

Information Systems Security Governance Research: A Behavioral Perspective

Sushma Mishra and Gurpreet Dhillon
Virginia Commonwealth University
1015 Floyd Avenue
Richmond, VA 23284 4000

Abstract- Behavioral information systems security governance entails managing the informal structures in an organization to ensure an appropriate security environment. Informal structures in an organization comprise the individual values, beliefs and behavior prevalent in an organization guiding the norms and employee perception of job responsibilities. Five consistent themes arise from a critical review of the extant literature in this area: security culture, internal control assessment, security policy implementation, individual values, beliefs, and security training. A theoretical framework from the field of sociology is proposed to investigate the current issues in behavioral aspects of security governance. Contributions of this paper are discussed and future research directions suggested.

Keywords- Information systems security, security governance, theory of anomie, behavioral aspects.

1. INTRODUCTION

Information systems security initiatives have been recognized as the top priority by corporate America [42]. Information systems security governance helps in protecting informational assets by creating proper internal controls in the business processes and ensuring responsibility and accountability in organizational structure [8]. Recent incidents of security governance failure such as those at Barings Bank, Enron and Ameriquest, emphasize the need for revisiting the current information systems security governance practices and adopt more stringent means to ensure security. Reports about security governance breaches are frequently encountered in media. Hence, the incidents at Water and Sewer department at San Diego, where an employee accessed privileged information and committed identity theft. In another reported security breach at FedEx, where W-2 forms including workers tax information and SSN were inadvertently exposed affecting 8,500 people [32], shows the severity of such threats today. Incidents of governance failures to prevent security breaches due to employees within the organization are

indicators of the failure of information systems security governance programs, which do not address individual values, beliefs and means to encourage conformity with policies.

Behavioral information systems security governance emphasizes on management of people in an organization. The aim of behavioral aspects of security governance is to ensure that employees show conformity with rules and policies. A system, which punishes deviant behavior (people who do not follow the rules) and takes strong deterrent actions to ensure that procedures are followed comes under the purview of behavioral information security governance. After all, people are the weakest link in information systems security [14]. Insider threats (i.e. threat to information systems from within the organization) are high and the majority of security breaches fall in this category [46], [3], [16], [25], [34]. Organic nature of organizations demands a continuing, dynamic and real time information management system [2], where “people” in organization are the drivers of such ongoing security governance efforts.

A survey of literature shows that research about technical and formal controls for security management of information systems is abundant but security governance at informal level has rarely been emphasized in the security literature. Chen [5] emphasizes that informal organization structures are important for information systems alignment. Various informal “relationship-based structures that transcend the formal division of labor and coordination of tasks” (pp. 107) cannot be separated from formal structures as it comprises an integral part of the socio-technical system of an organization. To attain comprehensive information system security in an organization, organizations need to attend to behavioral issues of security governance such as informal management of security behavior, culture, norms and individual values.

This paper proposes a theory of anomie as a means to facilitate behavioral information systems security governance research. Theory of anomie suggests that deviant behavior in a group setting arises due to cultural and environmental pressure for conformity with organizational (groups or societies) rules and norms. This paper argues that using theory of anomie is an appropriate conceptual framework to study information systems security governance from a behavioral perspective.

The rest of this paper is organized as follows. In section two, a discussion on the guiding definitions of the basic constructs is presented. There are several definitions and perspectives about information systems, information systems security and behavioral information systems security governance in research. Thus explicit definitions of these terms, as endorsed in this paper, are presented. In section three, a critical review of behavioral information systems security governance research is presented. The literature was classified along two dimensions: theoretical foundations and emergent themes. Results of this classification are presented. In section four, a theoretical framework from the field of sociology, anomie theory, is presented. An argument about appropriateness of this framework to inform research in behavioral information systems security governance is presented. The concluding section presents future research areas and contributions of this research.

2. DEFINITIONS

There is ambiguity in research about the definitions of information systems security, behavioral information systems security and information systems security governance. A review of research shows that usually no explicit definitions of such terms are provided and often these terms are used interchangeably, which makes the research confusing to read. Thus, a guiding definition of the above mentioned terms is provided for better clarity of scope and intent of this paper.

