Utilizing a Learning Loop Framework in IS Security

Angela Mattia, Ph.D.
Assistant Professor
Department of Decision Sciences and Information Management
Davis College of Business, Jacksonville University
Jacksonville FL 32211, USA

Abstract

Information systems (IS) security is a much broader perspective than computer security and as such, it must include manual systems and "human processors." Yet this broader organizational view seems to be often ignored. Information Systems Security must take into account the vulnerability of organizations' proprietary information when placed in the hands of its members. Understanding and perception can affect behavior with respect to protecting the organizations' proprietary information. This paper proposes applying a learning loop framework as a management technique for information systems (IS) security. The framework is based on double loop learning theory and the theories of action which offer insight into managing inconsistent behavior. An exploratory case study illustrates how learning loops can help organizations learn, adapt and manage the process of securing organizational assets.

Keywords: IS Security, IS Security, interpretive perspective, IS security design, socio-organizational perspective, double loop learning, learning loops

1. Introduction

In today's world, public awareness of computer security is at an all-time high because of terrorism, hacking and just the general attention given to computer abuse and mishandling of secured data. It continues to be important, therefore, that we remember that Information systems security is a much broader perspective than computer security and as such, it must include manual systems and "human processors." It is this need for a complete organizational security map that opens up the behavioral aspects of information security(Richard Baskerville, 1992), such as motivation, cognition and organizational learning. Yet this broader organizational view seems to be often ignored.

> "Every year that we study threat actions leading to data breaches, the story is the same; most victims aren't overpowered by unknowable and unstoppable attacks. For the most part, we know them well enough and we also know how to stop them." (Baker et al., 2011)

This begs the question, why? An organization's espoused theory (management controls) and their "theory-in-use" (what they actually do) is often contradictory, leading to security problems that cause considerable financial loss. In the past, IS security relied on conventional IS security methods such as checklists and risk analysis. As a result, many organizations that engaged in identifying security issues have created relevant security policies and mechanisms (i.e., checklists, risk analysis, etc.), but as the investment in security has went up, so has the number of security breaches (Gurpreet Dhillon, 2007). "In 2010, the Secret Service arrested more than 1,200 suspects for cybercrime violations. These investigations involved over $500 million in actual fraud loss." (Baker, et al., 2011).

More recently, the information system research communities have extend their considerations to a broader range of technical and organizational IS security issues in an effort to reduce the number of security breaches. Consequentially, several more advanced but less well-known approaches to develop secure information systems are now available. This paper discusses just a few approaches in the IS literature(Backhouse & Dhillon, 1996; G. Dhillon, 1997; G. Dhillon & Backhouse, 2001; Pahnila, Siponen, & Mahmood, 2007; M. T. Siponen, 2000) that address the issue of IS security with respect to an organizational members' behavior. Discussing these studies allow us to observe the differences, possible strengths and weaknesses of the different approaches. In addition, since the traditional information system development methods do not trouble themselves with security concerns (R. Baskerville, 1993), this paper would be equally important for all organizations as for the security community
This paper proposes using learning loops to address information systems (IS) security. The approach is based on double loop learning theory(Chris Argyris, 1993; Chris Argyris & Schon, 1978; Mattia & Dhillon, 2003), which pertains to learning about the governing variables of an organization and then using what is learned to solve problems that are complex and which change as problem-solving advances.

Double loop theory is based upon a "theory of action" perspective. An important aspect of the theory is the distinction between an individual's espoused theory (organizational goals and mission, formal documents, such as policy statements) and their "theory-in-use" (what they actually do); bringing these two into congruence is a primary concern of double loop learning. Double loop learning (Mattia & Dhillon, 2003) is especially relevant to decision-making skills that are necessary for security related management controls since it focuses on analysis of the assumptions and implicit rules underlying the organization. This paper is organized as follows. First, we discuss how the IS literature addresses the issue of IS security with respect to organizational members' behavior. Second, we present double loop learning and the process of loop learning as a way which researchers and practitioners can help evaluate the potential threats to an organization, due to incongruent perceived and actual behavior. Third, a discussion on how to engage the learning loop process when a mismatch occurs, thus strategically impacting IS security. Lastly, an exploratory case study example illustrates how learning loops can help organizations learn, adapt and manage the process of securing organizational assets.

