Proceedings of the 14th Colloquium for Information Systems Security Education
Baltimore Marriott Inner Harbor
Baltimore, Maryland June 7 - 9, 2010

A Systematic Approach to Information Systems Security Education

Joseph J Simpson, *System Concepts*, and Dr Barbara Endicott-Popovsky, *University of Washington*

Abstract – A new systematic approach to information systems security education is proposed that includes the concepts of target, system and threat. These concepts cover the complete security context, and allow the Asset Protection Model (APM) the ability to define information systems security in a specific context. The APM is based on existing, well-established information assurance models. The APM provides cognitive support as well as a static and dynamic view of the model information.

Index terms – information systems security, security, security education, systems engineering

I. Introduction

The increasing value associated with high-quality information is driving the push toward the collection, processing, storage and distribution of vast amounts of information. The need to understand the specific characteristics and attributes of information that will maintain and/or increase the value of any given information set further focuses attention on the character, context and use of specific data sets. In this paper, system science and engineering techniques are used to expand and modify a classical information security model in a manner that allows a larger security operational context to be evaluated, considered and modeled. Human cognitive limitations associated with short-term memory and information processing are used as design constraints in the expanded model. The standardization of this expanded security context will provide a basis for the controlled, detailed exploration, analysis and discussion of the information systems security area. This type of stable model standardization will support information systems security education by establishing a consistent, logical basis around which the instructional material may be organized. Security education will be further benefited by the expanded models design which is tailored to support individual cognitive limitations.

II. Comprehensive Model of Information Systems Security

Hardware, software, protocols and operational techniques associated with the process of managing information change at a very high rate. A stable information security model must be based on environmental, organizational, system and information aspects that remain relatively constant over extended periods of time. The last two decades of tumultuous change and growth in the information processing and management area has shown that the Comprehensive Model of Information Systems Security (CMISS) presented in 1991 by McCumber has the basic model components and characteristics that allow this model to remain useful over this extended period of time [1]. The key aspects of the CMISS that provide the foundation of this continual period of application and usefulness are its focus on information along with a model structure that allows human beings the ability to organize and reason about information at the proper level of abstraction.

With a focus on characteristics of information that are independent of implementation technology and organizational structure, the CMISS distills the essence of information security practices in a manner that is useable by security planners and managers. By arranging primary concepts in groups of threes and constraining model relationship views to nine or less items, the CMISS also addresses critical cognitive complexity issues associated with the application of these types of models. The application of these cognitive complexity reduction techniques has been reviewed, analyzed and evaluated to produce an expanded model of the general security domain.

The stable form presented by the CMISS is of great benefit to seasoned information assurance professionals that have an extensive background and expert understanding of the information assurance domain, and the specific security application context. The CMISS is less useful to students of information assurance and system security due to the weakly defined and inferred

Joseph J. Simpson, Principal, Systems Concepts; MS in Systems Engineering, Missouri University of Science and Technology; MS in Environmental Systems Engineering, University of Washington.
Barbara Endicott-Popovsky, Ph.D., Director for the Center of Information Assurance and Cybersecurity and Research Associate Professor, Information School, University of Washington.

system security application context [2]. Further, the changes in the information assurance arena have generated a modified model that incorporates the concepts of authentication, non-repudiation and time into the base CMISS [3]. The need for a more comprehensive security model is clear. The authors believe that this model must cover the complete security context by explicitly recognizing that a complete security context contains a target and a system as well as a threat. The rest of this paper presents details for a comprehensive model of information systems security.

III. The Asset Protection Model

The expanded view for a system security domain space includes the concepts of system, information (target) and threat. The expanded model has been developed based on analysis of the cognitive complexity reduction aspects of the CMISS, the limitations of human cognitive ability, and general characteristics of the security domain. Metrics associated with the limitations of human cognitive ability were developed by Miller and expressed as "seven plus or minus two." This means that a person can keep between five and nine distinct ideas in their short-term memory for evaluation and analysis [4]. When a person exercises design judgment and synthesizes domain specific information, only three distinct elements can be processed because there are eight elements in the lattice of three items. Figure 1 shows this eight element lattice that was adapted from Warfield [5].

