Human Behavioral Aspects in Information Systems Security

Literature Review

Sushma Mishra
School of Business
Virginia Commonwealth University
Richmond, VA 23284-4000, USA
mishras@vcu.edu

Mark A. Harris
School of Business
Virginia Commonwealth University
Richmond, VA 23284-4000, USA
harrisma3@vcu.edu

Abstract:

Recent literature has identified three areas that must be considered when creating a secure information system: technical, formal and informal systems. With much of the literature focusing on the technical and formal systems, this paper explores the literature aimed at the informal system. The goal of this paper is to explore theories and empirical studies about human behavior and information systems security (ISS) to discover common denominators and best practices for organizations in regards to the softer side of security. The most commonly used theories in the behavioral aspects of ISS are theory of reasoned action, deterrence theory, social bond theory, social learning theory, and theory of planned behavior. The emerging themes that need more attention from organizations in regards to the human element and ISS are organization culture, training/awareness, and internal controls.

Introduction:

The term "Information Systems" (IS) has different connotations to different researchers in IS research. At times, it is used interchangeably as Information technology (IT), while on many occasions it is referred to synonymously as computer usage. Having various definitions of information systems, in our opinion, leads to much confusion in IS research. We will attempt to define IS in our next section. It is also apparent that there are various meanings of "security" of information systems. A review of information systems security (ISS) research presents us with a plethora of perspectives in security related problems, solutions and goals. Most commonly, it has been argued that the goal of ISS is to ensure confidentiality, integrity and availability of data and system. Arguably, research pertaining to this view of ISS is concentrated on technical solutions to security problems, presenting solutions in the form of tools that ensure high quality of data integrity, better access control mechanisms, sophisticated firewalls, and other solutions to similar effect. The technical solutions to security problems are becoming increasingly sophisticated and easier to use, pointing towards the fact that research in this domain has accomplished a lot. But increasing incidents of security breaches (both from inside as well as outside of the organization), computer abuse, data theft, intrusions in user's privacy, and malicious attempts to hack commercial systems leads us to believe that even though being technically advanced, these solutions at best are inadequate in providing overall comprehensive security to information systems.

We have categorized ISS research into broad clusters, based on the types of research we have found in the current literature: behavioral, social, and economical perspective. These are convenient labels using criteria like unit of analysis, objective of research, and the part of information system that its solution emphasizes. Needless to say, the clusters defined above are not by any means a binding compartmentalization. There will always be an overlap between the components in each division. A goal of this paper is primarily directed towards understanding the research efforts in the behavioral domain of information systems security. We have drawn conclusions based on 30+ journal and conference papers that studied the behavioral aspects of information systems security. Our review helped us identify some of the frequently researched problems in this area, theories being used, solutions being suggested, current challenges, and future research in the behavioral domain.

Human behavior can wreck havoc on the security of an information system through intentional or unintentional abuse. The person can work within the organization or be from the outside. Many of the technical controls implemented by organizations fend off attacks from the outside, such as stopping a hacker or a denial of service attack. Other technical controls and formal polices work to stop internal threats, such as an employee guessing passwords or viewing unauthorized data. But if an organization has technical and formal controls, such as firewalls and security policies, can human behavior still lead to insecure information systems? The goal of this paper is to explore theories and empirical studies about human behavior and information systems security (ISS) to discover common denominators and best practices for organizations in regards to the softer side of security.

The rest of this paper is organized as follows. In the next section, the guiding definitions of the basic constructs are defined. The next sections identify some of the broader topics found in the literature: organizational culture, internal controls, prediction/classification, and training/awareness. In the concluding section, gaps in research are identified and future research directions are suggested.

Definitions:

Before going any further with this paper, we would like to define and scope our basic constructs: information systems, information systems security, and the behavioral domain of information systems security.