2. Information System Security Literature

James (1996) has developed an approach for planning and management of IS security based on Checkland's Soft System Methodology (SSM). The aim of the SSM approach to IS security is to concentrate on the human behavior, which is often overlooked. The author especially emphasizes the role of user participation, which is encouraged to increase security awareness and user commitment in security development. User participation should give users the feeling that they are "owners" of the security solutions. Active participation is advocated by (Fishbein & Ajzen, 1975) in the behavioral literature, as a good way of producing change in human beliefs. In addition, Siponen (2000) has suggested, active participation may lead to intrinsic motivation (Deci, 1980). Sometimes user participation may be intentionally neglected, because it is seen as a threat by security personal. James (1996) criticizes the traditional approach as being too technical, and promotes the role of user participation as vital in IS security.

The use of responsibility as a basis for secure IS development has been recognized by the IS communities (Dobson,1990; Backhouse and Dhillon, 1996; Dhillon, 1997). The concept of responsibility suggests that the security requirements can be found by exploring the role of responsibilities. Analyzing responsibilities help to gain an understanding of the organizational context in which they arise (Strens and Dobson, 1993). Backhouse & Dhillon (1996) identify the agents, the patterns of behavior and communications between agents (Backhouse & Dhillon, 1996) to infer security requirements. It is argued that an analysis of the structure of responsibility in organizations leads to the development of secure information systems. Dhillon and Backhouse (2001) mapped the current territory of information systems and security research by using the Burrell and Morgan framework as an intellectual map to analyze the socio-philosophical concerns in various information systems and security approaches. In addition, information systems and security research is analyzed and presented showing a need for the socio-organizational perspectives to be part of the IS security solution and criticized an over emphasis of technical solutions.

Awareness is a key conponent of IS security and has been researched from many perspectives (Pahnila, et al., 2007; M. Siponen, 2001; M. T. Siponen, 2000). Siponen (2000) looked at the normative and prescriptive nature of end-user guidelines in order to understand human behavior. A behavioral science framework, consisting of intrinsic motivation, a theory of planned behavior and a technology and an acceptance model, is described and applied to current approaches (such as the campaign) in the area of information security awareness and education. Strengths and vulnerabilities are assessed using their theoretical framework. Strategies aimed at increasing a users' commitment to security guidelines are presented. This study conceptually supports that IS security needs a theoretical framework for awareness and must take into account the vulnerability of an organization, not only from a technical standpoint, but from a socio-organizational perspective as well.

When an organizations' proprietary information is placed in the hands of its members, vulnerability exists. Understanding and perception of an issue can affect a member's behavior with respect to protecting the organizations' proprietary information. Incongruent behavior negatively affects IS security. It becomes a threat to the organization and a gap that needs closed. The approaches presented in this paper do not provide a complete, or even a partial solution, but together they provide sufficient background to present a useful conceptual framework that researchers and practitioners can use to help evaluate the potential impact organizational and behavioral issues may have on perceived and actual information security.

3. The IS Security Learning Loop Theoretical Framework

Mainstream accounts of security controls are shown to be ineffective when implemented on their own (Gurpreet Dhillon, 2007). It is a partial solution and although very useful, as the research and practitioners literature suggests (G. Dhillon & Backhouse, 2001) it needs to be extended into a more comprehensive solution. Mattia and Dhillon (2003) introduced action science (Chris Argyris, Putnam, & Smith, 1985) in the context of IS security, as a very different way of dealing with the failure to achieve intended security consequences. Mattia and Dhillon (2003) introduced double loop learning as a way to evaluate the mismatch between IS security espoused theory (i.e., policy mandates) and theory-in-use (i.e., what is done in practice).

3.1 Double Loop Learning

Double loop learning is a mindset where security problems are consciously sought out and resolved. It requires that resources be allocated in such a way that allows the correct mindset. The double loop mindset results in changing the underlying governing variables, policies, and assumptions of either the individual or the organization. Fiol and Lyles (1985) classify higher-level organization learning as a double loop process, yielding organizational characteristics such as acceptance of non-routine managerial behavior, insightfulness, and heuristics behavior.

3.2 Single Loop Learning

In contrast, the single loop mindset ignores any security contradictions. One reason is that the blindness is designed by the mental program that keeps us unaware. We are blind to the counterproductive features of our security actions. This blindness is mostly about the production of an action, rather than the consequences of the actions. That is why we sometimes truly do not know how we let something happen. Thus, organizations exhibiting single loop security have the mindset that comes from lower level organization learning. Double and single loop learning impact the bond between organizations and their members. This type of organizational learning is a way for perceived and actual information security practices to become congruent. Management or impact issues, operational and technical controls and individual behavior are some of the means that should be considered when focusing on measures for an agency-wide security program (Chew et al., 2008). Failure to achieve the intended result leads to a reexamination of the means (Chris Argyris, et al., 1985) and a search for more efficient measures. Administrative, operational decision making and technical controls, which are used for routine, programmed security activities or emergency situations would fall into the area of single-loop learning.

