Information Systems Principles for Developing Secure Information Systems

Bennet Hammer and Roy A. Boggs
Florida Gulf Coast University, Fort Myers, FL, USA

bennethammer@comcast.net rboggs@fgcu.edu

Abstract

Even though there have been several Information Systems Security (ISS) methods put forward, especially the ISS design theory framework and six kernel theories with distinctive principles of Siponen and Iivari (2006), these methods very often lack security features referencing the actual users themselves. This study proposes that, when developing secure systems without design principles focused on end users, efficient and effective secure system designs cannot be achieved. This study coalesces the principles of these works with the principles proposed by Siponen and Iivari (2006) in order to better understand the relationships among styles of thinking by end users in making systems security decisions. This is by nature an interdisciplinary undertaking, which in turn identifies those assumptions about the characteristics of systems thinking that can be used to design secure system, built upon end user considerations. And by focusing secure systems design principles on the end user, future ISS will be become more efficient and more secure.

Keywords: Systems Design, Secure Systems, End User Security, Information Systems Security

Introduction

Past research has shown that Information System development methods lack security features (Baskerville, 1993). To overcome this problem, several Information Systems Security (ISS) methods have been proposed, which include an ISS design theory framework and six kernel theories with distinctive application principles (Siponen & Iivari, 2006). However, the modern ISS approaches have received little attention in either the ISS literature or practice (Siponen & Iivari, 2006). Researchers need to better understand the design principles for developing secure systems.

As described by Siponen and Iivari (2006), the modern world increasingly relies on the use of computers for ensuring information systems security. Therefore, it is very important that an organization's information systems are properly secured to prevent any loss or damages. Even though technical solutions and secure system development methods exist for securing organization's systems, researchers agree that an information system security policy and enforcement is the necessary foundation to prevent any information losses or damages (Siponen & Iivari, 2006).

Straub and Welke's (1998) research shows that information security continues to be neglected by managers and employees in organizations. Information security managers waste a lot of money and resources due to their lack of knowledge. These managers often put secure information at risk and create a

potential loss for future business. Sun, Srivastava, and Mock's (2006) research showed that the estimated security loss caused by all security incidences is estimated at a total loss of $130 million annually in the United States. The study also revealed that there is an estimated $31 million annual loss caused in the United States by theft of proprietary information as well (Sun, Srivastava, & Mock, 2006). Over the years, a number of substantial research studies have shown actual or potential system losses due to the failure of securing the systems.

Although practitioners and academics stress the importance of security governance that involves end-user behaviors, there has been minimal research conducted on behavioral information security. Most of the studies conducted in the past focused on the organizational security practices and their effectiveness. Since the prior studies focused on IT administrators and top-level managers it is questionable whether their views are representing the organization at large. For example, the research study adopted by Dhillon and Torkzadeh (2006) focuses on "a broader perspective and presents an understanding of IS security in terms of the values of people from an organizational perspective" (p. 293). Additionally, the research conducted by Straub and Collins (1990) focuses on the need to minimize the information liabilities of managers and their organizations. The study identifies key issues and highlights implications for information managers (Straub & Collins, 1990). However, both studies just focus on IT administrators and top-level managers and not the end-user community.

While many organizations have information security policies and procedures in place, many employees tend to ignore them. As indicated by Vroom and Von Solms (2004), statistics demonstrate that not all security breaches are deliberate, but rather the result of negligence or ignorance of the security policies of the organization. Furthermore, in an organizational setting, it is very uncertain how employees act toward security policies especially when employees and IT management have conflicting interests (Herath & Rao, 2009). Employees may opt to break security policies for malicious purposes and harm the organization or they may choose to adhere to the security policies. According to Dhillon (2001), violations of safeguards by trusted personnel resulting in information security breaches are real and need to be addressed. Herath and Rao (2009) suggested that organizations start to monitor the behavior of their employees by employing surveillance control systems in the workplace. However, monitoring every information security related action of every user in the organization could be very costly and may not be practically possible.

It is arguable that with the lack of design principles focused on the end users for developing secure systems, efficient and secure system design cannot be achieved. Furthermore, it is vital to understand the fundamentals of system design beginning with C. West Churchman (1971) in order to build on these principles to achieve secure system design. Having no understanding of these principles is one of the reasons why computer abuse and computer disasters are very high.