We adhere to the socio-technical view of an organization, where both social and technical elements interplay to give life to an organizational form. The technical aspects in organizations are manifested through technical solutions required to perform tasks. The social side of it requires control structure for coordination and formalization of business processes. Both of the above aspects of an organization require human intervention to achieve above-mentioned functions. The meanings of technical solutions implemented in an organization are socially constructed and these technical artifacts bring in a change into the dynamics of an organization. As described by Lee (2004), "an information system in 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 an information system includes the technology, people implementing the technology, interaction of people and technology and the emergent organizational context of this interaction.

Information systems security thus means protecting the information systems from undesired consequences. Security efforts pertaining to the above definition of information systems would need measures aimed at technical components, people components, and organizational components. Dhillon (2007) proposes a "fried-egg" analogy, where the security of an IS should be effective at three levels: *technical* (helps in automating and standardizing parts of formal systems such as computers helping in operational tasks), *formal* (helps in organizational level security mechanisms like governance, policies or standardizing processes, such as establishing controls in structure of organization) and *informal* (helps in individual level security mechanisms, like shaping the norms, beliefs, values, and attitudes of employees, such as establishing normative controls). A comprehensive ISS effort entails that security measures in an organization should be administered at all the three levels simultaneously. Thus, managing ISS in organizations requires the implementation of various controls at all the levels and the security measures at each level should complement and reinforce the security objective.

Stanton et. al. (2005) defines the behavioral domain of ISS as "complexes of human action that influence availability, confidentiality and integrity of information systems" (p. 3). The challenge in this domain lies in the fact that people are the ones who create these complex solutions for security and they are the ones who break them. People are the weakest link in information systems security (Gonzalez and Sawicka, 2002). Insider threats (i.e. threat to information systems from within the organization) are high and the majority of security breaches fall in this category (Whitman, 2003; Bottom, 2000; Hitchings, 1995; Magklaras and Furnell, 2005; Schultz, 2002). This domain corresponds to the informal level of security in an organization. The unit of analysis for this domain is individual (i.e. research in this area is concerned about behavioral issues like values, attitude, beliefs, and norms that are dominant, and influencing an individual employee regarding security practices in an organization). Any area that deals with individual level phenomenon ends up with a variety of evaluation approaches due to the complexity and wide range of problems. Similarly, in this domain we find various theories being used and different kinds of evaluation techniques being applied. Considering the complexity of research problems in this domain, it is not surprising that solutions suggested for this domain are more descriptive than prescriptive in nature. Since the findings at this level need to be effectively implemented through other levels (i.e. formal and technical), this domain merely acts as a "means to an end" part of the whole security puzzle. Intervention from other levels in the form of formal controls, security policies, or technological artifacts is required towards achieving desired outcome in this domain.

The general research trend in systems security is that there is more concentration and discussion regarding one level at the cost of neglecting security research at other level. The need of the hour is an integrated approach in security research such that all the three levels are secured simultaneously. There is more emphasis on securing the technical level in the above model and less effort on other two levels. It is in the informal system that we find strong effects on human behavior on information systems security.

Theories used in ISS Research:

General Deterrence Theory – "suggests that when the possibility of punishment is high and the sanction is severe, potential criminals will be deterred from committing illegal acts, especially when their motives are weak" (Theoharidou et al., 2005). Several papers are grounded in this theory. Straub and Welke created a four stage model, including *deterrence*, *prevention*, *detection*, and *remedies* (Straub & Welke, 1998). Parker (1998) created a variation of this model and added a few more categories. His framework included: avoidance, deterrence, prevention, detection, mitigation, sanction, transference, investigation, recovery, and correction.

Theory of Reasoned Action – according to the theory, the most important determinant of a person's behavior is behavior intent. The individual's intention to perform a behavior is a combination of attitude toward performing the behavior and subjective norm. The individual's attitude toward the behavior includes; behavioral belief, evaluations of behavioral outcome, subjective norm, normative beliefs, and the motivation to comply. TRA works most successfully when applied to behaviors that are under a person's volitional control. If behaviors are not fully under volitional control, even though a person may be highly motivated by her own attitudes and subjective norm, she may not actually perform the behavior due to intervening environmental conditions (Levine, et al. 1998).