The security of information systems involves individual behavior, organizations and technical controls. Consequently, the Learning Loop process presented in this paper must consider all three for a more comprehensive solution to IS security. In addition, we must take into consideration that we are unaware of many of our theories-in-use (i.e., what is done in practice). This means that we supply the data that we can learn from, but don't recognize it. This adds a complexity to our security solutions and may account for some of the continued gap between the implemented technical solution to security and how secure an information system really is. One way we can close the gap is by using learning loops in IS security. How? By encouraging a learning mindset that increases awareness, so that others learn to see our theories-in-use (what we are unaware of) and we learn to see theirs. This means people are crucial to each other's learning (C. Argyris, 1982) and the security of their information systems.

3.3 Loop Learning

Loop learning is especially relevant to decision making skills that are necessary for security related management controls (strategic decisions) since it focuses on analysis of the assumptions and implicit rules underlying the organization and setting the security objectives and goals. Consequently, loop learning is an effective strategy for managing the two forms of theory of action.

The first theory of action is espoused theory, which is used to explain or justify a given pattern of activity. Examples include checklists, risk analysis and security evaluation, policies, plans and formal rules. Theory-in-use is the second theory of action, which is implicit in the performance of the pattern of activity. Theory-in-use is not a "given," it must be constructed from an awareness that occurs through the observation of the pattern of action in question. IS security loop learning is an adaptation to the double loop learning process. These changes include a sub-process to increase awareness, therefore making it a better tool to manage IS security (refer to Figure 1).

4. IS Security Loop Learning Awareness Theory

Unfreezing is a process that interrupts participants' unawareness of their theory-in-use. The notion of unfreezing was itself first developed by Lewin (1951), and it is built on the idea that existing theories or skills must be brought to awareness and unlearned before new ones can be learned. The participant must overcome inertia and dismantle the existing "mindset" (Lewin, 1951). To achieve this, behaviors must be identified that participants recognize as a valid sample of their own behavior. One way is for a group to choose one participant and identify the behaviors (i.e., behavioral and attitudinal) or mismatches. Mismatches are a consequence of ill-defined governing variables and inappropriate actions. Once the behaviors or mismatches have been discovered (awareness), the organization identifies the participants and the resulting vulnerabilities. Behavioral and attitudinal vulnerabilities have been well studied in the literature and are based on the theory of reasoned action (Ajzen & Fishbein, 1980); behavioral intentions are attitudinal (personal) and social (normative).

A series of low-level inferences about the nature of chosen participants' theories-in-use and the identified vulnerabilities should be generated. The participants can make and publicly test these inferences against espoused theory, while inquiring into the chosen participants' responsibility in any consequences. As participants engaged in the unfreezing process, they became aware of their theories-in-use for the first time, and this triggers an interruption of the participants' unawareness of their theory-in-use (Chris Argyris, et al., 1985). An effort to manage the identified vulnerabilities occurs at this point and if successful new governing variables are generated. Loop learning awareness (refer to Figure 2) theory has three basic steps that are initiated when a mismatch occurs in the process of loop learning.

IS security loop learning awareness theory indicates:

- **(Awareness) The discovery of espoused and theory-in-use**

  Participants first become aware through their own or group evaluations of their behavior that they are acting inconsistently and/or unfairly, but they are unaware of why they are acting the way they do. This is where an IS security threat can be accidentally triggered or intentionally exploited.

- **Identify vulnerabilities**

  As the process continues, the participants' self-confidence begins to decrease (attitudinal), and they start to feel less in control of themselves and less in touch with their intentions, evoking feelings of vulnerability. This is another point where an IS security threat can be intentionally exploited.

- **Efforts to manage vulnerabilities**

  Efforts to manage this vulnerability (threat) vary, depending on the individual and the actions of the other participants (social). Some participants may act defensively (attitudinal) but remain open to learning; for example, by confronting the other participants (social) while examining their own intentions and actions. Alternatively, other participants may act in ways that inhibit learning, rejecting efforts (attitudinal) to examine their own incongruent mindset (mismatches) or holding others participants responsible for their incongruent mindset.