2.1 Information systems security

Any attempt to define information systems security first requires clarity about information systems itself. This paper adheres to socio technical view of information system that comprises an interaction of technology and people. As defined by Lee [20], “an information system is not the information technology alone, but the system that emerges from the mutually transformational interactions between the information technology and the organization”

(p. 11). Thus, both technology and people are an inherent part of an information system, which makes it emergent, contextual and dynamic in nature. Consistent with the above definition of information systems is the fact that any attempt to secure or protect such systems from undesired consequences, would require solving the technical as well as people issues. Information systems security protects all information assets from misuse, harm or any other unintended result. This includes securing information in computers, maintaining integrity of business processes, retaining skilled knowledge workers with their implicit knowledge and also encouraging employees to claim ownership of their share of information assets [8]. Information is a shared asset, which has to be protected from all possible distortions by everyone sharing it.

Dhillon [8] proposes a “fried egg” analogy for information systems security. Accordingly, information systems have to be secured at three levels simultaneously for achieving comprehensive security in an organization. These levels are: Formal: At this level messages from all external parties are interpreted and communicated for effective operations of the organization. Example: business strategies, corporate board, financial planning, human resources and marketing planning. Informal: This level acts as means to support the formal systems. Example: subgroups formed within organizations, belief system of employees, implicit knowledge about work procedures and power and politics equation amongst groups. Technical: This level presumes that a formal system exists and automates parts of formal system. Example: information technology automating business process workflow. Information systems security has to be an integrated approach at all the three levels.

2.2 Behavioral information systems security

Behavioral domain of information systems security focuses primarily on ‘people’ aspects of information systems. The level of analysis in the behavioral domain is ‘individual’. Thus, complex problems, such as how to instill proper values regarding security in employees or how to reduce insider threats to security are researched in this domain. Stanton et al. [38] define the behavioral domain as “complexes of human action that influence availability, confidentiality and integrity of information systems” (p. 3). The nature of the research in this area makes it suitable to borrow theories and methods from the fields of psychology and criminology.

The issues researched in behavioral domain of information systems security such as values, attitudes, beliefs, and norms influencing an individual employee, are more pertinent to the informal level of security in an organization. Dealing with individual level phenomenon, behavioral information systems security uses a variety of evaluation approaches and a wide range of problems. The complexity of the problems studied in this domain leads to solutions that are more descriptive than prescriptive in nature. Understanding the intentions and motivations of individual behavior, cannot be easily generalized to form the common denominator of behavior. Hence, the findings at this level need to be effectively implemented through other levels (i.e. formal and technical).

2.3 Information systems security governance

Moulton and Coles [28] define information systems security governance as “the establishment and maintenance of the control environment to manage the risks relating to the confidentiality, integrity and availability of information and its supporting processes and systems”. This definition does not include audit processes, security operational details and development of security artifacts for meeting security objectives. Role of human actors and issues relating to management of people in the organization is not emphasized in popular definitions of information systems security governance. In behavioral aspects of security governance, emphasis should be on managing people who enact the security solutions thus becoming inevitable part of security process itself. By creating responsibility and accountability in structures, management ensures that employees align their personal value system with those of the organization.

Development of proper security policies for risk mitigation is also a part of security governance effort. Communication of these policies is equally important as having useful policies [44] because the commitment and seriousness of management regarding security of assets is conveyed through policies. Ownership of systems and security methods is encouraged. Accountability on part of top management is crucial for effective security governance practices [44] and becomes more compelling in regulatory compliances era. Based on the “fried egg” analogy, figure 1 presents the cyclical nature of information systems security governance at all three levels:

Formal: Institutionalization of security governance practices by management. These efforts include

creation of security policies, procedures, assessment of internal controls, encouraging group behavior, leadership style and strong measures against non-conformity and deviant behavior.

Informal: Reinforcement of security practices by taking into account normative controls, creating security conscious culture, prevalent norms, individual believes and personal values.

Technical: Enactment of the formal governance practices through stringent rules, procedures, operational details, monitoring, and feedbacks.