Theoretical Development

A - Information Systems Security Design Theory Framework (Siponen and Iivari, 2006)

Siponen and Iivari (2006) proposed a theoretical framework that addresses the issue of the unpredictability in the business environment and how it forces organizations to make rapid business decisions. In order for an organization to handle such an exceptional situation, organizations may be required to temporarily violate the predefined information systems security policies. Siponen and Iivari (2006) argue that normative design theories offer insights for organizations to handle exceptional situations. Specifically, Siponen and Iivari (2006) introduce six design theories such as the conservative-deontological, liberal-intuitive, prima-facie, virtue, utilitarian, and universal-

izability theories that can help guide the application of information systems security policies. Specifically, in the case that the conservative-deontological theory is applied, the Information Systems security policies and guidelines must be followed exactly without thinking about the possible consequences (Siponen & Iivari, 2006). The opposite view is the liberal-intuitive theory, which states that in the case that certain situations are not covered in the information systems security policies and guidelines the employees can do whatever they want in those situations (Siponen & Iivari, 2006). The prima-facie theory recognizes that guidelines should be followed in general, however, one may violate the guidelines if the business benefits outweigh the benefits of complying with them (Siponen & Iivari, 2006). The virtue theory focuses on cultivating the proper virtues in exceptional situations and the utilitarian theory suggests that the key issue is the maximization of utility (Siponen & Iivari, 2006). Whereas the universalizability theory suggests that the action should be one that one would except no matter in what position that person is (Siponen & Iivari, 2006).

The research study conducted by Siponen and Iivari (2006) develops an ISS design theories with application principles by which conflicts can be resolved. As the research showed, the conservative-deontological theory is recommended for stable business environments (Siponen & Iivari, 2006). The prima-facie, virtue, utilitarian, and universalizability theories are recommended to be utilized by outside rule-oriented organizations (Siponen & Iivari, 2006).

B - A Review of Formal Inquiry Systems (Churchman, Mitroff, Richardson, Courtney, & Paradice)

As important as the proposals by Siponen and Iivari (2006) are, they need a more interdisciplinary underpinning. To their research must be added knowledge gained from earlier studies of inquiry systems, especially those of Churchman (1971), Mitroff (1974) and Courtney, Croasdell and Paradice (1998). They represent different academic fields, but ones that are relevant for understanding end users. Churchman (1971) had interpreted the viewpoints of philosophers Leibniz, Locke, Kant, Hegel and Singer in the context of designing information systems. Unfortunately, very little attention has been given in literature to developing an understanding of human capabilities critical for system design in organizations with an emphasis on creating secure and efficient systems. The following is a brief review of this research.

The concepts of inquiry systems that Churchman (1971) introduced have been studied and implemented in many sciences, including public policy (McIntyre, 2003), environmental sciences (Richardson, Courtney, & Paradice, 2001), management systems, and behavioral and religious sciences (Eriksson, 2003). However, technology and information systems' disciplines have lately focused on mathematical calculations and formulas to develop new tools and applications to solve business problems; and it has involved the theoretical foundations of information and computation along with its applications in computer systems. It has driven a significant trend of continuous improvement, not only in processes and operations, but also in supporting making-decisions and competitive strategies (Davis, Fuller, Tremblay, & Berndt, 2006). These concepts provide only a historical knowledge of inquiry systems, but no science to incorporate inquiry systems analysis. There is one very important factor that is being ignored which will become the main focus for future development of new systems; it is the involvement of people and the human factors, which Churchman (1971) refers to in his work, in secure systems development.

The models of inquiry systems have inputs, processes, and outputs. The output of an inquiring system is considered as true knowledge, or at least knowledge that is believed not to be false. One of the most distinctive features of inquiring systems design is the inclusion of elaborate mechanisms for guaranteeing that only valid knowledge is produced. The guarantor (guarantees a valid result) in scientific inquiry is generally based on the use of the scientific method, and scientists in general include many checks and balances that usually consume a great deal of time and effort, to

ensure that the results of their inquiries are acceptable to the rest of the scientific community. All five inquiry modes identified by Churchman (1971) contain analogous provisions for ensuring that outputs are consistent with the underlying philosophy, so that the knowledge generated may be considered valid for all time. These are reviewed here for later reference.

