable to attacks through their networks and their information systems. Proper management of information security has become a very important consideration. As this paper was developed from a panel discussion, the comments from the members of the audience further underscored the importance of addressing the various problems of information security from a multitude of perspectives. Audience members ranged from seasoned researchers looking for new research questions to practitioners transitioning into academia. The questions ranged from potential publication outlets to working more closely with industry in identifying and addressing problems of interest. It appeared quite clear that everyone in the room was in agreement that information security is not only a technical issue, best left to our computer science and engineering colleagues, but is a risk management and business process issue, that must be viewed through multiple lenses.

In order to properly address this issue, we have identified three relevant management problems. These are: 1) addressing security after the system has been developed, resulting in an overall less secure system; 2) parallel design of security and information systems; and 3) lack of theories in the development of solutions to these problems. This identification provides a fertile ground for development and testing of new theories. We suggested various reference disciplines for this development. Among others, these include economics, game theory, strategic management, psychology, sociology, and criminology. Research methodologies for developing and testing the theories could vary widely from ethnographical methods to various types of experiments. The most important consideration in developing the theories is that they should explain at least one and preferably a collection of similar experiences in the field. This requires deep understanding of real world security management problems followed by their classification, categorization, and attribution. It is clear to us that opportunities for research in the information system security domain will continue to grow as our dependence on information technology grows.

DISCLAIMER

The views expressed in this paper are those of the authors and do not reflect the official policy or position of the United States Air Force, the Department of Defense, or the U.S. Government.

REFERENCES

EDITOR'S NOTE: The following reference list contains the address of World Wide Web pages. Readers, who have the ability to access the Web directly from their computer or are reading the paper on the Web, can gain direct access to these references. Readers are warned, however, that:

1. These links existed as of the date of publication but are not guaranteed to be working thereafter.

2. The contents of Web pages may change over time. Where version information is provided in the References, different versions may not contain the information or the conclusions referenced.

3. The authors of the Web pages, not CAIS, are responsible for the accuracy of their content.

4. The author of this article, not CAIS, is responsible for the accuracy of the URL and version information.

Associated Press. (2007). "Defense Department Blocks YouTube, MySpace from Military Computers," Fox News, May 14, 2007, http://www.foxnews.com/story/0,2933,272014,00.html

Anderson, R. (2001). "Why Information Security is Hard - An Economic Perspective," *17th Annual Computer Security Applications Conference*. New Orleans, LA.

August, T.,and T. I. Tunca. (2006). "Network Software Security and User Incentives," *Management Science*, (52)11, pp. 1703-1720.

Baskerville, R. L. and V. Portougal. (2003). "A PossibilityTheory Framework for Security Evaluation in National Infrastructure Protection," *Journal of Database Management*, (14)2, pp. 1-13.

Baskerville, R. (1988). *Designing Information Systems Security*. New York: John Wiley & Sons.

Blakely, B., E. McDermott, and D. Geer. (2001). "Information Security is Information Risk Management," *Proceedings of the 2001 Workshop on New Security Paradigms* (Cloudcroft, NM, Sept. 10-13), New York: ACM Press pp. 97-104.

Cavusoglu, H., B. Mishra, and S. Raghunathan. (2005). "The Value of Intrusion Detection Systems in Information Technology Security Architecture," *Information Systems Research*, (16)1, pp. 28-46.

Cazemier, J. A., P. L. Overbeek, and L. M. Peters. (2000) *Security Management (IT Infrastructure Library Series)*, Stationery Office, UK.

Consumer Affairs. (2005). "Latest Security Breach Exposes 40 Million Credit Card Accounts to Potential Fraud," ConsumerAffairs.com, http://www.consumeraffairs.com/news04/2005/cardsystems.html

Cyert, R. and J. March. (1963). *A Behavioral Theory of the Firm, 2nd Edition,* Blackwell Publishers Inc, Malden, MA.

Dhillon, G. and J. Backhouse. (2001). "Current Directions in IS Security Research: Towards Socio-Organizational Perspectives," *Information Systems Journal* 11(2): 127-153.

Dhillon, G. and G. Torkzadeh. (2006). "Value Focused Assessment of Information System Security in Organizations," *Information Systems Journal* 16(3): 293-314.