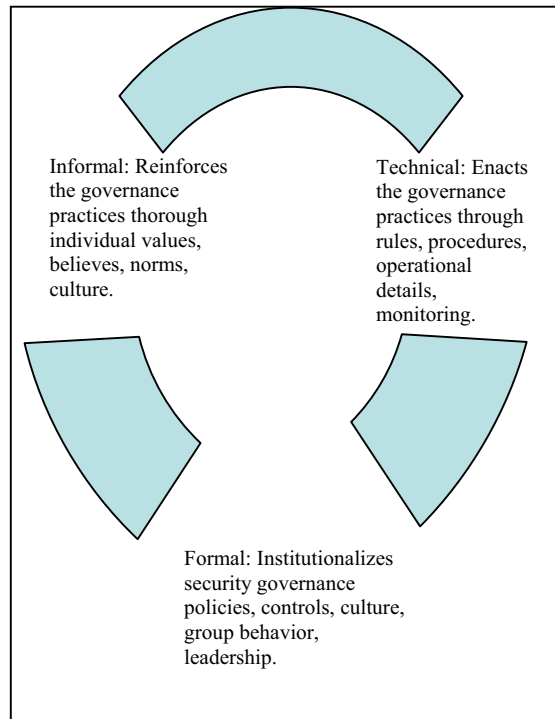


Figure 1-Cyclical Nature of Information Systems Security Governance

3. EXTANT LITERATURE ON INFORMATION SYSTEMS SECURITY GOVERNANCE

Relevant information systems security literature was reviewed from top twenty journals in information systems. In addition, the specialist journal “Computers & Security” was added to the list. According to the definitions provided above of the behavioral information systems security governance, a content analysis was conducted by the two researchers involved in this work. Consistent with our scope of behavioral domain of information systems security governance, a group of forty-one papers were chosen as appropriate for our analysis. The literature on information systems security governance has been reviewed and analyzed on two dimensions. These are: theoretical

foundations and emergent themes. A review of the literature is presented below followed by an analysis on two dimensions mentioned.

Moulton and Cole [28] define information systems security governance as a way of establishing and maintaining a control environment. This environment is required to manage risks that relate to confidentiality, integrity and availability of information and its supporting processes and systems. Such a mechanistic definition does not allow incorporating the importance of the audit process of systems and management of security details at operational level of business processes. Adhering to similar technical view of security governance, Certified Information Systems Auditor (CISA) review manual [18] defines information security governance as a “focused activity with specific value drivers: integrity of information, continuity of services and protection of information assets (pp.385)”. Definitions as provided above acknowledge the importance of global integration of organizations and technical challenges involved in providing security in such environment. Information systems security governance for researchers adhering to above definition of governance means managing the technical aspects of security better for better governance results.

Ward and Smith [44] emphasize the role of proper security policies as crucial for effective information systems security governance. Clear and concise security policy formulation is important for security governance [4]. Communication of these policies to employees enhances the adoption and results in better implementation of such policies [41], [23], [19]. Researchers emphasizing organizational role in comprehensive information systems security governance argue that responsibility and accountability in organizational structures are two important requirements for effective security governance [7]. By creating responsibility and accountability in structures, management ensures that employees have a sense of ownership towards information security measures within the organization. Warkentin and Johnston [45] argue that compliance with security governance procedures can only be achieved by enforcing internal controls. Periodic assessment of internal controls is important for operational efficiency leading to less vulnerabilities and better security management [46], [31], [33], and [13]. Thus, ownership of systems and security methods is encouraged for intended security management results [6].

Researchers emphasizing the importance of human aspects in security management argue that information systems security governance should reflect the objectives, values and beliefs of management regarding the informational assets in the organization. Policies and controls do not have human considerations [36]. Successful implementation of the controls and policies is only possible when individuals are able to align their value system with management. A consensus amongst these researchers is that if there is a misalignment between individual and organizational goals, there are greater security threats to information systems from the insiders in the organization [25], [38], [26], [24] and employees should be treated as owners of information assets [1]. An environment promoting the importance of security behavior in organization should be proactively created [43], [11], [9], [41]. An effective way creating such facilities in the organization is through promoting security training programs [3], [29], [21], [35].