Leibnizian inquiring systems

According to Churchman (1971), a Leibnizian inquiring system is a closed system with a set of built-in elementary axioms that are used along with formal logic to generate more general fact nets or tautologies. This system, which is rational in nature, mainly relies on the theory of autopsies for its existence. The fact nets are created by identifying hypotheses, with each new hypothesis being tested to ensure that it could be derived from, and is consistent with, the basic axioms. Once so verified, the hypothesis becomes a new fact within the system. The guarantor of the system is the internal consistency and comprehensiveness of the generated facts.

Leibnizian inquiring systems can be considered as a small society or culture where the basic theorems are so defined and mutually consistent with any direct element in that specific culture. In other words, new ideas, vision, future plan, and the way of thinking developed within the culture must be compatible with the existing principles. Therefore, anything new that has been created by the system will be in a creative tension so that it can be brought closer to the system vision or goal. Such a test of consistency must be and will be continuously reviewed for accuracy and up to par with the rest of the system (Churchman, 1971).

According to Ian Mitroff (1974), the Leibnizian inquiry system is characteristic of formal-deductive systems. It is purely theoretical and emphasizes the formal, mathematical, logical, and rational aspects of human thought. The Leibnizian inquiry system is strong in consistency, precision, and a lack of ambiguity. It is weak in the same points that make it strong: rigor, precision and logic.

Courtney, Croasdell, and Paradice (1998) explain the Leibnizian inquirer as one who learns by using logical thinking to make decisions of cause and effect. According to Courtney, Croasdell, and Paradice (1998), this inquiry system shows that certain components of a system are used to make new components enabling the system to be recreated. This method uses a closed system; thus it only has the power of knowledge generated internally. Any new changes within the organization must be compatible with the previous policies and procedures. One should not ignore the fact that it is possible and likely that once at a certain level of learning, everything stops and the organization falls behind. Once this happens, it is very difficult to return to high success. Because the inquiry system is closed by definition and there is an assumption of an absolute guarantor within the Leibnizian process, there is not an opportunity to question or refute the guarantor. Therefore, this system relies completely on the accuracy and integrity of the guarantor, which makes the Leibnizian inquiry facts and decision indefensible. Leibnitzian inquiry represents an expert systems decision making process. When applying the Leibnizian inquiry system to information technology, a few examples include: an online registration page for an e-newsletter; a shopping cart software application for an online retailer; and a GPS application for use in a car. The security of these systems depends upon guaranteeing an uninterrupted, accurate, and secure data flow. Additionally, according to the research conducted by Zajac, Kraatz, and Bresser (2000), the Leibnizian inquiring system could be interpreted and described as a strict normative decision making in the sense of von Neuman theory. The basic information for description and interpretation of the human notions are expert relations measured in different scales, theorems of existence, utility function evaluation, optimization procedures in accordance with the measurement scales and final optimal decisions in normative sense.

Lockean inquiring systems

Churchman (1971) defines the Lockean inquiring system as experimental and consensual. It is capable of supporting itself with both an adaptive and a generative method of learning. In contrast to the Leibnizian inquiring systems, the Lockean inquiry system is an open system and can be influenced by elements outside its environment. Empirical information, gathered from external observations, is used inductively to build a representation of the world (Churchman, 1971). It consists of no built-in preconceptions of the world and is set apart from the rest the world by how the learning process occurs. Elementary observations form the input to the Lockean inquirer has a basic set of labels which it assigns to the inputs, and is capable of observing its own process by means of reflection and backwards tracing of labels to the most elementary labels. Agreement on the labels by the Lockean community is the guarantor of the system (Churchman, 1971).

According to Ian Mitroff (1974), the Lockean inquiry system perpetuates the purely sensory and empirical aspects of human knowledge. The primary strength of the Lockean inquiring system is the potential for great amounts of experiential data to be included from a group. Two major weaknesses of Lockean inquiring system are that the experience can be fallible and misleading which leads to assumptions by the guarantor and the potential cost that exists for arriving upon an agreement.