Theory of Planned Behavior – developed to predict behaviors in which individuals have incomplete volitional control. The major difference between TRA and TPB is the addition of a third determinant of behavioral intention, perceived behavioral control. Perceived Behavioral control is determined by two factors; Control Beliefs and Perceived Power. Perceived behavioral control indicates that a person's motivation is influenced by how difficult the behaviors are perceived to be, as well as the perception of how successfully the individual can, or can not, perform the activity. If a person holds strong control beliefs about the existence of factors that will facilitate a behavior, then the individual will have high perceived control over a behavior. Conversely, the person will have a low perception of control if she holds strong control beliefs that impede the behavior conditions (Levine, et al. 1998).

Social Bond Theory – a criminology theory that suggests that "despite a person's natural inclination towards crime, strong social bonds deter him/her from committing criminal acts" (Theoharidou et al., 2005). Hirschi (1969) proposes four types of social bonds: attachment, commitment, involvement, and beliefs. Lee et al. (2003) conducted a study that concluded that social bonds played an important role in deterring computer crime.

Social Learning Theory – "a person commits a crime because (s)he has been associated with delinquent peers, who transmit delinquent ideas, reinforce delinquency, and function as delinquent role models" (Theoharidou et al, 2005). Hollinger (1993, as cited by Theoharidou et al.) "points out the existence of a strong positive correlation between and individual engaging in computer abuse and the involvement of his/her friends in similar acts").

Organizational Culture:

Edgar Schein defines organizational culture as (Schein, 1999 as mentioned in Vroom and Solms, 2004):

> *"the pattern of basic assumptions that a given group has invented, discovered, or developed in learning to cope with its problems of external adaptation and internal integration, and that have worked well enough to be considered valid, and, therefore to be taught to new members as the correct way to perceive, think, and feel in relation to those problems."*

It is a set of beliefs, attitudes, values, personalities, customs, and norms that represents the unique character of an organization. It is a result of beliefs of management and employees and can be both positive and negative.

Research in behavioral aspects of information systems security suggests organization culture as an important aspect of creating good security practices in an organization and instilling security principles in minds of employees. Vroom and Solms (2004) suggest using the organizational behavior model developed by Szilagyi and Wallace (1990). The model's three levels of organizational behavior are the individual, group, and formal organization (Vroom & Solms, 2004). They suggest all three levels need to be examined to determine how the overall culture of the organization is affected. Weaknesses in security behavior can then be changed at each level and since each level affects the other levels, the overall security culture of the organization begins to change. Vroom and Solms believe that changing the organizational culture to a more security aware culture can increase corporate security beyond the reach of traditional policies and auditing.

Dhillon and Backhouse (2000) suggest "facing pressures of organizational cost containment and external competition, many companies are rushing headlong into adopting IT without carefully planning and understanding the security concerns." This lack of planning can create significant security concerns. Therefore, they suggest incorporating RITE in addition to CIA (confidentiality, integrity, and availability of data) into the organizational culture. RITE stands for *responsibility* and knowledge of roles, *integrity* as a requirement of membership, *trust* (distinct from control), and *ethicality* as opposed to rules. Responsibility refers to everyone knowing exactly what their role is in regards to security. Integrity refers to the integrity of the person that has access to information. Corporations should limit access to information to need to know people and work to maintain integrity. Trust refers to trusting people. Dhillon and Backhouse refer to trust as having a half-life that deteriorates over time and needs to be renewed with face-to-face meetings (p. 127). Ethicality refers to the "ethical content of informal norms and behavior" (p. 128). This ethical content is from the informal side and not the formal rules and procedures. The informal side is unwritten, but yet still is very important to organizational culture and the security culture.

In another paper, Dhillon and Torkzadeh assess values at the group and organizational level. "When individual values are shared within a group, there are implications for commonality in values that a group or organization might share" (Dhillon & Torkzadeh, 2005, p. 6). The authors collected data via interviews and propose 86 objects essential in managing IS security. These objects are broken down into 25 clusters of 9 fundamental and 16 means categories. Because these objects are social-organizational in nature, they can lead to the creation of new IS security measures. Adopting organizationally grounded (culture) principles is a necessary step beyond technical considerations (p. 2).