It is important to note that, as the feedback loops indicate, those who actively inquire into and reflect on their actions tend to learn (acquire new actions) and to feel increased competence, as well as a new sense of confidence (attitudinal). In contrast, those who avoid such moves and resist (attitudinal) looking at their incongruent mindset tend to reinforce their present actions and their unawareness. This is point where governing variables can address the mismatches and generate new opportunities for security awareness, training, and education in the organization. Organizational learning is a learning mindset. It is two-fold, loop learning occurs through an awareness that results in improved managerial controls. Loop learning occurs when mismatches result in awareness and are then corrected by first examining and altering the governing variables and then the actions. Whereas, single loop learning occurs when matches are created, or when mismatches are corrected by changing actions (C. Argyris, 1993). The classification of lower level IS security (operational and technical level) is a single loop process, which yields organizational characteristics such as rules and routine. In IS security loop learning, the process of awareness creates an opportunity to uncover and manage vulnerabilities and inaccurate assumptions. It is a process that enables loop learning and espoused single loop processes. It encourages an awareness that leads to underlying management controls to be questioned and hypotheses about their behavior to be tested publicly. Loop learning leads to learning about the governing variables (managerial controls) of an organization and then using what is learned to solve security problems that are complex and which change as problem-solving advances.

It results in changing the underlying governing variables, policies, and assumptions of either the individual or the organization, but loop learning adds an opportunity to address accidently triggered or intentionally exploited.

4.1 Awareness, Vulnerabilities and IS Security Controls

When using IS security learning loops, technical controls (see Table 1) are integrated into the process of loop learning. Loop learning is significantly different from the inquiry characteristics of single loop learning. To begin, the organization must become aware of the security conflict. The actions have produced unexpected outcomes; this is a mismatch (error), a surprise. They must reflect upon the surprise to the point where they become aware that they cannot deal with it adequately by doing better what they already know how to do. They must become aware that they cannot correct the error by using the established security controls more efficiently under the existing conditions. It is important to discover what conflict is causing the error and then undertake the inquiry that resolves the security conflict. In such a process, the restructured governing variables become inscribed in the espoused theories. Consequently, allowing the espoused theories and theories-in-use to become congruent and thus more susceptible to effective security realization.

5. Methodology

To engage the IS security learning loop as a security tool, a different relationship is needed between participants. The learning loop framework is used to map IS security issues to espoused theory and theories-in-use. The resulting actions are intended to be jointly controlled, with participants taking responsibility for their own learning and therefore seeking an increased awareness. It is important to note that the IS security learning loop awareness theory can start out under conditions of inequity because on the outset participants are largely unaware of their theories-in-use and only vaguely aware or able to envision the alternatives. Participants therefore enter the learning loop process in a position of dependence on the framework to guide them. They uncover the implicit and discover in an explicit sense their own theories-in-use. This framework is a complex one, involving the continual unfolding (unfreezing) process of new awareness and actions on the part of the participants.

5.1 Using a Case Study Analysis to Test the IS Security Loop Learning Framework

This study must meet four methodological requirements when testing a theory using the natural science model. The theory must:

1. Be falsifiable. In effect, the theory must be formulated and stated in a way that it is open to being refuted by observation.
2. Be logically consistent. In effect, when deducing different predictions from the theory, they cannot be contradictory.
3. Display superior relative predictive power. In effect, it must be more explanatory than any rival theory.
4. Survive any attempts (thus far) to falsify it.

Lee (1989a, 1989b) argues successfully that qualitative case studies can be used to test theories in a controlled or logical deductive sequence that meet the natural science model of scientific research standards (see Table 2).

5.2 A Case of Hacking at Hyundai Capital Services, Inc.

It is useful to illustrate the concepts of loop learning and their applicability to IS security by applying the learning loop framework to an organization that experienced an IS security crisis. The organization chosen is South Korea's largest consumer-finance company, Hyundai Capital Services (HCS). Hyundai Capital Services, Inc. provides numerous financial services (Bloomsberg, 2011). Ted Chung is CEO of Hyundai Capital Services and a successful strategic level decision maker. He demonstrated this by leading one of the most successful turnarounds in recent Korean corporate history by selling a 43% stake in Hyundai Card and Hyundai Capital Services to GE Financial Services Co. and then adopting GE's risk-assessment practices. He understood the big picture of the business. He proved this by re-shaping the image of both firms and by doing so became one of the most widely followed Korean executives on Twitter. Hyundai Card and Hyundai Capital went from a $900 million loss in 2003 to a net profit of $714 million in 2010 (WSJ, 2010). This background information is important because the case study analysis must take the context into consideration when selecting a case and when reporting the findings and the practical implementations. The IS security incident that is the focus of this study began between March 6 and April 7, 2011 when a hacker stole personal customer information by implanting a malicious program in the company's homepage. The program was downloaded onto computers of customers who accessed the homepage. In the past, organizations have extensively relied on technical controls like access control systems as a principal means to manage access of authorized users.