Courtney, Croasdell, and Paradice (1998) explain the Lockean inquiring system as an organization that learns by making observations about society and expressing these observations enabling one to create a conclusion for what has just happened. Lockean inquiring system attempts to build teamwork among the members and come to an agreement with everyone helping to create organizational knowledge. This type of inquiry supports both adaptive and generative learning. These systems are willing to listen to outside opinions for new ideas or ways to look at a given scenario. Lockean inquiring system believes this is why it is possible to see everything that happens in an event. However, because of these factors, the group or guarantor of the system may need to make broad or incorrect assumptions and thus, make the decisions unreliable. Lockean inquiry is best represented by the group decision support system.

An information technology example in terms of this inquiry system is the Delphi Exercise, which involves a group of participants that share some common characteristic. Their input is the raw data for the system, and their agreement transforms the data into well-substantiated policy for the group. Another example of how Lockean learning is achieved is in deciding whom to hire for a position. Since it is unlikely that total agreement will happen, it is likely that the group would agree on the advertising of the hire. Using agreement among its members enables the organization to experience a shared vision. Vision and agreement are two necessary specifics for creative tension, and the guarantor of a Lockean inquiry system is the group creating the knowledge. Therefore, the system security depends upon guaranteeing secure and correct human interaction with the data flow. Furthermore, the Lockean inquiring system could be interpreted and described as a group decision making process. If the measurement scales are “ordering” then the Arrow's impossibility theorem applies (French, 2007). A possible solution would be to follow the research conducted by Hammond, Keeney and Raiffa (1999), which suggests measurements in interval scales and construction of multi attribute utility functions.

Kantian inquiring system

As defined by Churchman (1971), the Kantian inquiring system is a mixture of the Leibnizian and Lockean inquiry modes in the sense that it contains both theoretical and empirical components. The Kantian inquiring system scans both internal and external environment for true knowledge. The empirical component is capable of receiving inputs, so the system is open. It generates hypotheses on the basis of inputs received. The Kantian inquirer is able to use explicit knowledge and tacit knowledge to consider the many interpretations of inputs. This allows the system to

compare incoming knowledge to what is already located in the system memory and to create and incorporate that new knowledge.

Perhaps the most unique feature of Kantian systems is that the theoretical component allows an input to be subjected to different interpretations. This occurs because the Kantian theoretical component maintains alternative models of the world. Representations and interpretations are based on causal connections maintained in the models. The theoretical component contains a model building constituent, which constructs Leibnizian fact nets. It tests the alternatives by determining the best fit for the data, and the guarantor in this approach is the degree of model/data agreement. Additionally, an executive routine can turn the Kantian models on and off and can examine their outputs in terms of the degree of satisfaction with their interpretations. Therefore, if a model does not produce satisfactory results it can be turned off, while those that are more successful can proceed.

Ian Mitroff (1974) explains the Kantian inquiring system to be characteristic of synthetic multimodel systems. Kantian inquiring system is synthetic because it seeks to reconcile the rationale of Leibnizian inquiring system with the empirical of Lockean inquiring system. They are multimodel because they produce at least two alternate models (Mitroff, 1974). Due to its synthetic nature, the greatest strength of Kantian inquiring system is in their ability to counter the weaknesses of the Leibnizian and the Lockean inquiring system. The weaknesses of Kantian inquiring system are due to the multiple models presented. The correct answer is uncertain and not guaranteed in the models presented. The inquirer may not have enough knowledge to choose the appropriate model, and multimodel systems are more costly to operate.

Courtney, Croasdell, and Paradice (1998) view the Kantian inquiring system as a system that uses internal and external environments for creating useful and meaningful knowledge. Kantian inquiring system believes new knowledge is created from existing knowledge which gives it the characteristic of both open and closed systems. Using hunches, intuition, and experience, Kantian based inquiry is able to see variations of inputs. This incoming knowledge is compared to original organizational structure enabling one to create new knowledge. While decisions are made based on open input and consensus, there is no guarantee that the process or guarantor represents the best solution. Decisions are subject to bias and incorrect input of information.

