Journal of International Technology and Information Management

Volume 16 | Issue 2 Article 2

2007

The Role of Quantitative Analysis in the Information Security Systems Development Lifecycle

Stephen R. Rosenkranz
Scott & Stringfellow, Inc.

Michael E. Busing
North Carolina A&T State University

Faye P. Teer
North Carolina A&T State University

Karen A. Forcht
North Carolina A&T State University

The Role of Quantitative Analysis in the Information Security Systems Development Lifecycle

Stephen R. Rosenkranz
Scott & Stringfellow, Inc.

Michael E. Busing
Faye P. Teer
Karen A. Forcht
North Carolina A&T State University

ABSTRACT

Today's numerous Quantitative Analysis (QA) tools have been successfully utilized to solve business problems in diverse applications. However, the application of QA tools in solving information security problems has been sparse. Devising the means and ways to use QA tools in resolving industry-wide security problems has the potential to yield enormous global economic benefit.

The purpose of this paper is to explore the use of QA tools as a means of improving the processes involved in the Information Security Systems Development Lifecycle (SecSDL). Information security professionals use the SecSDL as a guide for formulating a comprehensive information security program. The paper examines the fit between QA tools and the processes of the SecSDL. A case application illustrates an example of QA tools applied specifically to risk assessment in the SecSDL.

INTRODUCTION

Modern usage quantitative analysis (QA) tools, developed during and refined since World War II, provide objective solutions to today's business problems. These tools include such methods as linear programming, queuing analysis, simulation, PERT/CPM, and decision theory. QA tools have been successfully utilized to solve complex problems in many diverse areas and applications. However, the use of QA tools in solving information security problems has been sparse. Devising the means and ways to include use of QA tools in resolving industry-wide security problems has the potential to yield enormous global economic benefit. The purpose of this paper is to explore the use of QA tools as a means of improving the processes involved in one information security application—the information security systems development lifecycle (SecSDL). This paper discusses the importance of using QA tools in solving information security problems and presents a framework of today's information security environment. The paper examines the fit between QA tools and SecSDL processes, illustrating specific QA tools for use in the SecSDL. The paper ends with a case application in which QA tools are applied to risk assessment in the SecSDL.

EMPLOYING THE USE OF QA TOOLS IN SOLVING INFORMATION SECURITY PROBLEMS

With 137,529 reported security incidents during 2003 (CERT/CC Statistics, 2005), effective information security has become a necessity, rather than an after-thought. Failure to take the necessary steps to secure vital business operations from both intentional and unintentional harm will result in catastrophe for the errant organization (Forcht and Kruck, 2001). QA tools have the potential to become an integral part of solving these information security problems. Failure to use this valuable tool quite literally puts the whole organization at risk. "A manager who is knowledgeable in quantitative decision-making procedures is in a much better position to compare and evaluate qualitative and quantitative sources or recommendations and ultimately to combine the two sources in order to make the best possible decision" (Anderson, et al., 2005). Additionally, top management support has been shown to affect

success of such decision making (Jitpaiboon and Kalaian, 2005). Adequately employing QA tools does not release an organization from risk. Proper implementation, however, should minimize or greatly reduce risk.

Some barriers to implementing QA tools to solving information security problems are:

- the variety and complexity of existing and evolving threats;
- the complexity of existing information and communications systems;
- rapid advances in technology, which could render existing security solutions moot;
- difficulty in determining industry-wide security trends to develop security solutions;
- difficulty in monetarily quantifying the impact threats have on business operations;
- difficulty in formulating problems into mathematical models;
- historic reliance on qualitative and subjective assessments to solve security problems.

Overcoming these barriers is a daunting proposition even for a seasoned information security professional. The effort must be made, however, if the information security community is to take permanent steps towards developing industry-wide solutions to common security problems. Management and security professionals neglecting to employ these trusted and time-tested methods are vulnerable to implementing a less-than-optimal solution, and may unwittingly adopt an unacceptable level of residual risk.