Data on 1.75 million Hyundai Capital Services customers was leaked during the attack, but due to lax security practices the company was unaware. On April 7, 2011 CEO of Hyundai Capital Services, Ted Chung received a phone call saying its computer system had been hacked. The caller attempted to blackmail the company by threatening to release stolen confidential information onto the internet if Hyundai Capital Services didn't pay him.

6. Findings

The case study analysis generates numerous instances of loop learning from a strategic level (CEO) viewpoint that are noted in Table 3 and Table 4. Single loop learning is basically learned through the socialization process and may or may not be based on valid governing variables. This was noteworthy because it establishes the conceptual significance of the relationships and establishes the importance of using the loop learning IS security framework. The single loop mindset ignores any security contradictions. One reason is that the blindness is designed by the mental program that keeps us unaware. We are blind to the counterproductive features of our security actions. This blindness is mostly about the production of an action, rather than the consequences of the actions. That is why we sometimes truly do not know how we let something happen. Mismatches are a consequence of ill-defined governing variables and inappropriate actions. Loop learning occurs when mismatches result in awareness and are then corrected by first examining and altering the governing variables and then the actions. The organization identifies the participants and the resulting vulnerabilities. Awareness is necessary to establish valid governing variables and actions. The consequences of the security actions generate a match or a mismatch. The Hyundai Capital Services hacking was an instance of a mismatch. The case study has been compiled from information freely available from numerous online sources. It is only intended to be used for explicatory purposes in this instance of business research.

7. Practical Implications

The lessons of this hacking experience (awareness) have led to fundamental changes in the company (action) and how Chung leads it (governing variables). Considering the organizational situation after the hacking, a number of organizational issues emerged that could be appropriately placed in the categories of espoused theory and theories-in-use. The issues revolve around Hyundai Capital Services' use of information technology, but also involve organizational policies, public relations, and the management of risk (refer to Figure 3). Since the attack, Chung has spent weeks learning the ins and outs of network architecture, security infrastructure and the trade-offs between data protection and customer satisfaction. In Mr. Chung's words as reported by the Wall Street Journal interview (Ramstad, 2011), there are five lessons to learn from the experience: 1) Trust the authorities; 2) Stay open and transparent; 3) Learn IT and know where vulnerabilities are; 4) Create a philosophy that drives IT decisions; 5) Reassess plans for products and services.

7.1 Turning Lessons Learned into New Governing Variables:

Today, IT is central to everything a company does. Ted Chung used to treat his IT department as simply one of many units that helped the company get its job done. He admitted this was a big mistake after the hacking. The instance of hacking caused a mismatch in the IS loop learning process. Ted Chung became aware of the companies IT vulnerabilities. As a result, the case study analysis shows how five lessons learned from the mismatch turn into new governing variables and actions.

Governing Variable 1: Information Technology (IT)
Actions: The IT department reports directly to the CEO. The company took steps to ensure company growth and product development doesn't outpace computer security.
Lesson Learned: IT is central to an organization and network security is a top priority of IT.

Governing Variable 2: Have a learning mindset
Actions: "These days," says Chung, "the CEO should understand the basic structure of hacking even though he cannot do programming. No CEO is that stupid not to pay attention (to IT), but maybe they paid the same attention I did, which is increasing the budget, giving encouragement but then saying, What do I know about (IT)? That's the wrong support." Adds Chung, "Spend your time to understand IT….I believed I was too old to understand IT security issues. Nobody is too old or too remote for that." (MakingItReallyWork, 2011; Ramstad, 2011)
Action: "If you lock the restroom and garage because you are trying to protect the jewelry in the bedroom, sooner or later, the rest of the family complains and finds a way around it," Mr. Chung says. "Like everything, IT security needs a philosophy, and only the CEO can make that kind of a decision." (MakingItReallyWork, 2011; Ramstad, 2011)

Lesson Learned: Learn IT, create a culture of awareness and know where vulnerabilities may exist.