Kantian theory can best be seen in the Decision Support System (DSS) decision process. One example of a Kantian inquiring system example in information technology is when a project manager is presented with the task of determining the best mix of software and hardware for a new project. There are several options, or models, available for the project manager to select from and then use experience and data to pick from the models, but there is no guarantee that the mix of software and hardware chosen is the correct mix. Another example of a Kantian inquiring system as applied in information technology is for the running of a new online advertising campaign. Various advertisements are often used to determine which method receives the most hits. Each advertisement produces a different model to be evaluated; then the advertisement or advertisements are selected. When this happens simultaneously, the organization in the advertisement along with the marketing agency both have the chance to learn about the product market for that specific area. The system security depends upon guaranteeing correct assumptions about the security of the data flow. Furthermore, the Kantian inquiring system could be interpreted and described as a system which includes the previous two system and additional logical rules. The system has to include a module for determination of the structure of the main purpose. The system is open in the sense that the main purpose and the structure are refined iteratively.

Hegelian inquiring systems

Churchman (1971) defines a Hegelian inquiring system to be a system that functions on the premise that greater enlightenment results from the conflict of ideas. The Hegelian dialectic is comprised of three major players. The first player begins the dialectic with a strong conviction about a fundamental thesis. The second player is an observer of the first subject. The observer generates an opposing conviction to the original thesis. In fact, the observer is passionately dedicated to destruction of the first subject's conviction (Churchman, 1971). The final player in the Hegelian dialectic is a bigger mind and an opposition to the conflict between the thesis and the antithesis. This bigger mind synthesizes a new view of the world which absorbs the thesis/antithesis conflict. Synthesis generated by the objective bigger mind acts as guarantor of the system. The promise made is that the movement from thesis-antithesis to synthesis is a soaring to greater heights, to self-awareness, more completeness, betterment, progress (Churchman, 1971).

The Hegelian systems rely upon the dialectic to resolve diametrically opposing viewpoints, the thesis and antithesis. In the Hegelian component of an inquiring system, arbitration is used to evaluate and synthesize contributions from opposing viewpoints resulting in a larger mind which absorbs the thesis/antithesis conflict. Knowledge gained through Hegelian inquiry may result in an entirely new strategic direction for a given system.

According to Mitroff (1974), Hegelian inquiring system is characteristic of conflictual and synthetic systems. They embody the antagonistic and conflict components of human thought. Strengths of the Hegelian inquiring system include: the decision maker is involved in creating knowledge; the process is active; and the conflict can create interest. Not all personalities, however, are geared to conflict, and this is a major weakness of Hegelian inquiring system. In fact, the cost of debate, without a guarantee of resolution or knowledge creation, is another weakness of this system.

Hegelian inquiry in organizations has little structure or formal mechanisms to guide it. Group support systems that include negotiating and arbitration elements assist organizations in Hegelian inquiry. An example of Hegelian inquiring system in information technology involves business managers meeting with programmers to debate the difference between what was documented in user requirements during systems analysis and what is actually functional, but not satisfactory, in the testing phase of development.

A potential weakness of the Hegelian system is within the guarantor of the bigger mind. Due to bias or inequity of the conflict and synthesis process, the prevailing thesis may not always be the correct thesis. The system security depends upon guaranteeing a correct selection of alternatives for the security of the data flow. Additionally, Hegelian inquiring system could be developed in a gaming environment. The empirical information (data flow, functions in min-max procedures) have to be measured obligatory in interval scales.

Singerian inquiring systems

Churchman (1971) declared two premises when defining the Singerian inquiring system. The first premise establishes a system of measures that specify steps to be followed in resolving disagreements among members of a community; and the second principle guiding Singerian inquiry is the strategy of agreement (Churchman, 1971).

Mitroff (1974) explains the Singerian-Churchmanian inquiring system as characteristic of interdisciplinary, synthetic systems. These systems are holistic in nature and call upon aspects of human knowledge that include: scientific, ethical, and aesthetic (Mitroff, 1974). Mitroff (1974) describes Singerian inquiry as believing that reality is not proven but arrives when enough decision makers are convinced as to what is real. According to Mitroff (1974), both systems differ from

Lockean inquirers because they presuppose that raw data is correct input for a system, since the input is based on prior consensus.

Courtney, Croasdell, and Paradice (1998) assert that the purpose of the Singerian inquiring system is to establish knowledge for deciding the proper means for one's end. Knowledge is judged by making improvements which are considered to be measurable. These improvements are considered in seeing what is best for the society. Knowledge should be useful to everyone in the company or organization in order for it to be effective. Employees play a big role in making decisions for the organization. While the Singerian inquiry model provides flexibility and open input into the inquiry process, these attributes may make the decision process unreliable, uncertain, and negative. Although an observer exists within the system, there is no oversight of the observer.