Internal Controls:

Whitman (2003, p. 95) suggests that organizations use internal controls of various types to combat security threats. First, an organization must identify their threats, which can vary among organizations. Prioritizing the threats and placing them in a control matrix will help security managers plan specific controls for each threat. The matrix should first be undated with whatever current controls are in place. This will help managers see where additional controls are need. At a minimum, each threat "should contain one policy related control, one education and training related control, and one technology related control (p. 95). A policy related control is a control that is a part of the organizations formal rules, such as passwords need to be 8 characters long. An education or training related control is a preventative measure by educating users on the treats to security in hopes to avoid problems before they occur. An example of a technology control would be a router/firewall that directs or blocks network traffic as managers see fit.

Dhillon (2001) suggests "a majority of computer security breaches occur because internal employees of an organization subvert existing controls" (Dhillon, 2001, p. 165). In his paper, he writes about the control problems that led to the fall of Barings Bank in 1995. The cause was the wrongdoing on one individual and security failures of the organization (p. 166). Nicholas Leeson, a general manager for the bank, fraudulently lost millions of dollars worth of Nikkei futures and was able to conceal these losses by doctoring the books.

Dhillon blames Barings for not managing, prioritizing, and maintaining proper internal controls that may have prevented Leeson's fraud. Segregation of duties was a major control that was missing and allowed Leeson to cover up his transactions. He was in charge of overseeing trading, trade processing, settlement, and administration. One person had too much control. There should have been controls in place at Barings to prevent any one person from having this kind of control. "Some companies even separate controls even further in such a way that it would require two or even three individuals to commit this crime and conceal it on the books" (p. 167). Another control problem was a lack of an effective internal audit department. An audit department's responsibility is to monitor high-risk areas and discover abuse. They did not.

Dhillon suggests five components of an ideal internal control system. The first is to create a control environment that

> "consists of actions, policies, and procedures that reflect the overall attitudes of top management about control and its importance to the corporation….. Second, management should assess the risk in the design of its internal controls to minimize errors and fraud….. Third, control activities include other policies and procedures that help to ensure that necessary actions are take to address risks in the achievement of the company's objectives….. Fourth, information technology is used to gather company transactions and to maintain accountability to clearly communicate what is happening in the organization…. Fifth, monitoring the quality of controls periodically is essential to have effective controls" (Dhillon, 2001, p. 168).

Prediction/Classification:

Schultz (2002) suggests that behaviors and symptoms (indicators) of users can be used to predict insider threats. His indicators are deliberate markers, meaningful errors, preparatory behaviors, correlated usage patterns, verbal behavior, and personality traits. Schultz suggests clues from these indicators can be used with quantitative methods and multiple regression formulas to predict insider abuse. *Deliberate markers* are left by attackers to make a statement. Often, small markers precede a big attack. *Meaningful errors* are errors a perpetrator may make while preparing for an attack. *Preparatory behavior* is when a perpetrator attempts to gain information about the system they plan to attack. Running commands on the system to get system information may be an indicator of a future attack. *Correlated usage patterns* are patterns that occur on multiple systems. The behavior may not set off any alarms on one particular system, but may seem odd if done to multiple systems. *Verbal behavior*, written or spoken, that expresses hatred or hostility toward the company or individuals may be an indicator. The most common place to find this kind of behavior is in e-mail. *Personality traits*, particularly introversion, can also be used to predict insider attacks (Schultz, 2002, p. 530).