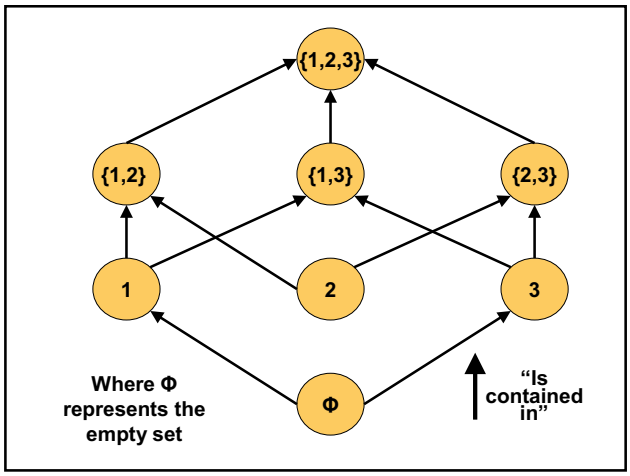

Fig. 1. The Lattice of Subsets of a Three-Element Set

The expanded model, named the Asset Protection Model (APM), is presented as a hierarchy of three dimensional cubes. Using a three dimensional cube to focus on and organize a specific area of the security problem establishes a structured framework required to support clear human reasoning and communication. The asset cube has three dimensions: the system, the threat and the target. At the next lower level of abstraction, each of these dimensions is transformed into its own unique cube. The system dimension becomes an individual system cube with three dimensions: system type, system specification and system program. The threat dimension becomes an individual threat cube with three dimensions: threat exposure, threat action and threat effect. The target dimension becomes an individual target cube with three dimensions: target configuration, target value, and target protection [6]. The APM graphical model and its levels of abstraction are shown in Figure 2. A primary benefit of the APM is the creation of a complete security model that is designed to be effectively evaluated by human experts at a high level of abstraction. At lower levels of abstraction, computer programs are used to automate the evaluation of the more detailed model relationships and interactions. The model is designed to allow a human being the ability to reason about a security problem and/or an asset protection problem without overloading the human cognitive capability limit. Computer assistance may be used to assist in the problem space analysis and communication when a large number of problem space characteristics must be systematically considered and evaluated.

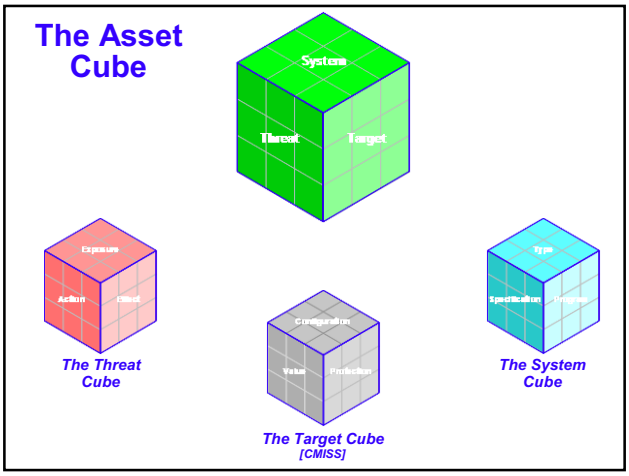

Fig. 2. The Asset Protection Model Cube Hierarchy

The three dimensions of the asset cube cover the complete scope of the asset protection security model. All aspects of a security domain problem can be addressed using one, or a combination, of these three dimensions. As a tool for information systems security education, this bounded model provides a stable model framework upon which specific instances of information system security problems can be arranged and mapped. The creation of a stable, common framework supports and enhances the ability of security educators to clearly communicate typical security problems, typical security solutions, and system security patterns. The design goal of the APM is to establish a stable, useful model that will stand the test of time, like the CMISS.

A. The System Cube

The system cube design is based on foundational components and concepts from the practice of systems engineering. Systems engineering is an organizational and project neutral type of technology management approach used to guide the design, development, deployment and operation of large-scale systems. The selected system engineering concepts are organizationally and technically independent, and have stood the test of time and application over the last few decades. These selected system concepts are: system type, system specification and system program [7].

The system type concept is further decomposed into the product system, the process system and the environment system. These system types are organized around the production and use of a technical or a socio-technical system. The product system is the system being designed, built and operated. The production system is the system that produces the product system. The environment system is the system that contains the product system, the production system, the product system customer as well as everything else. In general every type of system should fit into one of these three categories.

The system specification concept is further decomposed into system function, system requirements and system architecture. The system specification components are designed to address the function of the system, how well the system functions must be performed (system requirements) and the artifacts that perform the system functions (system architecture). All essential components of a system specification are covered using these three system specification concepts.