TODAY'S INFORMATION SECURITY ENVIRONMENT

Modern information security began in the early part of the 20th century, evolving from computer security. At its inception, computer security consisted of securing the physical site where the computer was located and controlling access using badges, keys, and facial recognition of authorized users (Whitman and Mattord, 2003). While these computer security techniques are still employed today, increased sophistication of computers, storage devices, and communications technologies served as a forcing mechanism for information security to become a discipline and profession in its own right. In that vein, Bidgoli (2003) illustrates common security threats to the private sector's e-commerce activities and proposes a six-step comprehensive model designed to help reduce this risk.

Recent legislation grants force of law to certain industry-specific information security requirements. Some examples of recent information security legislation include:

- Health Insurance Portability and Accountability Act (HIPAA) 1996. "...addresses the security and privacy of health data." (Centers for Medicare and Medicare and Medicaid Services, 2002)

- Gramm-Leach-Bliley Act (GLBA) 1999. Its primary purpose is to ensure privacy of customer information through requiring comprehensive data protection measures by financial service organizations (Progressive Technologies Group, 2003).

- Federal Information Security Management Act (FISMA) 2002. "This act requires the chief information officer (CIO) of each federal agency to develop and maintain an agency-wide information security program." (Harold, 2003). Each agency must report annually on compliance with published requirements.

In today's increasingly regulated and complex information security environment, CIOs must continually make certain that their organizations are aware of and in compliance with federal laws and regulations that impact information security. This paper stresses the importance of compliance and provides insight on tools that can reduce risk of non-compliance.

RELATED LITERATURE PERTAINING TO QA TOOLS AND THE INFORMATION SECURITY SYSTEMS DEVELOPMENT LIFECYCLE

A few studies relating to the application of traditional QA tools to the information security systems development lifecycle (SecSLC) were found in the related literature. What follows is a brief chronology of the more significant advances in the art of applying QA tools to SecSLC (Butler, 2003):

- 1990. Thomas Lane developed a framework for classifying user interface design knowledge so software designers could make good structural choices based on the user's functional requirements.

- 1996. Jyrki Kontio first proposed using a well-known decision analysis technique called Analytic Hierarchy Process to help software engineers make systematic decisions about selecting commercial-off-the-shelf (COTS) products.

- 1998.
  - Thomas Finne suggested formal decision-making techniques should be applied to making decisions about information security. However, he did so without specifying a framework for using those techniques in selecting risk-mitigation controls.

  - D.W. Straub and R.J. Welke developed a countermeasure matrix which compares two security risk-mitigation controls by highlighting their strengths and weaknesses relative to deterrence, prevention, detection, and available remedies. This matrix is largely qualitative in nature.

- 2000. Rick Kazman, et al. used multi-attribute analysis techniques to estimate the costs and benefits of software architectural attributes, such as performance, security, and modifiability, thereby permitting software engineers to make informed decisions regarding tradeoffs among information system architectural design decisions.

- 2003. Shawn Butler devised the Security Attribute Evaluation Method (SAEM), using multi-attribute analysis techniques, to support security managers in making cost-effective design decisions about security architectures.

Information security professionals should have a goal of selecting a QA tool sophisticated enough to permit them to more effectively decide between available security solution alternatives, while simultaneously demonstrating the cost-benefit of their choices. Another goal is to provide a tool that is functional without overwhelming the user with its complexity.

AN EXAMINATION OF THE FIT BETWEEN QA TOOLS AND SecSLC PROCESSES

The SecSDL is a natural extension of the traditional, broader information systems development lifecycle (SDL). The information systems development process is the collection of methods and automated tools used to define organizational problems and develop information systems to address those problems (Whitten and Bentley, 2007). The six phases in the SecSDL are summarized in Table 1.

Table 1: SecSDL Summary (Whitman and Mattord, 2003).

Phase Number	Phase	Summary
1	Investigation	• Management defines project processes and **goals** and documents these in the program security policy. • Management dictates the SecSDL budget and other **constraints**.