Magklaras and Furnell (2005) suggest that a user's sophistication can be used as a predictor of internal threats. They divide users into three categories: advanced, ordinary, and novice. Advanced users "clearly exhibit a high level of sophistication, which indicates mastery" (Magklaras and Furnell, 2005, p. 5). Ordinary users have intermediated knowledge and novice users know very little. They then propose to place users into these categories by tracking end-user computer usage. This is done by monitoring what programs the user's access, how long they access the programs, how many different programs they have open at once, what tools or features are accessed within these programs, CPU usage, and RAM usage. Ratings are given by experts to the various programs and percentages of CPU and RAM utilization to be used as scales that will classify users as advanced, ordinary, or novice. The authors tested their model with a small sample of 60 UNIX users and concluded their model was valid.

A six category taxonomy end user behavior and information system security is proposed by Stanton et at. (2005) along two dimensions: intentionality and technical expertise. A user's intentions are rated as malicious, neutral, or beneficial. Their expertise is either high or low (Stanton et al, 2005, p. 126). This taxonomy was validated via a survey of 1167 end users, where their behaviors fit well with the two dimensional model.

Training/awareness:

This is a consistent theme arising in most of the papers that we have studied (Whitman, 2003; Bottom, 2000; Orgill et. al., 2004). There is a heavy emphasis on user training and awareness of security issues. Stanton et. al. (2005) identifies a positive relationship between training and awareness to information security success. Bottom (2002) finds that training employees and executives could prevent a social engineering threat to security. The findings suggest training in WAECUP (waste, accidents, error, crime and unethical practices) could also educate employees regarding potential threats and its impact. Leonard (2004) emphasizes the need for training to condition the ethical behavior intentions that would lead to more secure organization.

Conclusion and Future Research Directions:

ISS behavioral domain faces challenges and any furthering of knowledge in this domain needs to address these problems. Some further steps in this direction that could add to the body of knowledge in the domain are identified. These are suggestions not only for researchers in this area, but act as a tool for practioners. Research in these areas could establish the importance of these prescriptions and validate them empirically.

- **Fill the gap:** There is clearly a gap in literature and practices in real organizations in terms of not giving adequate attention to the softer side of information systems security. Informal aspects of systems security are hard to conceptualize and implement, but very important nonetheless. Implementing stronger normative controls in organizations could be a step towards the management of human aspects of security.

- **Promote security culture:** Evidences in literature clearly suggest that healthy security culture in an organization promotes better management of the informal aspects of security. An awareness of security practices has to be drilled into the minds of employees through training and education programs. There should be an incentive structure in organizations that rewards people with higher security awareness and practices.

- **Create better risk perception:** Through organizational culture and training programs, employees will be better able to assess the risks involved in allowing or creating security breaches. The management has to communicate clearly the severity of these threats to the organization. These practices could considerably reduce intentional and unintentional attacks on the system.

- **Ensure better security compliance:** Effective communication of management goals and objectives of a security program, with deterrent activities and a clear reward structure would ensure that there is a better compliance of formal controls. However good formal or technical controls are, unless the message of creating these controls is clearly communicated and adversities associated with failure to meet these objectives explained, it is highly probable that the seriousness of these attempts will not be clearly absorbed by employees.

- **Accommodate employee's values and beliefs in policy formulation:** Any policy or directive that does not align with the personal value system and beliefs of employees is likely to fail. If there is a 'disconnect' between personal and organizational goals regarding security, there are more chances of security threats. Thus policy formulation, governance restructuring and change management initiatives should accommodate the values and principle of employees. This empowers the employees and helps them adhere to these rules better, as a sense of participation is developed

- **Better Information security governance practices:** Information security governance as a management focus is gaining widespread acceptance. The governance structure and practices has to play an important role in managing the informal aspects of security. A sense of accountability and responsibility in the structure can make the employees more answerable for their behavior. Trust and ethicality as a virtue of security governance needs to be emphasized.

- **Assess individual traits and motivations for employee recruitment:** More research is required in the area of employee recruitment, especially regarding security. Efforts in the form of screening employee's motivations and ethical stand in the recruitment process could help in creating a secure workforce. We feel conceptually it makes more sense to screen employees while admitting them into organizations to ensure better security behavior, rather than training them in ethical and related issues after recruitment. Even though there are no clear evidences that this could lead to better security behaviors, conceptually they are found to highly correlated.