Governing Variable 3: Be Transparent
Action: "We got more people's help," says the CEO, "because we were transparent and open." Since Hyundai Capital's experience, other South Korean companies have reported hacking attempts. "Because we raised the flag," says Chung, "other companies are coming out to fight." (MakingItReallyWork, 2011; Ramstad, 2011) Ted Chung is one of the most widely followed Korean executives on Twitter.
Action: Consumers increasingly understand how vulnerable companies are to sophisticated hackers and mainly insist on being informed of breaches in Internet security.
Lesson Learned: Communicate openly about everything

Governing Variable 4: Align IT with policies.
Action: "We have to decide what kind of philosophy or policy direction we are going to take. For example," says Chung, "if we put in a much stronger security system, then our customers may have to wait a couple minutes every time they access our website. That's not an IT issue." It's an issue decided by executive management under advice from IT. (MakingItReallyWork, 2011; Ramstad, 2011)
Lesson Learned: Create IT policies and practices that support the company philosophy

Governing Variable 5: Balance IT strategies with IT support practices.
Action: "We need to put a price tag on every IT door and window," says Chung. Additional websites, additional online apps, wherever the outside world "touches" your organization may create new hacking routes. While Chung says security is now first for his firm, the need remains to balance risk and reward, growth and security. (MakingItReallyWork, 2011; Ramstad, 2011)
Lesson Learned: Continuously assess the balance of risk and reward, growth and security.
The main limitations of this study are inherent in the case study analysis research method used. Replication logic and the assortment of documents were limited. A variety of empirical studies are now needed to consider the validity and practical application of the IS security loop learning framework presented here.

8. Conclusion

This study is a IS security awareness approach that is theoretically and empirically grounded. The research suggests that the goal of an efficacious organizational loop learning process is to generate positive organizational consequences from the behavior and actions of individuals. The IS security learning loop framework is a tool organizations use to guide the learning loops process. It is used to analyze the behavior and actions, encourage a culture of awareness (match or mismatch), synchronize the governing variables to the strategic mission of an organization, and modify or change actions to create a congruency to the governing variables. Loop learning is especially relevant to uncovering the theories-in-use and managing them so that the formation of security related espoused theory results. Awareness is a key part of the process that contributes to organizational learning, which leads to the discovery of vulnerabilities. The goal of the IS security loop learning framework is to secure systems by organizing and emphasizing awareness and learning. When used properly the result is the discovery of vulnerabilities that need secured. Governing variables, individual and organization behaviors, actions and security controls (refer to Table 1) can be created or modified at this point into an equivalent state by making espoused theory and theories-in-use congruent.

The power of the IS security loop learning framework is that this "framework" draws attention to the integration of organizational behavior, actions into management, operational and technical controls. It is constructed to ensure the company philosophy and strategy drive IT practices and that employees comply with the governing IS security policies. The ability to perceive and appreciate the meaning of loop learning in IS security is enhanced by the IS security research literature presented at the beginning of this paper. These approaches investigate many of the same elements, and presented partial solutions to many behavioral issues. If we want to enrich our understanding of these issues further, we need to continue adding to the research and developing a more comprehensive solution that includes engaging the learning process. We may then discover why "awareness" + "change" is better defined as "learning," and why the involvement of the learner is so crucial to any kind of planned change or, as it might better conceptualize it-- "managed learning" as part of a comprehensive solution for IS security.

9. *References*

Ajzen, I., & Fishbein, M. (1980). *Understanding attitudes and predicting social behavior* (Paperback ed.). Englewood Cliffs, N.J.: Prentice-Hall.

Argyris, C. (1982). *Reasoning, learning, and action: individual and organizational* (1st ed. ed.): San Francisco: Jossey-Bass.

Argyris, C. (1993). *On organizational learning*: Cambridge, Mass.: Blackwell Publishers.

Argyris, C. (1993). *On organizational learning*. Cambridge, Mass.: Blackwell Publishers.

Argyris, C., Putnam, R., & Smith, D. M. (1985). *Action science* (1st ed.). San Francisco, (Calif.): Jossey-Bass.

Argyris, C., & Schon, D. A. (1978). *Organizational learning*. Reading, Mass.: Addison-Wesley Pub. Co.

AsiaOne. (2011). Hacking has no immed impact on Hyundai Capital Services Retrieved from AsiaOne website: http://www.asiaone.com/Business/News/Story/A1Story20110412-273242.html

Backhouse, J., & Dhillon, G. (1996). Structures of responsibilities and security of information systems. *European Journal of Information Systems, 5*(1), 2-10.

Baker, W., Hutton, A., Hylender, C. D., Joseph Pamula, P. D., Porter, C., & Spitler, M. (2011). Data Breach Investigations Report. Retrieved from www.verizonbusiness.com/dbir/

Baskerville, R. (1992). The Developmental Duality of Information Systems Security. *Journal of Management Systems, 4*(1), 1 - 12.

Baskerville, R. (1993). Information systems security design methods: Implications for information systems development. *ACM Computing Surveys 25*(4).

Bloomsberg. (2011). Consumer Finance Hyundai Capital Services Inc. Retrieved from Bloomsberg Businessweek website: http://investing.businessweek.com/research/stocks/private/snapshot.asp?privcapId=6454588

Chew, E., Swanson, M., Stine, K., Bartol, N., Brown, A., Robinson, W., & Gutierrez, C. M. (2008). NIST Special Publication 800-55 Revision 1 Performance Measurement Guide for Information Security.