Research in information systems borrows theories from other disciplines such as psychology, criminology, management and sociology. A review of information systems security governance research shows that theories from other disciplines informs research in this domain and helps in better investigate issues and find comprehensive solutions grounded in these theories. Theories such as general deterrence theory, theory of reasoned action, theory of planned behavior, social bond theory, social learning theory, behavioral regulation theory and value theory, have been used by researchers in information systems security research. A brief description of these theories and its uses in information systems security governance research is provided. A critical review of the research in information systems governance domain shows some emergent themes that are being actively researched and emphasized for better security governance results. A description of these themes is presented below.

3.1 Theoretical foundations

Information systems security governance borrows theories from other disciplines and uses them as conceptual foundations to investigate the issues in this domain. *General deterrence theory* is from discipline of criminology used by researchers in information systems security research to understand the deterrent actions and behaviors for better security management [40], [39], and [30]. This theory propagates the value of strong deterrent actions on potential fraud situations. According to

this theory, deterrent actions at an organizational level should be able to impact the individual and group behavior and intention about crime. Theories from psychology have been frequently used to understand the behavior, intentions and perception of hackers as well as employees for security management. *Theory of reasoned action* has been used by researchers [22], [24] to understand the behavioral intentions of people regarding security issues. *Theory of planned behavior* [22] adds another dimension to theory of reasoned action by including perceived behavioral control as a factor. Strong control beliefs about existence of favorable factors leads to high control in actual behavior. The only difference between these two theories is that theory of reasoned action predicts better the behavior of people under volitional control whereas theory of planned behavior predicts behavior of people who do not have complete volitional control. A summary of the theories used in behavioral information systems security governance research is presented below in table 1.

Social bond theory originates in discipline of criminology and has been used in information systems security governance research [40], [15], [21]. According to this theory, strong social bonds and prevents a person from committing crimes. Thus from information systems security governance perspective, it is advisable to have strong normative pressure on individuals in an organization as such a force makes people abide by rules. Social learning theory [40], [17] suggests that influence of peer behavior encourages a person to do certain things under pressure, which they would not do otherwise.

This theory has implications from information systems security perspective as it suggests strong correlation between a person committing a crime and having friends who have committed similar crimes. Behavioral regulation theory adheres to systems perspective of organizations, which is mechanistic. Gonzalez and Sawicka [14] use this theory to create dynamic models of compliance. Based on systems modeling and simulation concepts, this theory explores questions about instrumental conditioning such as what makes something effective as a reinforcer and how does the reinforcer produce such effect? Dhillon and Torkzadeh [9] used value theory to understand the organizational and social objectives of information systems security. Value theory emphasizes the role of individual values in multi criterion decision making situations and is suitable for studying the objectives of information systems security governance.

TABLE 1
THEORIES USED IN BEHAVIORAL INFORMATION
SYSTEMS SECURITY GOVERNANCE RESEARCH

<i>Theories</i>	<i>Authors</i>
General Deterrence Theory	Theoharidou et al. [40]; Straub & Welke [39]; Parker [30].
Theory of Reasoned Action	Whitman [46]; Dhillon [7]; Posthumus and Solms [31]; Rezmierski et al. [33]; Flowerday and Solms [13].
Theory of Planned Behavior	Levine, et al. [22]
Social Bond Theory	Theoharidou et al. [40]; Hirschi [15]; Lee et al. [21].
Social learning Theory	Theoharidou et al [40]; Hollinger [17].
Behavioral Regulation Theory	Gonzalez and Sawicka [14]
Value theory	Dhillon and Torkzadeh [9].

3.2 Emergent Themes

A critical review of the information systems security governance research reveals five emergent themes from the literature. Researchers in information systems security domain have considerably emphasized certain areas of concern and measures to meet the challenges from such issues. A description of the emergent themes is provided below and a summary of the themes is presented in table 2. These themes are:

1. Proactive security culture: information systems security governance research argues in favor of creating proactively a security culture in an organization for better governance purposes [43]. Proactively creating strong security awareness amongst employees and instilling proper values helps in management of security affairs [9]. Creating security consciousness amongst employees creates a unique character of an organization through a set of norms, beliefs and values. This uniqueness is specific to organizations that constitute its culture. Adopting organizational culture grounded in security principles creates an environment conducive for security practices [10], [41].
2. Internal control assessment: creation of internal controls and periodic assessment of these controls

have been identified as an effective measure for providing adequate security governance [45], [46]. Internal controls are the practices, procedures, policies and responsibility structures in an organization that helps in managing risks and protecting informational assets [7]. Internal controls are created by management after assessing risks and prioritizing alternatives to combat such risks [31], [33]. There could be various kinds of controls such as password protection, physical assets protection and segregation of duty. These controls are established through creating right policies and procedures for such objectives. Effective assessment of these controls regularly is critical for security governance success [13].