2	Analysis	• Analyze existing security policies and programs. • Analyze current **threats** and **controls**. • Examine legal issues. • Perform risk analysis.
3	Logical Design	• Develop security blueprint. • Plan incident response actions. • Plan business response to disaster. o Continuity planning. o Disaster recovery. • Determine feasibility of continuing and/or outsourcing the project.
4	Physical Design	• Select technologies needed to support security blueprint. • Develop definition of successful solution. • Design physical security measures to support technological solutions. • Review and approve project.
5	Implementation	• Buy or develop security solutions. • At end of phase, present tested packed to management for approval.
6	Maintenance	• Constantly monitor, test, modify, update, and repair to meet changing threats.

Numerous parallels present themselves when comparing the SecSDL process with the QA tools. Similarities exist because both methodologies exist to perform the same primary functions: facilitating decision making by determining feasible alternatives for solving a specific problem, recommending an optimal solution, and affording organizational leadership the luxury of having a choice between proposed alternatives. Anand and Chung (2005) utilize statistical process control techniques for determining whether or not support incidents are in control. Out of control incidents should be investigated to determine root cause. Table 2 compares the two processes, focusing on where QA tools overlap with the SecSDL to illustrate how the SecSDL mirrors the QA process.

Table 2: Comparing the SecSDL and Quantitative Analytical Processes.

Phase	SecSDL/ QA*	Applicable QA Method(s)	Step
1	SecSDL	Linear Programming (LP), PERT/CPM	Management defines project processes and goals.
	QA		Management defines objectives.
1	SecSDL	LP, PERT/CPM	Management dictates budget and other constraints.
	QA		Management dictates budget and other constraints.
2	SecSDL	Queuing Analysis (QuA)	Analyze current threats and controls.
	QA		Analyze arrivals and services.
2	SecSDL	LP, QuA, Simulation (Sim), Decision Tree (DT)	Perform risk analysis.
	QA		Conduct data preparation.
3	SecSDL	LP, QuA, DT	Develop security blueprint.

	QA		Formulate mathematical problem.
3	SecSDL	LP, DT	Determine feasibility of continuing and/or outsourcing the project.
	QA		Determine if possible solutions are feasible, given available resources and specified constraints.
4	SecSDL	LP	Select technologies needed to support security blueprint.
4 (cont.)	QA		Delineate feasible solutions, determine which solution is optimal, and, if there is more than one optimal solution, select which optimal solution to implement.
6	SecSDL	The models for the QA methods chosen.	Constantly monitor, test, modify, update, and repair to meet changing threats.
	QA		During and after implementation, continue to monitor the model's contribution. Expand or refine as necessary.[1]

*(QA - Quantitative Analysis)

SPECIFIC QA TOOLS FOR USE IN THE SecSDL

The information security professional can often formulate security problems in terms that can then be examined by QA tools. While this intellectual exercise can be daunting, the potential benefits for performing the task far outweigh the effort. Once a problem is properly specified, it has the potential to save time and effort in the future when the organization revisits the problem. When revisiting the problem, the information security professional can make needed modifications to ensure the formulation is relevant. Depending upon how much the current situation and circumstances have changed, however, it may be necessary to scrap the existing problem specification and start from scratch. The following is a brief overview and discussion of several QA tools used in business today and the suggested relevance of each to the SecSDL.

Linear Programming

Of all the QA tools, linear programming holds the most promise for identifying optimal security solutions. Linear programming is a valuable tool for the information security profession when examining possible controls to mitigate risk, while simultaneously operating within narrowly defined, management-directed constraints. The added benefit is linear programming can assist in identifying binding constraints which preclude finding a more optimal solution. Identifying these "roadblocks" provides the information security professional with an argument to either remove or relax constraints. A less-than-optimal solution in information security often equates to accepting residual risk. Convincing management to relax constraints often necessitates demonstrating a sufficient return on investment for the proposed control.

Queuing Theory

Information security requires a layered approach. Up to a certain point, the greater the number of protective layers between a threat and the protected information, the better. However, there is a point of diminishing return at which adding more security can actually inhibit operations (see Figure 1). Relying on the reasonable comparison of a succession of attacks to a waiting line, an information security professional can use queuing analysis and waiting line models to ascertain the operating characteristics of their security system.