The system program concept is further decomposed into system cost, schedule and technical components. The system cost component is used to track the projected or budgeted system cost. The system schedule component is used to track and report the system attributes and characteristics that are time dependent. These are standard project management and control techniques that are independent of technology and organizational structure.

B. The Target Cube

The target cube is based on fundamental factors from the CMISS as well as basic aspects of a target-threat framework that was developed to address a wide range of target types and potential threat vectors [8]. The resulting target characteristics are independent of organization, technology and threat type. For the information security domain, the target is information. The target's fundamental characteristics are information configuration, information value and information protection. The information configuration characteristic is decomposed into information transmission, storage and processing. Information value is divided into information confidentiality, integrity, and availability. Information protection is divided into technology, policy, and human factors. This provides a robust set of target characteristics that have been used effectively for about 20 years.

C. The Threat Cube

The threat cube construct is also based on the Simpson target-threat framework developed to address a wide range of potential threat types, vectors and effects from a large domain of potential sources [8]. The selected threat characteristics are threat exposure, threat action and threat effect. The threat exposure is decomposed into threat actor, threat mechanism and threat vector. The threat action is divided into pre-event, event and post-event. The threat effects are decomposed into immediate effect, near-term effect, and long-term effect. This comprehensive set of threat characteristics are organization and technology independent, and provide the required stable conceptual foundation to maintain this model applicability as technology, organizations and threat techniques change over a period of time.

D. The Asset Cube Design and Structure

The APM structure is designed to allow human subject matter experts to effectively orient themselves and identify specific focus areas in the general model. Cognitive complexity is addressed by limiting the number of items and/or relationships that are addressed at any one time to three. Further, the three focus areas of the APM are designed to provide focal points for various types of security and organizational experts. At the highest level of abstraction the APM is represented as an asset cube with three primary categories (system, target and threat) listed on each axis of the cube. The asset cube then provides a collection of 27 sub-cubes that address the intersection of each of these high-level concepts (see Table 1). This provides a structured framework to support the description, discussion, organization and documentation of information security educational concepts and technical content, as well as educational process goals and objectives.

Table 1. The Twenty-Seven (27) Sub-Cube Structure

X Axis	Y Axis	Z Axis
System Type	Threat Exposure	Target Configuration
System Type	Threat Exposure	Target Value
System Type	Threat Exposure	Target Protection
System Type	Threat Action	Target Configuration
System Type	Threat Action	Target Value
System Type	Threat Action	Target Protection
System Type	Threat Effect	Target Configuration

X Axis	Y Axis	Z Axis
System Type	Threat Effect	Target Value
System Type	Threat Effect	Target Protection
System Spec.	Threat Exposure	Target Configuration
System Spec.	Threat Exposure	Target Value
System Spec.	Threat Exposure	Target Protection
System Spec.	Threat Action	Target Configuration
System Spec.	Threat Action	Target Value
System Spec.	Threat Action	Target Protection
System Spec.	Threat Effect	Target Configuration
System Spec.	Threat Effect	Target Value
System Spec.	Threat Effect	Target Protection
System Program	Threat Exposure	Target Configuration
System Program	Threat Exposure	Target Value
System Program	Threat Exposure	Target Protection
System Program	Threat Action	Target Configuration
System Program	Threat Action	Target Value
System Program	Threat Action	Target Protection
System Program	Threat Effect	Target Configuration
System Program	Threat Effect	Target Value
System Program	Threat Effect	Target Protection

At the next lower level of abstraction there are three cubes that represent the three axes of the asset cube. Each specific cube domain supports the associated subject matter experts; however, at this next lower level of abstraction, there are 19,683 individual points of conceptual intersection which generate a level of cognitive complexity that is beyond the ability of human subject matter experts to clearly comprehend and understand without the aid of an automated information system.

IV. The Information System Security Framework

The APM was designed to support information systems security education by providing a general framework for structuring the activities, processes and data associated with information systems security and information systems security education. A key aspect of this model is the balancing of human cognitive capabilities, and the natural complexity associated with the dynamic world of information systems security and security education. Security education that includes topics of digital forensics, network forensic readiness and forensic investigations will benefit greatly from the APM structure and approach [9].

In addition to balancing a range of human subject matter experts, the APM also provides the opportunity for various organizational types to participate in the development and maintenance of the APM data. The rapid rate at which threats to, and attacks on, information systems morph, develop, and change presents an especially difficult and challenging situation for information systems security education. The APM addresses some of these challenges by allowing the development and maintenance of a distributed model that can naturally handle increasing levels of information, detail and abstraction. Using this approach, sensitive information can be restricted in a natural manner.