3. Security policy implementation: security policies in an organization form the infrastructure for secure information systems management. Clear and concise policy creation is crucial for information systems security governance and quality of security policies decide how effective these policies are in serving its purpose [28], [41]. Policies should be based on core job functions rather than creating unnecessary changes in business process [4], [23]. Timely scrutiny of these policies in a periodic fashion with a feedback loop to incorporate revisions creates solid information systems security governance structure [19]. Research in this area argues for robust, adaptive and clear security policies [44]. Communication of policies to employees is as important as creating the policies.

4. Individual values and beliefs: individual beliefs of employees shape the interpretation and hence the success of all security measures in an organization [25], [26]. Importance of normative controls in an organization has been emphasized in literature. Normative controls help in managing employees informally and this channel is quite effective in actually reaching out to people and conveying management's ideas [1], [34]. Assessment of individual values, beliefs and attitude could be used for predicting employee's attitude and behavior [38]. User sophistication, social engineering and end user behavior are well-researched constructs in security literature [24] and the findings emphasize the importance of individual belief system in security management.

EMERGENT THEMES FOR BEHAVIORAL INFORMATION SYSTEMS SECURITY GOVERNANCE RESEARCH

Themes	Authors
<i>Proactive Security Culture</i>	Vroom and Solms [43]; Dhillon and Backhouse [10]; Dhillon and Torkezadeh [9]; Thomson and Solms [41].
<i>Internal Control Assessment</i>	Whitman [46]; Dhillon [7]; Posthumus and Solms [31]; Rezmierski et al. [33]; Flowerday and Solms [13].
<i>Security Policy Implementation</i>	Moulton and Cole [28]; Ward and Smith [44]; Campbell et al. [4]; Thomson and Solms [41]; Lindup [23]; Karydaa and Kokolakisb [19].
<i>Individual Values and Beliefs</i>	Magklaras and Furnell [25]; Stanton et al. [38]; McHugh and Deek [26]; Loch and Conger [24]; Adams and Sasse [1]; Schultz [34]
<i>Security training</i>	Whitman [46]; Bottom [3]; Orgill et al. [29]; Segev and Roldan [35]; Adams and Sasse [1].

5. Security training: training users about importance of security and controls increase the awareness of users and breaches due to ignorance can be prevented [29]. In addition, employee awareness of security issues prevents security attacks proactively [46], [3]. Security training has been consistently mentioned by many researchers as a prerequisite to implement security governance program [35], [1]. Training helps in better utilization of overall security measures used in an organization. Security training helps in better internal control management, implementation and communications of policies, creation of encompassing security awareness in the organization and provides value to security governance efforts in the long term.

An analysis of research in information systems security governance from behavioral perspective leads us to believe that there is more research in technical aspects of information systems security governance than in behavioral aspects. A trend of neglecting behavioral issues in research is detrimental to growth of overall integrated security governance solutions because behavioral aspects of information systems security governance are an integral part of a successful long term information

TABLE 2

systems security governance program. There is more emphasis, on securing the technical challenges for governance purposes, in practice as well. Information systems security governance should have adequate emphasis at informal level of security management and concentrate on people. There is an apparent gap in research and practice regarding research efforts for behavioral information systems security governance. To address this gap, a theoretical framework from the field of sociology, is proposed, as a conceptual foundation to investigate problems in behavioral information systems security governance.

4. THEORY OF ANOMIE AND INFORMATION SYSTEMS SECURITY GOVERNANCE: A LOGICAL FIT

Behavioral information systems security governance focuses on security management of information systems at an individual employee level, in an organization. Thus, behavioral security governance creates means to understand employee behavior, values, norms and informal practices in organization and established solutions of encourage security behavior in an organization. Theory of anomie presents a conceptual basis to understand the deviant behavior of individuals in a group setting and provides taxonomy to understand different kinds of behavioral pattern that individual might adhere to, when pressurized to show conformity. Deviant behavior of individuals and pressure to show conformity with rules are two important issues for behavioral information systems security governance. The argument to use anomie theory as a theoretical framework to inform research in information systems security governance is logically sound and compelling. The next subsection provides an overview of theory of anomie.