Using mathematical formulas and relationships, waiting line models provide a framework to assess whether or not security measures are adequate to deal with various threats by:

- analyzing the probabilities of different rates of a specific type of attack in a given period of time;
- assessing the probability individual security measures will provide their claimed level of protection in a given period of time;

- determining the average number of times a specific threat will manifest itself in a given time period;
- determining whether or not the frequency of a specific form of attack will overwhelm individual security measures;
- permitting management the luxury of comparing the probable effectiveness of different designs for security operations.

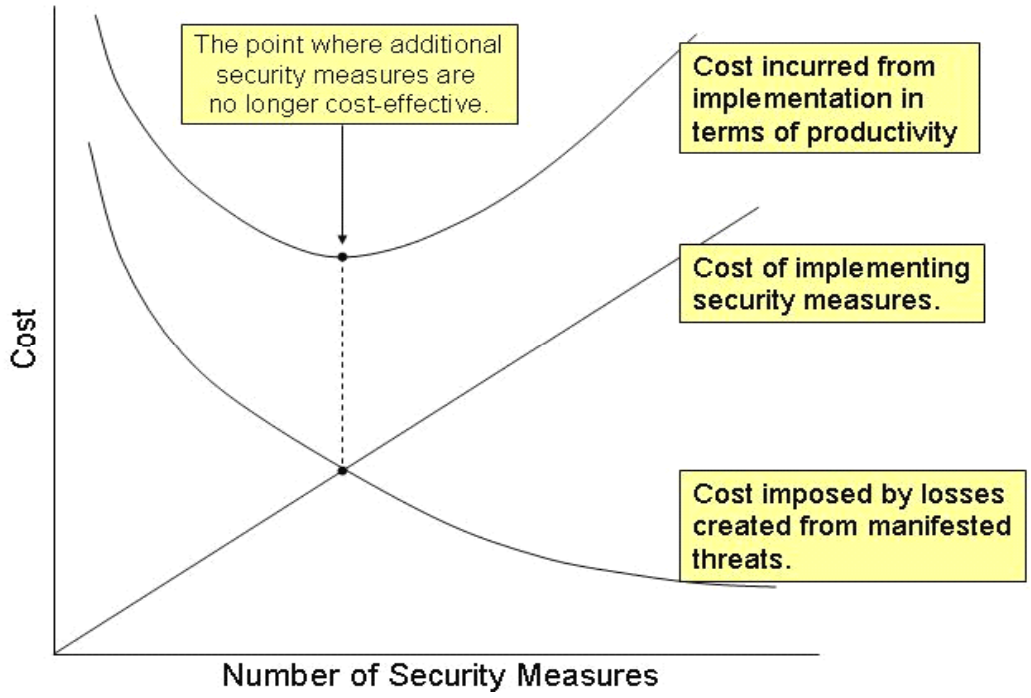

Figure 1: Cost of Implemented Security Measures.

Simulation

Simulation provides valuable feedback by predicting how a system will operate given certain controllable inputs and randomly generated probabilistic inputs. For the SecSDL, the controllable inputs are the types of security systems and other measures implemented to mitigate threats and their quantifiable attributes. The randomly generated, probabilistic inputs would be the number and types of attacks on the systems (see Figure 2).