By doing all the above suggestions, we believe that the informal aspect of systems security will gradually become a formalized method of mitigating information systems security. Integrative attempts are required, where findings of research in this area (informal level) can be channeled as inputs for research in the other two levels (formal and technical).

References:

Bottom, N. (2000). "The human face of information loss." Security Management 44(6): 50-56.

Dhillon, G. (2007). Principles of Information Systems Security: Text and Cases. John Wiley & Sons.

Dhillon, G. (2001). "Violation of Safeguards by Trusted Personnel and Understanding Related Information Security Concerns." Computers & Security 20(2): 165-172.

Dhillon, G. and J. Backhouse (2000). "Information System Security Management in the New Millennium." Communications of the ACM 43(7).

Dhillon, G. and J. Backhouse (2001). "Current directions in IS security research: towards socio-organizational perspectives." Information Systems 11: 127-153.

Dhillon, G. and G. Torkzadeh (2005). "Value-focused Assessment of information systems security in organizations." (unpublished) Information Systems Journal.

Gonzalez, J. and A. Sawicka (2002). A Framework for Human Factors in Information Security. WSEAS International Conference on Information Security, Rio de Janeiro.

Hirschi, T. (1969). “Causes of Delinquency” Berkeley, CA: Univerisity of California Press.

Hitchings, J. (1995). "Deficiencies of the Traditional Approach to Information Security and the Requirements for a New Methodology." Computers & Security 14: 377-383.

Hollinger, R. (1993). “Crime by computer: correlates of software piracy and unauthorized account access.” Security Journal 4(1): 2-12.

Lee, A.S. (2004). Thinking about Social theory and Philosophy for Information Systems. In Social Theory and Philosophy for Information Systems. Chichester UK: John Wiley & Sons, p. 1-26

Lee, et al. (2003). “An Integrative Model Of Computer Abuse Based On Social Control And General Deterrence Theories.” Information and Management 41(6): 707-718.

Levine, et al. (1998). *Theory Of Reasoned Action/Theory Of Planned Behavior*. Retrieved December 6, 2005 from http://hsc.usf.edu/~kmbrown/TRA_TPB.htm

Leonard, L., T. Cronan, et al. (2004). "What influences IT ethical behavior – planned behavior, reasoned action, perceived importance, or individual characteristics?" Information & Management 42: 143-158.

Magklaras, G. and S. Furnell (2005). "A preliminary model of end user sophistication for insider threat prediction in IT systems." Computers & Security 24: 371-380.

Orgill, G., G. Romney, et al. (2004). The Urgency for Effective User Privacy-education to Counter Social Engineering Attacks on Secure Computer Systems. SIGITE.

Parker, D. (1998) “Fighting Computer Crime: A New Framework For Protecting Information” New York, NY: John Wiley and Sons.

Schultz, E. (2002). A framework for understanding and predicting insider attacks. Compsec, London.

Stanton, J., K. Stam, et al. (2005). "Analysis of end user security behaviors." Computers & Security 24: 124-133.

Stanton, J., I. Yamodo-Fagnot, et al. (2005). The Madness of Crowds: Employees Beliefs about Information Security in Relation to Security Outcomes. 4th Security Conference, Las Vegas, Nevada.

Straub, D. (1998). “Coping with systems risk: security planning models for management decision making.” MIS Quarterly 22(8): 441-465.

Szilagyi, A. and Wallace, M. (1990). “Organizational behavior and performance.” 5th ed. Illinois: Scott, Foresman and Company.

Theoharidou, M., S. Kokolakis, et al. (2005). "The insider threat to information systems and the effectiveness of ISO17799." Computers & Security 24: 472-484.

Vroom, C. and R. Von Solms (2004). "Towards information security behavioral compliance " Computers & Security 23: 191-198.

Whitman, M. (2003). "Enemy at the Gate: Threats to Information Security." Communications of the ACM 46(8): 91-95.