Doherty, N. F., and H, Fulford. (2005). "Do Information Security Policies Reduce the Incidence of Security Breaches? An Exploratory Analysis," *Information Resources Management Journal*, 18(4), 21-39.

Drucker, P. (1999). *Management Challenges for the 21st Century*, New York: Harper Business Books.

Finne, T. (2000). "Information Systems Risk Management: Key Concepts and Business Processes," *Computers & Security* (19)3, pp. 234-242.

FTC Complaint. (2006, February 26). "Federal Trade Commission Compliant In the Matter of CardSystems Solutions, Inc., and Solidus Networks, Inc., Doing Business as Pay by Touch Solutions," Federal Trade Commission, File No. 052 3148, http://www.ftc.gov/os/caselist/0523148/0523148complaint.pdf

Fung, P., L. F. Kwok, and D. Longley. (2003). "Electronic Information Security Documentation," *Proceedings of the Australasian Information Security Workshop Conference on ACSW Frontiers 2003* (Adelaide, Australia). (21), pp. 25-31.

Gal-Or, E. and A. Ghose. (2005). "The Economic Incentives for Sharing Security Information," *Information Systems Research*, 16(2), 186-208.

Goodhue, D. L. and D. W. Straub. (1991). "Security Concerns of System Users: A Study of Perceptions of the Adequacy of Security," *Information & Management*, 20(1), 13-28.

Gordon, L. A. (2006). "Economic Aspects of Information Security: An Emerging Field of Research," *Information Systems Frontiers*, 8(5), 335-337.

Gordon L. A., M. Loeb, W. Lucyshyn, and R. Richardson. (2005). "2005 CSI/FBI Computer Crime and Security Survey," Computer Security Institute, 2005.

Gordon, L. A. and M. P. Loeb. (2002). "The Economics of Information Security Investment," *ACM Transactions on Information and System Security*, 5(4), 438-457.

Grimaila, M. R. and L. W. Fortson. (2007). "Towards an Information Asset-Based Defensive Cyber Damage Assessment Process," *Proceeding of the 2007 IEEE Symposium on Computational Intelligence in Security and Defense Applications,* April 1-5, 2007, Honolulu, HI. 206-212.

Gupta, M., J. Rees, A. Chaturvedi, and J. Chi. (2006). "Matching Information Security Vulnerabilities to Organizational Security Profiles: A Genetic Algorithm Approach," *Decision Support Systems*, 41(3), 592-603.

Hamill, J. T., R. F Deckro, and J. M Kloeber. (2005). "Evaluating Information Assurance Strategies," *Decision Support Systems*, 39(3), 463-484.

Harrington, S. J. (1996). "The Effect of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgments and Intentions," *MIS Quarterly*, 20(3), 257-278.

House. (2005). "Credit Card Processing: How Secure Is It?" Hearing before the Subcommittee on Oversight and Investigation of the Committee on Financial Services U.S. House of Representatives, 1-153. http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_house_ hearings&docid=f:29461.wais

March, J, and H. Simon. (1958). *Organizations*. John Wiley & Sons, Inc. New York.

Mercuri, R. T., (2003). "Analyzing Security Costs," *CACM*, (46)6, pp.15-18.

Mimoso, M. S. (2006). "Cleaning up after a Data Attack: CardSystems' Joe Christensen," Information Security Magazine, http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1180411,00.html

Popper, K. (1959). "The Logic of Scientific Discovery," *Basic Books*, New York.

Pipkin, D. L. (2000). *Information Security: Protecting the Global Enterprise*, Prentice Hall; 1ed., Upper Saddle River, NJ, USA.

Straub, D. W. J. and R. W. Collins. (1990). "Key Information Liability Issues Facing Managers: Software Piracy, Proprietary Databases, and Individual Rights to Privacy," *MIS Quarterly*, 14(2), 143-156.

Straub, D. W. J. and W. D. Nance. (1990). "Discovering and Disciplining Computer Abuse in Organizations: A Field Study," *MIS Quarterly*, 14(1), 45-60.