Applications of the Singerian inquiring system are aligned with the Executive Support System (ESS). Examples of this inquiry system can be seen in the Institute of Electrical and Electronics Engineers (IEEE) and the International Organization for Standardization (ISO) standards process. Singerian inquirers pay close attention to new technologies coming out that will make advancements within the organization. A specific example would involve the concurrent and future release of open source code for a particular operating system. The system security depends upon guaranteeing tools and applications to manage and secure data flows. Furthermore, the Singerian inquiring system is a mixture of the previous four systems. The construction of such a system needs accordance between the different measurement scales and the used mathematical methods. The first step is obligatory structuring of the main purpose to sub-objectives and criteria and determination of the appropriate measurement scales, utilization of factor analyze, and pattern recognition.

C- Information Systems Security Design Theory Supported by Formal Inquiry Systems

It is necessary not only to learn, but also, to understand how human inquiry systems affect decision-making processes. The discussions by Churchman (1971), Mitroff (1974), and Courtney, Croasdell, and Paradice (1998) proffer philosophical and interdisciplinary underpinnings for the six levels suggested by Siponen and Iivari (2006). Organizational learning is the formation of new knowledge that has the opportunity to be molded into creating and influencing new behaviors. Inquiring systems and knowledge management matched with advances in information technology such as the intranets and extranets increase knowledge. Most of the technology modules have used mathematical models or programmed logic to solve an organization's problems. However, without human capital such knowledge would not be possible; and humans do not all make the same decisions in the same manner. This applies equally as well to interacting with secure information systems.

The first information inquiry systems presented above is classified as a Leibnizian inquiry system and the second system is known as a Lockean inquiry system. Leibnizian systems are closed systems with no way of seeing the external environment. These systems operate based on axioms and fact nets that are known and may be put into competency traps. For Siponen and Iivari (2006) these might be understood as conservative-deontological where security policies and guidelines are to be followed exactly and without thinking about the possible consequences. Lockean systems are also closed, but are based on consensual agreement; and, with Siponen and Iivari (2006), one would expect a universality in which people would make the same decisions when faced with the same data. For both of these types of systems, one is faced with the intense and demanding environment today, compiled with the need for variety and complex interpretations, that are crucial in determining how decisions are made. If one cannot guarantee an uninter-

rupted, accurate and secure data flow, or if one cannot guarantee secure and correct human interaction with the data flow, then other systems need to be considered.

Two other types of inquiry systems as presented above are meant for a multiplicity of world views. These are open systems. Kantian inquiry systems consider numerous views of a complementary nature that coalesce as the best solution for a current situation. Based on the fundamentals of Siponen and Iivari (2006), a utilitarian aspect exisits which suggests that the key issue is utility. Look at the different possibilities and make the best fits the problem at hand. Here the system must guarantee correct assumptions about the model under consideration and the data flow. Even so these systems may still be affected by traps characterized by plurality. Hegelian inquiry systems are recognized by multiple completely antithetical representations that are seen by some type of conflict. Hegelian systems use multiple interpretations (models) along with contradictions of focal information. This type of method calls for the constant readiness for change to happen and being ready to modify the problem readily. Furthermore, Siponen and Iivari (2006) suggest that the prima-fascia theory recognizes that guidelines should be followed in general; however, one may violate the guidelines if another option (model) would be more beneficial. An information system must then guarantee a correct selection of alternatives for the security of the data flow; and in open, multiplicity systems security depends upon making correct choices.

Singerian inquiry systems are pragmatic, eclectic and seek the shortest route to a payoff with an interest in innovation. They employ as needed any or all of the four formal systems discussed above. For Siponen and Iivari (2006) these are similar to the liberal-intuitive in which case certain situations not covered in security policies and guidelines permit novel and interesting solutions. It is, of course, understood here that virtue cultivates proper solutions even in exceptional circumstances. Security depends to a large degree on guaranteeing proper tools and choices.