Deci, E. L., Ryan, R. M. . (1980). *The Empirical Exploration of Intrinsic Motivational Processes. In: Advances in Experimental Social Psychology* (Vol. 13): (eds): L. Berkowitz Academic Press.

Dhillon, G. (1997). *Managing information system security*: Basingstoke, Macmillan.

Dhillon, G. (2007). *Principles of information systems security : text and cases*. Hoboken, NJ: John Wiley & Sons.

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

Fishbein, M., & Ajzen, I. (1975). *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research*: Addison-Wesley, reading, MA.

Infosecindia. (2011). Suspected hackers caught in Hyundai Capital data leak case. Retrieved from Infosecindia website: http://infosecindia.com/2011/04/19/suspected-hackers-caught-in-hyundai-capital-data-leak-case/

Lee, A. (1989a). A scientific methodology for MIS case studies. *MIS Quarterly, 13*(1), 33-50.

Lee, A. (1989b). Case Studies as Natural Experiments. *Human Relations, 42*(2), 117.

Lewin, K. (1951). *Field theory in social science; selected theoretical papers* ([1st ed.). New York,: Harper.

MakingItReallyWork. (2011). Lessons Learned - What a CEO learns from a hack Retrieved July 10, 2011, from http://www.makingitreallywork.com/

Mattia, A., & Dhillon, G. (2003). *Applying double loop learning to interpret implications for information systems security design.* Paper presented at the Systems, Man and Cybernetics, 2003. IEEE International Conference on.

Pahnila, S., Siponen, M., & Mahmood, A. (2007). *Employees' behavior towards IS security policy compliance*.

Ramstad, E. (2011). Executive Learns From Hack Retrieved from Wall Street Journal website: http://online.wsj.com/article/SB10001424052702303936704576395123202899068.html

Siponen, M. (2001). Five dimensions of information security awareness. *SIGCAS Comput. Soc., 31*(2), 24-29. doi: 10.1145/503345.503348

Siponen, M. T. (2000). A Conceptual Foundation for Organizational Information Security Awareness. *Information Management & Computer Security, 8*(1), 31-41.

WSJ. (2010). Hyundai Executive Challenges Korean Ways *2011*(June 16). Retrieved from The Wall Street Journal website: http://online.wsj.com/article/SB10001424052748703999304575398720358607774.html

Yin, R. K. (1994). *Case study research : design and methods* (2nd ed.). Thousand Oaks: Sage Publications.

Yonhap. (2011). (LEAD) Regulator plans to discipline Hyundai Capital over hacking Retrieved from YONHAP NEWS AGENCY website:
http://english.yonhapnews.co.kr/business/2011/05/18/55/0503000000AEN20110518003500320F.HTML

10. Figures and Tables

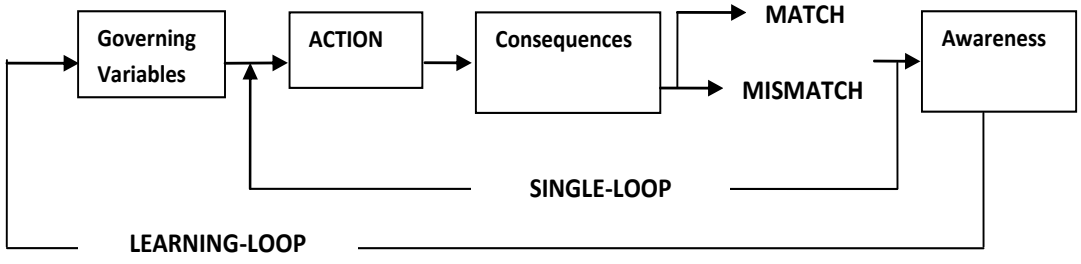

Figure 1: IS Security learning loops.
Adapted from (C. Argyris, 1993)