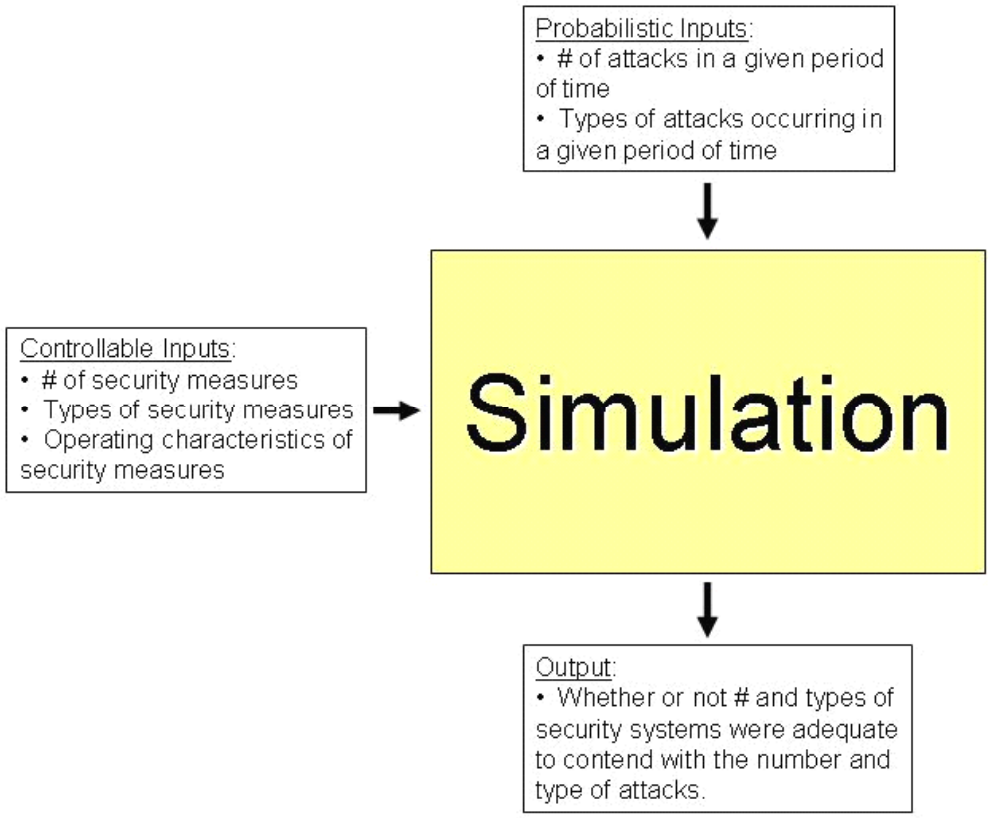

Figure 2: A Generic Diagram Demonstrating the Essential Components of an Information Security Simulation Model.

The output for this dynamic simulation model would, theoretically, demonstrate the likelihood that the current security system would be adequate for dealing with and mitigating different volumes and types of attacks.

An ancillary benefit of simulation modeling would be to generate different training scenarios involving different volume and types of attacks for incident response teams and business continuity planners. The model could also be modified to generate different possible attack outcomes to provide even more "realistic" scenario training.

PERT/CPM

Program Evaluation and Review Technique (PERT) and the Critical Path Method (CPM) are two additional QA tools that can be applied to managing the SecSDL. The PERT/CPM process provides a coherent framework for managing security architecture development and implementation.

PERT/CPM analysis provides project managers with a powerful tool for managing a number of complex, simultaneous tasks. PERT/CPM analysis can facilitate the imposing task of designing and implementing an enterprise-wide information security system.

Decision Trees

Decision analysis can help determine an optimal strategy when a decision maker is confronted with several decision alternatives (Anderson, et al., 2005). This is certainly the case during the SecSDL and, while not all SecSDL decisions require formal decision analysis, those that do are far from trivial and may have some of the following characteristics (Samson, 2003):

- They involve significant, long-lasting impacts.
- The decision maker has many alternatives to choose from.
- They affect other people as well as the decision maker.
- The consequences may be uncertain or risk-filled.
- They involve multiple dimensions of value.

As with any QA tool, decision trees have the potential to facilitate the SecSDL process. Decision trees facilitate decision making because they ("Decision Tree Analysis," 2003):

- clearly lay out the problem so that all options can be challenged;
- allow us to analyze fully the possible consequences of a decision;
- provide a framework to quantify the probabilities of given outcomes;
- help us to make the best decisions on the basis of existing information and best guesses.

CASE APPLICATION: QA TOOLS APPLIED TO SecSDL RISK ASSESSMENT

The SecSDL focuses on identifying and resolving security issues by:

- identifying critical business functions;
- identifying the key assets required to perform those critical business functions;
- identifying threats to those key assets;
- assessing the potential impact the identified threats could have on key assets;
- assessing the likelihood of the threats inflicting damage or degradation to key assets;
- identifying risk reduction and mitigation measures;
- assessing residual risk of identified threats once reduction measures are implemented.