Straub, D. W. J. and R. J. Welke. (1998). "Coping with Systems Risk: Security Planning Models for Management Decision Making," *MIS Quarterly*, 22(4), 441-469.

Sun, L., R. P. Srivastava, and T. J. Mock. (2006). "An Information Security Risk Assessment Model under the Dempster-Shafer Theory of Belief Functions," *Journal of Management Information Systems*, 22(4), 109-142.

Wernerfelt, B. (1984). "A Resource-Based View of the Firm," *Strategic Management Journal,* 5(2), 171-180.

Wing, J. M. (1990). "A Specifier's Introduction to Formal Methods," *Computer* 23(9): 8-24.

Yue, W. T., M. Cakanyildirim, Y. U. Ryu, and D. Liu. (2007). "Network Externalities, Layered Protection, and IT Security Risk Management," *Decision Support Systems*, 44(1), 1-16.

ABOUT THE AUTHORS

Joobin Choobineh's research areas include security and information systems management. He has written more than 50 articles that have appeared in journals such as (in alphabetical order) *Annals of Operations Research, Communications of the ACM, Database Engineering, Decision Support Systems, IEEE Transactions on Software Engineering, Information and Management, Information Strategy, Information Systems, Information Systems Management, INFORMS Journal on Computing, Intl. J. Of Operations & Production Management, J. of Database Management, J. of Management Information Systems, Omega*, and the *Database for Advances in Information Systems*. Since 1986, he has delivered results on research and educational grants in excess of $1,200,000 that were funded by firms such as CISCO Systems, EDS, HP, and Texas Instruments. He has served as the chair of eight Ph.D. students. Dr. Choobineh is currently an associate editor of *INFORMS Journal on Computing* and serves on the editorial board of the *International Journal of Business Information Systems*.

Gurpreet Dhillon is professor of Information Systems and director of Information Technology Leadership Institute at the School of Business, Virginia Commonwealth University, Richmond, USA. He holds a Ph.D. from the London School of Economics and Political Science, UK. His research interests include management of information security, ethical and legal implications of information technology. His research has been published in several journals including *Information Systems Research, Information & Management, Communications of the ACM, Computers & Security, European Journal of Information Systems, Information Systems Journal, and International Journal of Information Management,* among others.

Gurpreet has authored six books including *Principles of Information Systems Security: Text and Cases* (John Wiley, 2007). He is also the editor-in-chief of the *Journal of Information System Security*, is the North American regional editor of the *International Journal of Information Management* and sits on the editorial board of *MISQ Executive*. Gurpreet consults regularly with industry and government and has completed assignments for various organizations in India, Portugal, UK and the U.S.

Michael R. Grimaila's research areas include information warfare; communications and information security; and information resource management. His articles have appeared in journals such as *IEEE Communications; IEEE Computer Security and Privacy; IEEE Transactions on Engineering Management*; the *Information System Security Association (ISSA) Journal*; and the *Terrorism and Political Violence Journal*. He has received funding in excess of $1,300,000 from organizations such as the Air Force Research Laboratory, Cisco Systems, the National Air and Space Intelligence Center, the National Security Agency, and Texas Instruments. Dr. Grimaila currently serves on the editorial board of the Information System Security Association (ISSA) Journal; holds the CISM, CISSP, NSA IAM/IEM, and SANS GSEC certifications; and serves on the Department of Defense Information Assurance, the Information Systems Audit and Control Association (ISACA), and International Systems Security Engineering

Association (ISSEA) Metrics Working Groups. He is a Senior member of the IEEE and is a member of the ACM, AIS, IRMA, $(ISC)^2$, ISACA, ISSA, ISSEA, and SANS Institute.

Jackie Rees is currently an associate professor of Management Information Systems at the Krannert School of Management at Purdue University. Her research interests include information security policy and risk management, particularly risk assessment. Her research articles have appeared in journals such as *INFORMS Journal of Computing, Communications of the ACM, European Journal of Operational Research, Decision Support Systems,* and *Information Technology and Management.* She serves on the editorial board of the *Journal of Database Management.* She is a member of AIS, INFORMS, DSI, and CSI.

Communications of the Association for Information Systems

ISSN: 1529-3181