A. The System Framework

The system component of the APM is designed to fit naturally into standard project and program management techniques that are ubiquitous throughout technical and management educational curriculum. Further, aspects of traditional systems engineering have been added to complete content and activity process interfaces to existing areas of instruction and expertise.

Key structure and content must be added to the system framework to support information systems security education. This content supports the unique view and values associated with the security profession and professionals. In many cases, these values and views may be shared and/or supported by other subject matter experts. The comprehensive form of the system framework provides a detailed structure to capture, review, and evaluate these shared values and views. The framework can be used to support the design of new systems as well as the operation of existing and/or upgraded systems. The tasks of forming the natural security concept clusters, associated subject matter interfaces and operational security practice clusters are all activities that are organized and guided by the form of the system cube. All security, project and operational aspects must be included in a comprehensive information systems security education program.

B. The Target Framework

The target framework is patterned after the CMISS which is further documented and detailed in a series of books and publications. The added value from the APM is the specific requirement for the explicit consideration of the system domain and the threat domain. While this new level of detail adds sufficient complexity that an automated system is required to effectively use the framework, this added complexity is deemed a small price to pay for a complete, general model.

C. The Threat Framework

The threat framework is designed to support the identification, classification and documentation of specific types of threats. Organized in a functional manner, the threat framework focuses the information set on an operational group of factors that naturally identify specific points of threat action and counteraction. By focusing on the threat exposure, action and effect, the framework highlights common points of security action

and threat counteraction given any specific threat context. The contents of the Threat Cube are shown in Table 2.

Table 2. Threat Cube Content

X Axis	Y Axis	Z Axis
Threat Actor	Pre-Event	Immediate Effect
Threat Actor	Pre-Event	Near-Term Effect
Threat Actor	Pre-Event	Long-Term Effect
Threat Actor	Event	Immediate Effect
Threat Actor	Event	Near-Term Effect
Threat Actor	Event	Long-Term Effect
Threat Actor	Post-Event	Immediate Effect
Threat Actor	Post-Event	Near-Term Effect
Threat Actor	Post-Event	Long-Term Effect
Threat Mechanism	Pre-Event	Immediate Effect
Threat Mechanism	Pre-Event	Near-Term Effect
Threat Mechanism	Pre-Event	Long-Term Effect
Threat Mechanism	Event	Immediate Effect
Threat Mechanism	Event	Near-Term Effect
Threat Mechanism	Event	Long-Term Effect
Threat Mechanism	Post-Event	Immediate Effect
Threat Mechanism	Post-Event	Near-Term Effect
Threat Mechanism	Post-Event	Long-Term Effect
Threat Vector	Pre-Event	Immediate Effect
Threat Vector	Pre-Event	Near-Term Effect
Threat Vector	Pre-Event	Long-Term Effect
Threat Vector	Event	Immediate Effect
Threat Vector	Event	Near-Term Effect
Threat Vector	Event	Long-Term Effect
Threat Vector	Post-Event	Immediate Effect
Threat Vector	Post-Event	Near-Term Effect
Threat Vector	Post-Event	Long-Term Effect

The Threat Actor (TA) is the entity that is posing the threat. The Threat Mechanism (TM) is the process and/or components the TA uses to express the threat. The Threat Vector (TV) is the medium and/or system used by the TA to facilitate the delivery of the TM.

Specific cyber threats obtained from the 2009 Internet Crime Complaint Center (IC3) Report are used next to demonstrate the manner in which the Threat Cube is used to classify the listed cyber crimes. The report has 79 complaint categories organized as 27 primary complaint types. The top ten complaint types are: (1) Advance Fee Fraud, (2) Auction Fraud, (3) Credit Card Fraud, (4) Computer Damage, (5) FBI Scams, (6) Identify Theft, (7) Miscellaneous Fraud, (8) Non-Delivery of Merchandise (non-auction), (9) Overpayment Fraud, and (10) SPAM.

An example of a SPAM (mass delivered) is used to demonstrate the use of the Threat Cube. The first nine of the 27 listed rows in Table 2 are organized around the Threat Actor. In the case of SPAM that is being delivered and managed by a bot-net, there is a continuous stream of SPAM email. Pre-Event is defined as activities necessary to set up the bot-net. Event is defined as the delivery of specific SPAM messages. Post-Event is defined as activities that are necessary to maintain the bot-net and gain additional customers for the TA. The Immediate, Near-Term and Long-Term Effect for the TA are associated with building an effective SPAM operation and large customer base. The specific details associated with describing a SPAM threat are recorded and tracked using the Threat Cube content divisions as an organizing structure.