There is a readiness for the consideration of the Kantian and Hegelian models that can provide the diverse and contradictory interpretations that are necessary. Being able to generate semantic views of the future with the increase in change will make surprises become anticipated rather than predicted. The individual in an organization plays a crucial role in the understanding of meaning. Thus, this is the importance of the human role in making knowledge happen in inquiring organizations.

Information technology enabled knowledge management is maintained by the way of the knowledge creation processes. These types of inquiring systems have given attention to the evolution of knowledge, the dimensions of knowledge creation, the making of the meaning of knowledge creation and the constructive nature of knowledge creation. These items are not necessarily meant to be limited as the only ones, but they do highlight some of the most important processes used during knowledge management.

The research study conducted by Siponen and Iivari (2006) provides an understanding of the philosophical approaches that can be employed when developing a security policy. Furthermore, by having this understanding, it is achievable to use a security policy approach that matches the organization’s culture. The understanding of the philosophical approaches is especially valuable if the life cycle development process is applied to policy development. This process should be a component of defining the organization's needs as it sets the parameters of the security policy. Based on the characteristics originally defined by Churchman (1971), Mitroff (1974), and Courtney, Croasdell, and Paradice (1998) and the theoretical framework proposed by Siponen and Iivari (2006), the following table shows a listing and progression of the profile generation stage. Its purpose is to support a wider dialog on ISS principles.

Table 1. Characteristics Applied

	LEIBNIZIAN	LOCKEAN	KANTIAN	HEGELIAN	SINGERIAN
PEOPLE	• Analyst • Formal logic & deduction • Seeks models & formulas theory and method over data • Theory and method over data	• Realist • Empirical view & induction • Seeks solution that meets current needs • Data over theory	• Idealist • Assimilative or holistic view • Seeks ideal solutions • Data & theory of equal value	• Synthesist • Integrative view • Seeks conflict and synthesis • Data meaningless w/o interpretation	• Pragmatist • Eclectic view • Seeks shortest route to payoff • Interested in innovation • Any data or theory that gets us there
	↕	↕	↕	↕	↕
PROPERTIES OF LEARNING	• Closed System • Behavioral adaptive learning style • Syntactic learning source	• Open system • Consensual, generative learning style • Pragmatic learning source	• Open/Closed system • Cognitive, generative learning style • Pragmatic/Semantic learning source	• Open system • Generative double-Loop learning style • Semantic learning source	• Open system • Generative, do loop learning style • Syntactic /Pragmatic learning source
	↕	↕	↕	↕	↕
INQUIRY SYSTEMS FOR INFORMATION RESOURCES ANALYSIS AND SECURITY POLICIES	• Rational • Formal-Didactic • Fact-Net • ES • Guaranteeing an uninterrupted, accurate, and secure data flow	• Empirical • Inductive-Consensual • Agreement • GDSS • Guaranteeing secure and correct human interaction with the data flow	• Ideal • Consensual-Conflict • Heuristic • DSS • Guaranteeing correct assumptions about the security of the data flow	• Dialectic • Conflictual-Synthetic • Conflict • IS • Guaranteeing a correct selection of alternatives for the security of the data flow	• Pragmatic • Synthetic-Complex • Adaptive • ESS • Guaranteeing varying tools and applications to manage and secure data flows

Summary

Advances in technology have led to globalization which has made the world flat. In a flat world territorial lines of economic and cultural ownership have become difficult to discern. Consequently, organizations must find various and new methods to become flexible with a focus on the human aspects of the organization, and integration of secure technologies must be addressed within the business arena in order to provide more secure systems. Looking forward, it will be critical for corporations to address the human factor of operations if they wish to remain competitive in a global market. This study suggest that the answer is found in coalescing research from various academic disciples; and it is intended to facilitate a focus on human capital and the human cognitive process. The proposed comparison of formal systems demonstrates how human cognitive processes relate directly to obtaining and retaining essential knowledge and experience within the knowledge management and information inquiry process. And this in turn reinforces

security decisions. Results reveals a series of assumptions about the characteristics of secure systems theories and the fit for business needs and the needs of the end user. By focusing the system design principles more on the end user, it will make future systems more efficient and secure. Specifically, past ISS design theories did not place sufficient emphasis on the styles of thinking of the end user of the system. This research begins at least initially this to better understand the needs of the design principles for developing secure systems.