4.1 Theory of anomie: an overview

Theory of anomie focuses on pressures toward deviant behavior that arises from discrepancies between cultural goals and approved modes of access to them and also on variations in access to legitimate means. Two broad schools of thoughts are encountered to understand deviant behavior of people, who are exposed to various pressures from environment around them.

Durkheim (in [6]) used anomie theory to explain deviant behavior. He emphasized various social conditions that lead to extra ambitious people turning their unlimited aspirations into breakdown of regulatory norms. Looking at possible sources of

anomie, Durkheim proposed that rapid technological changes could create possible motivations for deviant behavior. Extending this line of thought, Cloward argued that existence of vast unexploited markets for new technologies excites the imagination of people to accumulate wealth.

Merton [27] further extended this work and systematically extended this theory while directing attention to “patterns of disjunction between culturally prescribed goals and socially organized access to them (Cloward [6], pp. 165)”. According to Merton, goals and norms may vary independently of each other and could end up in non-integrated state. It could lead to emphasis on value of goals much more than the means to achieve these goals. It could also lead to following certain means and goals just because they have been followed historically and not because they really solve any problem. This is the condition where conformity becomes a central value. Merton focuses on theory of anomie by identifying mal-integrated societies and focusing upon cultural goals and norms.

Merton enumerates five basic types of behavior that are likely to emerge, when people are under pressure of conformity. These are conformity, innovation, ritualism, retreatism, and rebellion. He further explains how people are going to react to pressure and fit their behavior into one of these categories. This is also a factor of the relative extent of pressure and personal values of these people that governs the use of various illegitimate means. Dubin (1959) further extended this typology by adding ten deviant behavior types that supplement the first four suggested by Merton. He does not consider conformity, one of the behavior types suggested by Merton, in his taxonomy as it does imply deviation.

Cloward [6] suggested that apart from socially patterned pressures that give rise to deviance and personal values, which determine choices of adaptation. He calls it “differentials in availability of illegitimate means”. The argument being that not everyone has easily accessible illegitimate means to turn to whenever a need arises. The choice of getting things done through illegitimate means depends on an individual capability to get access to these illegitimate means. For example, if an employee really wants to steal some confidential information and sell it outside, then occurrence of this event is a factor of employee’s capability to access confidential information. Having an intention

to commit a crime is not enough if there are no means available to execute it accordingly.

4.2 Information systems security governance and deviant behavior

Anomie theory presents an appropriate epistemological base to study behavioral aspects of information systems security governance. Even though residing at an informal level of security management, the importance of individual values, norms and awareness culture, in an organizational setting has been identified and constantly highlighted in the security literature. This theory provides a conceptual lens to understand the various sources of deviant behavior in a group setting.

Using the taxonomy suggested by this theoretical framework, research in information systems security governance could be informed with better models about management of deviant behaviors at individual and group levels. Importance of reinforcement of positive behavior and attitude should be encouraged for sound security governance practices and similarly strong deterrent actions should be taken against individual deviant behavior in a group. Conformity to rules, laws and policies is the backbone of strong information systems security governance structure. This model, validated by a methodology, would help to find better means of understanding the underlying causes of negative attitudes of employees towards conformity and provide solutions to deal with such situations.

5. CONCLUSION AND FUTURE RESEARCH

This paper reviews the current research in information systems security governance from a behavioral perspective. The findings of this paper informs research by identifying the range of emergent issues and listing various theories being used in behavioral domain of security governance research. The paper also highlights the need for better security management techniques for “formally managing the informal” aspects of information systems security. A theoretical framework appropriate for behavioral information systems security governance is suggested. The proposed framework, borrowed from the discipline of sociology, is arguably a conceptual fit to study the values and behavior of individuals in a group setting. A Study of underlying factors of deviant behavior of individuals is potentially useful for better security governance practices.