The Threat Mechanism section of the Threat Cube addresses the SPAM delivery mechanism. This includes the actions necessary to develop the bot-net (Pre-Event stage) as well as to maintain on-going access to networks, servers and other communication capabilities to deliver the SPAM messages. Once specific SPAM TM processes are identified they then are recorded and analyzed using the Threat Cube format and structure associated with the TM area.

The Threat Vector section of the Threat Cube addresses the systems, networks and organizations that facilitate and enable the delivery of SPAM. The Immediate, Near-Term and Long-Term Effects associated with the TV elements vary between and among the enabling elements. The structure of the Threat Cube is used to organize these effects and begin the categorization and threat analysis process.

As shown in the Threat Cube example, the APM is designed to address different levels of abstraction as well as to structure the information and data associated with different types of cyber crime, cyber security issues, and information assurance activities in a manner that enhances the communication of the material. The primary design goal of the APM is to reduce the cognitive complexity associated with understanding information systems security practice and application. The base framework presented in this paper must be reviewed, adjusted and assimilated by the cyber security community to achieve the model's full potential.

V. A Dynamic System Security Model

The APM provides a set of 19,683 relationships at the lower level of abstraction. This is essentially a large check list of possible relationships that may or may not be valid for any given situation. The value in this large static check list of information system security concepts is the ability to determine if a specific security relationship is valid for the current situation; and if it is valid, to determine if the concept has been properly addressed. Further, this check list should cover, and therefore define, the complete domain of information systems security at this level of abstraction.

Many of the APM concepts have a dynamic nature and application. By adding the concepts of threat and system to the standard CMISS, the APM provides the basis for dynamic modeling of specific organizational security budget commitments, threat reduction techniques, and other security control processes. Once a specific organization's security posture has been evaluated and mapped, the dynamic properties and attributes associated with the organization's security can be effectively applied in a standard system dynamics modeling context to explore the outcomes and impacts associated with a given security course of action and/or organizational strategic security approach.

A number of system dynamic models that address the organizational domain of information security have been developed and applied to various aspects of the information system security problem. One system dynamic model highlights the "arms race" escalation cycle between the threat and the target [9]. In this model, the concept of the system that hosts the target information is distributed throughout the model. The APM structure that separates the system, target and threat provides a richer model and evaluation context.

A. Asset Protection Model Dynamic Components

Each of the three primary APM concepts can be arranged in a standard causal-loop diagram and/or a stock and flow diagram. These two basic diagram types have proven effective in the process of integrating and focusing the distributed knowledge contained in groups of subject matter experts. In addition, the stock and flow diagram organizes the security problem space in a manner that supports active discussion of system values, dependencies and cause-effect relationships. Figure 3 shows a causal-loop diagram based on Endicott-Popovsky's escalation cycle [9].

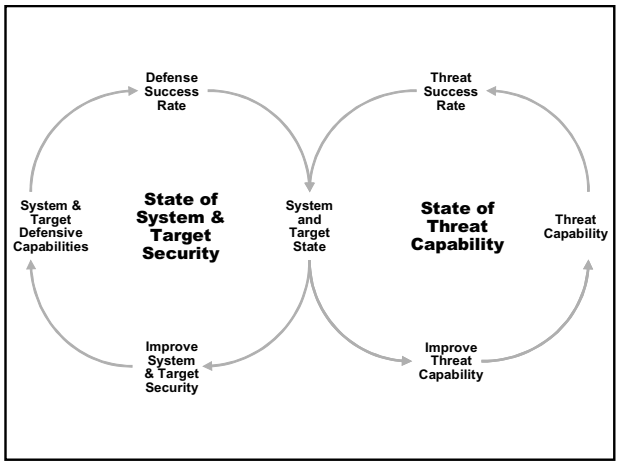

Fig. 3. Escalation Cycle in terms of System, Target and Threat

The system component of the APM is represented by the concept of system strength in a stock and flow diagram. The threat component of the APM model is represented by the concept of threat level. The target component of the APM is represented by the concept of target exposure. In general, these three concepts are linked in an array of interlaced causal-loop models. While the static APM data model provides an organization the ability to record specific data about security operations, the dynamic models provide the ability to structure cause-effect scenarios, and observe system behavior over a period of time. This dynamic modeling capability adds great value and insight to the process of delivering information systems security education and instruction.