As part of the SecSDL information security manager's analysis of key asset threats, each potential threat's impact on the three pillars of information security is examined closely. Once potential threats are delineated, QA tools can assist in assessing their likelihood of occurring and their probable effects. QA tools also have enormous potential to assist in selecting which controls to implement, how to implement the controls, and in performing an accurate assessment regarding the likely effect a specific control or set of controls will have.

There are three information security pillars: access, integrity, and availability. Each pillar is a critical aspect of information operations; organizational personnel must protect these pillars from internal and external threats. It is worth noting that these pillars are neither distinct nor discrete, such that a specific information security solution may benefit more than one pillar. These collateral benefits increase the cost-effectiveness of that particular information security solution. The following is a brief explanation of each pillar, coupled with a specific example of how QA methods could potentially help uncover an optimal solution to implement.

Access

Controlling access is the, "...[prevention of] disclosure or exposure to unauthorized individuals or systems. [Controlling access to] information is ensuring that only those with the rights and privileges to access a particular set of information are able to do so, and that those who are not authorized are prevented from obtaining access." (Whitman and Mattord, 2003)

A specific situation where using QA tools can help is in regulating access at controlled or restricted facilities. Since physically protecting information is critical, QA tools applied to the problem of controlling access to physical

facilities can be enormously beneficial. Table 3 identifies several problems or issues regarding facility access and proposes the QA tools that can best address them.

Table 3: Potential QA Applications for Resolving Access Issues at Government Agencies' Facilities.

Security Aspect	QA Method
The optimal numbers of both security personnel and controlled access points to accommodate the volume of people entering and leaving the facility.	Queuing Analysis
The number and types of additional security measures (other than security personnel), assuming the security utility for additional security measure can be quantified.	Linear Programming
How facility access security planning, resourcing, and implementation fit into the enterprise-wide security strategy.	Linear Programming, PERT/CPM, Decision Tree

Integrity

There are two primary considerations regarding information integrity:

1. Accuracy. Information is labeled accurately regardless of where it is stored, and information remains unaltered and untainted from capture to reporting.
2. Completeness. All necessary data elements, records, characters, and parameters and descriptors are evident and available.

Applying QA tools to solving the problem of maintaining information integrity primarily revolves around implementing access policies, procedures, and storage solutions to ensure captured information is not corrupted accidentally or intentionally. QA tools can assist in determining:

- Access Privileges. Establishing a system for differentiating information access privileges to restrict employee and customer access to information.

- Back-up Policies and Procedures.
  - Determining the frequency of information back-ups.
  - Selecting cost-effective media which provide the greatest chance of maintaining information integrity, given comparable attributes and specified constraints.
  - Deciding where to store and how long to keep archived information.

- Retrieval Process. Selecting and implementing a retrieval process which facilitates obtaining information while protecting it from unauthorized access or interference.

- Data Verification. There are many techniques and technologies available today to "guarantee" that the information sent was the information received; one example of such a technique is Public Key Infrastructure, or PKI ("Information Security," 2003). QA tools can help the information security professional determine which method, or combination of methods, best suits the organization.

Availability

Information availability refers to a situation where data and information are available and can be retrieved in usable form when needed and where needed by those who need it. This applies to both employees and customers for a given organization. Fortunately, many of the considerations, precautions, and solutions for access and integrity also help ensure information is available for those who need it.

The list in Table 4 addresses the primary problems and concerns inherent to availability, which would benefit from QA. Information availability can greatly enhance business operations. Likewise, the failure to make information available to authorized users can severely hamper business operations.

Table 4: Potential QA Applications for Resolving Availability Issues.