Contributions to existing security governance literature are theoretical as well as practical. This

paper provides a theoretical framework appropriate for information systems security governance research. This theory, best to our knowledge, has not been used to a great extent in information systems research. Applying a theoretical lens from another discipline to investigate security governance issues is a contribution to information systems research. This framework needs empirical validation in a security governance context. This framework can inform practitioner community about better management of employees by assessment of individual value systems in an organizational setting. Further research in this direction entails assessment of individual values and ethics of potential employees and predicting behavior from these results. Results from such an assessment could be applied to real world as a tool to screen job candidates for high profile security positions.

The findings emphasize the significance of contextual factors such as security culture and individual beliefs for better governance output. A comprehensive and stable security governance infrastructure is created with a long-term commitment to a proactive, security conscious and efficient work force.

REFERENCES

- [1]. Adams, A. and Sasse, M.A. "Users are not the enemy. Association for Computing Machinery," *Communications of the ACM* (42:12) 1999, pp 40-46.
- [2]. Booker, R. "Re-engineering enterprise security," *Computers & Security* (25) 2006, pp 13-17.
- [3]. Bottom, N. "The human face of information loss," *Security Management* (44:6) 2000, pp 50 - 56.
- [4]. Campbell, R., Al-Muhtadi, J., Naldurg, P., Sampemane, G. and Mickunas, M. D "Towards Security and Privacy for Pervasive Computing. In Theories and Systems," in: *Mext-NSF-JSPS International Symposium, ISSS*, Tokyo, Japan, 2002.
- [5]. Chen, Y.E. "Why Haven't We Mastered Alignment? The Importance of Informal Organization Structure," *MIS Quarterly Executive* (1:2) 2002, pp 97-112.
- [6]. Cloward, R. "Illegitimate Means, Anomie, and Deviant Behavior," *American Sociological Review* (24:2) 1959, pp 164 - 176.
- [7]. Dhillon, G. "Violation of Safeguards by Trusted Personnel and Understanding Related Information Security Concerns." *Computers & Security* 20(2): 165-172" *Computers & Security* (20:2) 2001, pp 165 - 172
- [8]. Dhillon, G. *Principles of Information Systems Security: Text and Cases* Wiley, 2007.
- [9]. Dhillon, G. and Torzadeh, R. "Value-focused Assessment of information systems security in organizations," *Forthcoming Information Systems Journal* 2006.
- [10]. Dhillon, G. and Backhouse, J. "Information System Security Management in the New Millennium,"