When using stock and flow, the system strength component can be modeled as a stock that increases when the proper type of organizational resources and operational priorities are applied. The system strength will decrease if sufficient resources and priorities are not correctly applied. While this represents a very simple base level model, the proper allocation of resources is far from simple. In fact these base scenarios present a rich learning environment that addresses not only the proper technical and process response and action, but also includes relevant management actions and value set considerations. Relative ranking and normalization of these types of disparate factors will provide the types of education and training needed to prepare students for the preparation and defense of operational budgets and resource requests.

The threat level component can be modeled as a stock that increases and decreases as a given set of conditions change. The challenge here is to determine if the threat component needs to be decomposed into its three sub-components: exposure, action and effect. After the proper level of abstraction is determined, the factors that impact the threat levels must be identified, evaluated and combined into a set of increasing and decreasing functions. This activity represents a rich vein of educational opportunities that are linked directly to the understanding of information systems security, organizational management, and operational values.

The target exposure component can be modeled as a stock that increases and decreases based on a number of system environmental factors including the system strength and the current threat level. The APM relationships provide a candidate set of sub-components – configuration, value, and protection – that must be considered when evaluating the factors that cause target exposure to increase and decrease. Detailing a well-reasoned set of candidate factors, for any given information target, is the foundation upon which information security principles, practices and operations can be compared and evaluated. The dynamic nature of these system problems stresses the need for

good judgment, sufficient experience and focused problem solving by the individuals that are selected to perform this type of analysis.

VI. Summary and Conclusions

The field of information systems security is in a formative stage that is proceeding with a high rate of change at organizational and technical levels. A fundamental security model is proposed in this paper that is independent of technology and organizational changes. Further, the APM builds upon the established base of the CMISS by explicitly adding the concepts of system and threat into the APM construct. In this manner the complete security context for any given situation can be effectively addressed.

The expanded context associated with the APM supports design, development and delivery of information systems security material and concepts that will stand the test of time by adapting technology and organizational changes to the constant concepts and characteristics detailed in the APM. The APM framework is designed to address the cognitive limitations of human analysts as well as support a static and dynamic, computerized information form and format. These basic tools provide both cognitive support and a structured domain information framework.

More research is needed to refine and validate the APM as well as begin the development of a set of security patterns and processes that can be applied in any given information system security context and/or security problem space.

VII. References

[1] McCumber, John, “Information Systems Security: A Comprehensive Model.” *Proceedings of the 14th National Computer Security Conference, National Institute of Standards and Technology (NIST)*, Baltimore, MD, October, 1991.

[2] Dark, Melissa Jane, Ekstrom, Joseph J., and Lunt, Barry M., “Integrating Information Assurance and Security into IT Education: A Look at the Model Curriculum and Emerging Practice.” *Journal of Information Technology Education*, Volume 5, pp. 389-403, 2006.

[3] Maconachy, W. Victor, Schou, Corey D., Ragsdale, Daniel, and Welch, Don, “A Model for Information Assurance: An Integrated Approach.” *Proceedings of the 2001 IEEE Workshop on Information Assurance and Security*, United States Military Academy, West Point, NY, 5-6 June, 2001.

[4] Miller, G. A., “The Magical Number Seven, Plus or Minus Two: Some Limitations on Our Capacity for Processing Information.” *Psychology Review* 63(2), 81-97, 1956.

[5] Warfield, John N., *A Science of Generic Design, Managing Complexity Through System Design, Second Edition*, Iowa State University Press, Ames, Iowa, 1994.

[6] Simpson, Joseph J. and Simpson, Mary J., "Complexity Reduction: A Pragmatic Approach." Submitted for publication to *Systems Engineering Journal*, Chicago, Illinois, February, 2010.

[7] Mar, Brian W., "Back to Basics." *Proceedings, Second Annual International Symposium of National Council on Systems Engineering (NCOSE), "Systems Engineering for the 21st Century,"* pp 37-43, Seattle, WA, July, 1992.

[8] Simpson, Mary J., “Conceptual Framework and Levels of Abstraction for a Complex Large-Scale System. *Proceedings, Third Annual Conference on Systems Engineering Research*, Hoboken, New Jersey, March, 2005.

[9] Endicott-Popovsky, B., Frinke, Deborah A., and Taylor, Carol A., “A Theoretical Framework for Organizational Network Forensic Readiness.” *Journal of Computers*, Vol. 2, No 3, May 2007.