References

Baskerville, R. (1993). Information systems security design methods: Implications for information systems development. *ACM Computing Surveys*, *25*(4), 375–414.

Bruvold, W. H., Parlette, N., Bramson, R. M., & Bramson, S. J. (1983). An investigation of the item characteristics, reliability, and validity of the inquiry mode questionnaire. *Educational and Psychological Measurement*, *43*(2), 483-493.

Churchman, C. W. (1971). *The design of inquiring systems: Basic concepts of systems and organization*. New York: Basic Books.

Courtney, J. F., Croasdell, D. T., & Paradice, D. B. (1998). Inquiring organizations. *Australian Journal of Information Systems*, *6*(1), 3-15.

Davis, C. J., Fuller, R. M., Tremblay, M. C., & Berndt, D. J. (2006). Communication challenges in requirements elicitation and the use of the repertory grid technique. *The Journal of Computer Information Systems*, *46*(5), 78-86.

Dhillon, G. (2001). Violation of safeguards by trusted personnel and understanding related information security concerns. *Computers & Security*, *20*(2), 165-172.

Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. *Information Systems Journal*, *16*(3), 293-314.

Eriksson, D. M. (2003). Identification of normative sources for systems thinking: An inquiry into religious ground-motives for systems thinking paradigms. *Systems Research and Behavioral Science*, *20*(6), 475-487.

French, S. (2007). Web-enabled strategic GDSS, e-democracy and Arrow's theorem: A Bayesian perspective. *Decision Support Systems*, *43*(4), 1476-1484.

Hammond, J. S., Keeney, R. L., & Raiffa, H. (1999). Management in action: The hidden traps in decision making. *Clinical Laboratory Management Review*, *13*(1), 39-47.

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154-165.

McIntyre, J. J. (2003). Participatory democracy: Drawing on C. West Churchman's thinking when making public policy. *Systems Research and Behavioral Science*, *20*(6), 489-498.

Mitroff, I. (1974). *The subjective side of science*. New York: Elsevier.

Richardson, S. M., Courtney, J. F., & Paradice, D. B. (2001). An assessment of the Singerian inquiring organizational model: Cases from academia and the utility industry. *Information Systems Frontiers*, *3*(1), 49-62.

Senge, P. M. (1993). *The fifth discipline: The art and practice of the learning organization*. New York: Doubleday.

Siponen, M., & Iivari, J. (2006). Six design theories for IS security policies and guidelines. *Journal of the Association for Information System*, *7*(7), 445-472.

Straub, D., & Collins, R. W. (1990). Key information issues facing managers: Software piracy, proprietary databases, and individual rights to privacy. *MIS Quarterly*, *14*(2), 143-156.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly*, *22*(4), 441-469.

Sun, L., Srivastava, R. P., & Mock, T. J. (2006). An information systems security risk assessment model under the Dempster-Shafer theory of belief functions. *Journal of Management Information Systems*, *22*(4), 109-142.

Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security*, *23*(3), 191-198.

Yolles, M., Iles, P., & Guo, K. (2006). Culture and transformational change with China's accession to the WTO: The challenge for action research. *Journal of Technology Management in China*, *1*(2), 147-158.

Zajac, E. J., Kraatz, M. S., & Bresser, R. K. F. (2000). Modeling the dynamics of strategic fit: A normative approach to strategic change. *Strategic Management Journal*, *21*(4), 429-453.

Biographies

Bennet Hammer is a student at Nova Southeastern University pursuing his PhD in Information Systems with a concentration in Information Security. Bennet completed his Master of Business Administration with a concentration in Information Systems at Florida Gulf Coast University. He currently holds undergraduate degrees in Management and Computer Information Systems, through Florida Gulf Coast University. Bennet is originally from Berlin, Germany and currently resides in Fort Myers, Florida.

Roy A. Boggs is Professor of Information Systems at Florida Gulf Coast University,. His interest in using information technology for teaching and scholarship began in the mid 1960s. His dissertation was one of the first to use this technology as a resource tool; and his subsequent activities have included both Arts & Sciences and Business applications. He has been a Fulbright and twice an Alexander von Humboldt scholar as well as a systems analyst and project manager for a large international bank.