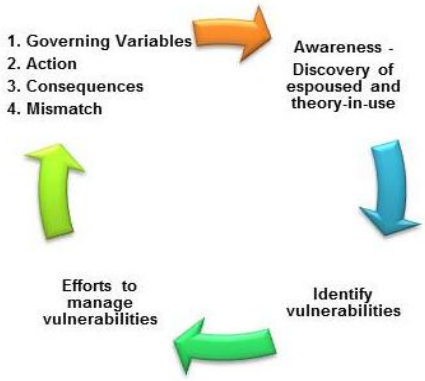

Figure 2: IS Security Loop Learning Awareness Theory

Figure 3: IT is central to organizations

Table 1: Emphasis of IS security loop learning on security controls

LOOP LEARNING Awareness	SINGLE LOOP Protect Vulnerabilities
Governing Variables **Management Controls** 1. Risk Management 2. Review of Security Controls 3. Life Cycle Maintenance 4. Authorize Processing (Certification and Accreditation) 5. System Security Plan 6. IS Security Loop Learning Framework 7. Other	**Actions** **Operational Controls** 6. Personnel Security 7. Physical Security 8. Production, Input/Output Controls 9. Contingency Planning 10. Hardware and Systems Software 11. Data Integrity 12. Documentation 13. Security Awareness, Training, and Education 14. Incident Response Capability **Technical Controls** 15. Identification and Authentication 16. Logical Access Controls 17. Audit Trails

Table 2: Quality Social Science Research Design Guidelines

Measure:	Guidelines from the literature (Lee, 1989a, 1989b; Yin, 1994)	Whether/how the guidelines are followed in this study
Construct Validity	Use multiple sources of evidence Maintain a chain of evidence Having key informants review the case study report	221 documents in a variety of formats (interviews, articles and webpages) were analyzed. Deduce theory from the literature and test the resulting framework by comparing them to the actual state of a specific case. A IS security person and non-IS person review a draft of the case study.
Internal Validity	Pattern matching	Empirical patterns were matched with framework deduced from the literature. ‘‘Natural controls’’ were used wherever feasible.
External Validity	Increasing degrees of freedom Applying replication logic	Multiple observations for the case Competing theory investigated but not tested Framework investigated (tested) in the before and after instances; each instance can be seen as a separate study.
Reliability	Creating/maintaining a case study database Developing a case study protocol	Case study notes (annotated documents) Case study documents (interviews, articles, webpages) Tabular materials (archival data) Case question-and-answer format; Literature review; case framework and models.

Table 3: Case Study Analysis Using the IS Security Loop Learning Framework BEFORE the Hacking

MATCH OR MISMATCH	AWARENESS	GOVERNING VARIABLES	ACTIONS	CONSEQUENCES
Ted Chung led one of the most successful turnarounds in recent Korean corporate history. He re-shaped the image of the firm and became one of the most widely followed Korean executives on Twitter.	Ignores security contradictions	**Espoused Theories** Information-technology department is simply one of many units that helped the company get its main job done How things look and how they work most important Increase the IT budget, give encouragement, but have little technical knowledge.	**Theories-in-use** Lax computer security Crazy making apps, creates a new route for hacking Did not meet electronic trading regulations.	Ted Chung received a phone call saying HCS's computer system had been hacked. The caller threatened to release stolen confidential information if the company didn't pay him. Data of some 1.75 million customers was leaked during the attack.
Data Sources: (Ramstad, 2011; WSJ, 2010)				

Table 4: Case Study Analysis Using the IS Security Loop Learning Framework AFTER the Hacking

MATCH OR MISMATCH	AWARENESS	NEW GOVERNING VARIABLES	ACTIONS	CONSEQUENCES
Ted Chung received a phone call saying HCS's computer system had been hacked. The caller threatened to release stolen confidential information if the company didn't pay him. Data of some 1.75 million customers was leaked during the attack	**MISMATCH** Ted Chung was too mystified to be shocked. "The whole thing was not very clear for me to get shocked," he says. "We had to figure out what really had happened."	**Espoused Theories** 1) Trust the authorities; 2) Stay open and transparent; 3) Learn IT and know where vulnerabilities are; 4) Create a philosophy that drives IT decisions; 5) Reassess plans for products and services. How things look and how they work is now secondary. Security is now first. Put a price tag to everything IT. The IT department, which has added a security unit, now reports directly to the CEO.	**Theories-in-use** Changed the way Ted Chung does his job. The experience led to fundamental changes in the structure of the company, as well as his own thinking about how he leads it. We had a press interview right away the next day. We contacted our clients to update them. Understand the basic structure of hacking even though cannot do programming.	Slow down the whole organization. Hacking incident does not have an immediate impact on the credit profile of HCS. No financial damage has been reported so far in relation with the hacking case, but potential damage is probable down the road. In the course of the "investigation, police also found that a former Hyundai Capital data center employee who quit at the end of last year illegally accessed the company's personal information system" FSS has formed a public-private task force, assigned with inspecting financial firms.
Data Sources: (AsiaOne, 2011; Infosecindia, 2011; MakingItReallyWork, 2011; Ramstad, 2011; Yonhap, 2011)				