- Communications of the ACM* (43:7) 2000, pp 125-128.
- [11]. Dhillon, G. and Backhouse, J. "Current directions in IS security research: towards socio-organizational perspectives," *Information Systems Journal* (11) 2001, pp 127 - 153.
- [12]. Dubin, R. "Deviant Behavior and Social Structure: Continuities in Social Theory," *American Sociological Review* (24:2) 1959, pp 147 - 164
- [13]. Flowerday, S. and Solms., R. "Real-time information integrity = system integrity+ data integrity +continuous assurances," *Computers & Security* (24) 2005, pp 604 - 613
- [14]. Gonzalez, J. and Sawicka, A. "A Framework for Human Factors in Information Security," WSEAS International Conference on Information Security, Rio de Janeiro, Brazil, 2002.
- [15]. Hirschi, T. *Causes of Delinquency* University of California Press, Berkeley, CA, 1969.
- [16]. Hitchings, J. "Deficiencies of the Traditional Approach to Information Security and the Requirements for a New Methodology," *Computers & Security* (14) 1995, pp 377-383.
- [17]. Hollinger, R. "Crime by computer: correlates of software piracy and unauthorized account access," *Security Journal* (4:1) 1993, pp 2-12.
- [18]. Information Systems Audit and Control Association (ISACA) *CISA Review Manual, 2004 Edition*. Rolling Meadows, IL: ISACA, 2004
- [19]. Karydaa, M., Kiountouzisa, E., Kokolakisb, S "Information systems security policies: a contextual perspective," *Computers & Security* (24) 2005, pp 246-260.
- [20]. Lee, A.S. *Thinking about Social theory and Philosophy for Information Systems* John Wiley & Sons, Ltd, Chichester, England, 2004, pp. 1-26.
- [21]. Lee, S.M., Lee, S. and Yoo, S. "An Integrative Model Of Computer Abuse Based On Social Control And General Deterrence Theories," *Information and Management* (41:6), July 2004, pp 707-718.
- [22]. Levine J., and Pauls, C. "Theory of Reasoned Action/Theory of Planned behavior", 1998 Retrieved on 06/06/06
- [23]. Lindup, K. "The Role of Information Security in Corporate Governance," *Computers & Security* (15) 1996, pp 477-485.
- [24]. Loch, K. and Conger, S. "Evaluating Ethical Decision Making and Computer Use," *Communications of the ACM* (39:7), July 1996, pp 74-83.
- [25]. Magklaras, G. and Furnell, S. "A preliminary model of end user sophistication for insider threat prediction in IT systems," *Computers & Security* (24) 2005, pp 371-380.
- [26]. McHugh, J.A.M. and Deek, F. D. "An incentive system for reducing Malware Attacks," *Communications of the ACM* (48:6), June 2005, pp 94-99.
- [27]. Merton, R. "Social Conformity, Deviation and Opportunity Structures: A Comment on the Contributions of Dubin and Cloward," *American Sociological Review*, (42:2) 1959, pp 177-189.
- [28]. Moulton, R. and Coles, R. S. "Applying Information Security Governance," *Computers & Security* (22:7) 2003, pp 580-584.
- [29]. Orgill, G.L., Romney, G.W., Bailey, M. and Orgill, P. "The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems," Conference On Information Technology Education ACM Press Salt Lake City, UT, USA 2004, pp. 177 - 181
- [30]. Parker, D.B. *Fighting Computer Crime: A New Framework For Protecting Information* John Wiley and Sons, New York, NY, 1998.
- [31]. Posthumus, A. and Solms, R.V. "A framework for the governance of information security," *Computers & Security* (23) 2004, pp 638-646.
- [32]. Privacy Rights Clearinghouse. "A Chronology of DataBreaches Reported Since the ChoicePoint Incident", 2006 Retrieved on 04/26/06.
- [33]. Rezmierski, V.E., Seese, M.R and St. Clair II, N. "University systems security logging: who is doing it and how far can they go?" *Computers & Security*, 21(6), pp 557-564, 2002
- [34]. Schultz, E. "A framework for understanding and predicting insider attacks," in: *Compsec* London, 2002.
- [35]. Segev, A.P., J. and Roldan, M " Internet security and the case of Bank of America. Association for Computing Machinery," *Communications of the ACM*. (41:10) 1998, pp 81-87.
- [36]. Solms, B. "Corporate Governance and Information Security," *Computers & Security* (20:3) 2001, pp 215-218.
- [37]. Solms, B.V and Solms, R.V. " From Information Security to...Business Security?" *Computers & Security* (24) 2005, pp 271-273.
- [38]. Stanton, J, K. Stam, "Analysis of end user security behaviors," *Computers & Security* (24:2), 2005, pp 124-133.
- [39]. Straub, D. and Welke, R. ". Coping with systems risk: security planning models for management decision making.," *MIS Quarterly* (22:8) 1998, pp 441-465.
- [40]. Theoharidou, M. and Kokolakis, R. "The insider threat to information systems and the effectiveness of ISO17799," *Computers & Security* (24) 2005, pp 472-484.
- [41]. Thomson, K. and Solms, R "Information security obedience: a definition," *Computers & Security*. (24): 1, 2005, pp. 69-75.
- [42]. Violino, B. "Expect Threats to get nastier as networks become more complex," in: *Computerworld*, 2006.
- [43]. Vroom, C. and Solms, R.V. "Towards information security behavioral compliance.," *Computers & Security* (23:3), 2004, pp. 191-198.
- [44]. Ward, P. and Smith, C. "The Development of Access Control Policies for Information Technology Systems," *Computers & Security* (21:4) 2002, pp 356-371.
- [45]. Warkentin, M. and Johnston, A. (ed.) *IT Security Governance and Centralized Security Controls* Idea Group Publishing, Hershey, P.A., 2006.
- [46]. Whitman, M. "Enemy at the Gate: Threats to Information Security," *Communications of the ACM* (46:8) 2003, pp 91-95.