Problem/Concern	QA Method
Volume. The number of users requiring access to available information at varying times during the course of the day. This, in turn, drives the following decisions and resultant decision-making processes: • Automation/Equipment. Number and types of equipment required to support demand for availability. This includes how and where the information is stored. • Format. How to present the information, both conceptually and physically.	Linear Programming, Queuing Analysis
Classification of Information. If the requested information restricted or privileged, the following problems need to be addressed in order to make the information available without compromising confidentiality. • Verification. How to verify a user requesting the information has the appropriate access. • Automated vs. Analog. Advantages and disadvantages of making sensitive information available in an electronic format, and whether or not to maintain certain information in a hard-copy format for accountability purposes. • Storage. Where and how to store information to safeguard it, while simultaneously making it available to those who require it to function.	Linear Programming, Decision Tree
Categories of Information. Not pertaining to classification, categorically there are many different types of information. There in lies the issue of how best to organize and present the information so those needing it can access it quickly.	PERT/CPM, Decision Tree

CONCLUSION

This article examined the fit between QA tools and SecSDL processes, illustrated specific QA tools for use in the SecSDL, and presented a case application in which QA tools are applied to risk assessment in the SecSDL. In doing so the authors have illustrated the importance of using QA tools in solving information security problems.

The SecSDL provides guidelines for information security professionals to prioritize which assets to protect, what to protect them from, how to pick a "best" security solution, and what residual risk remains after implementation. QA tools should play a crucial role in the information security process. QA tools permit a security manager to better illustrate the reasoning behind specific security recommendations and the cost-benefit justification for allocating resources to support the recommended security plan.

Future research in the area of utilization of QA tools as part of information security management is needed. The authors believe that this field can benefit from empirical research that examines the extent to which information security managers in organizations are using QA tools to enhance the SecSDL. As part of future research projects the authors also intend to perform empirical research that will provide an in-depth profile of how QA tools are being utilized in the SecSDL.

REFERENCES

Anand, B. and Chung, C.A. (2005). Statistical Process Control for the Engineering IT Support Incident Life Cycle. *Journal of International Technology and Information Management*, 14(2), 83-92.

Anderson, D. R., Sweeney, D. & Williams T. (2005). An Introduction to Management Science Quantitative Approaches to Decision Making (11th Ed.). Cincinnati, Ohio: South-Western College Publishing.

Bidgoli, H. (2003). An Integrated Model for Improving Security Management in the E-Commerce Environment. *Journal of International Technology and Information Management*, 12(2), 119-134.

Butler, S.A. (2003). Security Attribute Evaluation Method. (Working Paper, School of Computer Science, Carnegie Mellon University, Pittsburgh, PA).

Centers for Medicare and Medicaid Services (2002). Health Insurance Portability and Accountability Act of 1996 (HIPAA): HIPAA Administrative Simplification. (Online), December 10, 2003. http://www.cms.hhs.gov/hipaa/

CERT Coordination Center (CERT/CC) (n.d.). CERT/CC Statistics 1988-2005. (Online), April 18, 2006. http://www.cert.org/stats/cert_stats.html

Forcht, K.A. and Kruck, S.E. (2001). Physical Security Models, Philosophies, and Context. *Journal of International Information Management*, 10(2), 85-97.

GM Consultants (2003). Information security. (Online), December 16, 2003. http://www.gmtech.com/security.html

Harold, Jerry (2003, October). Washington Gets Tough. *SC Magazine*, 40.

Jitpaiboon, T. and Kalaian, S.A. (2005). Analyzing the Effect of Top Management Support on Information System (IS) Performance. *Journal of International Technology and Information Management*, 14(2), 131-144.

Mind Tools Ltd (n.d.). Decision Tree Analysis - Choosing Between Options by Projecting Likely Outcomes. (Online), December 14, 2003. http://www.mindtools.com/dectree.html

Progressive Technologies Group (n.d.). GLBA Compliance. (Online), December 16, 2003. http://www.ptgroup.com/finance.php

Samson, D. & Daft, R.L. (2003). Fundamentals of Management. Melbourne, Australia: Thomson Learning.

Whitman, M.E. and Mattord, H.J. (2003). Principles of Information Security. Boston, Massachusetts: Thomson Learning.

Whitten, J.L. and Bentley, L.D. (2007). Systems Analysis and Design Method, 7th Ed. New York: McGraw Hill.