Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2006 Proceedings

Americas Conference on Information Systems (AMCIS)

December 2006

A Process Approach to Information Security: Lessons from Quality Management

Ravi Behara
Florida Atlantic University

C. Derrick
Florida Atlantic University

Qing Hu
Florida Atlantic University

Follow this and additional works at: http://aisel.aisnet.org/amcis2006

Recommended Citation
Behara, Ravi; Derrick, C.; and Hu, Qing, "A Process Approach to Information Security: Lessons from Quality Management" (2006). *AMCIS 2006 Proceedings*. 169.
http://aisel.aisnet.org/amcis2006/169

This material is brought to you by the Americas Conference on Information Systems (AMCIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in AMCIS 2006 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

A Process Approach to Information Security: Lessons from Quality Management

Ravi S. Behara
Florida Atlantic University
rbehara@fau.edu

C. Derrick Huang
Florida Atlantic University
dhuang@fau.edu

Qing Hu
Florida Atlantic University
qhu@fau.edu

ABSTRACT
The prevalent approach to analysis of information security is typically event-centric and ad-hoc based primarily on risk management principles. However, we believe that scholars and practitioners in the information security field can benefit significantly from the experiences and principles of quality management, where process orientation dominates and continuous improvement is the essence. This paper reviews some key concepts in quality management and draws lessons for information security management. Based on this, a process-centric framework for managing information security is developed. The framework is then explored in the context of root-cause analysis of realized threats or security breaches. Future research directions are then suggested.

KEYWORDS
Information security, process approach, quality management, root-cause analysis.

INTRODUCTION
Security failures, epitomized by the 9/11 attacks, have produced dramatic events, and their outcomes often dominate the view of the observers. The technology, or the technical aspect, of information security events such a worldwide virus attack attracts the attention of users and management alike. As a result, quite often, the thinking and focus of information security are event-based, outcome-driven, and technology-centric. But vulnerabilities are intrinsic to all systems, and, as a result, security management deals with questions of "when" and "how much," not "if," as companies depend more and more on the use of information technology. With security concerns permeating all levels of information and systems management, the event-oriented view becomes insufficient for managing information security. Early markers of this shift in thinking in information security management can be seen in some changing beliefs (Berinato et al., 2004):

Exploiting fear, uncertainty, doubt to get attention and budgets to security concerns is *out* and metrics and returns-on-security-investment is *in*;
Blame games and fall guys for security incidents is *out* and risk management and shared accountability is *in*;
Tech talk and cop-speak is *out* and business language and communication skills is *in*; and
Silos or a fragmented security function is *out* and holistic security involving a coordinated approach to physical security, information security and risk management is *in.*

Such a shift in beliefs and their subsequent implementation poses difficult deployment dilemma organizationally; however, some pioneering efforts in influencing this transformation in information security management have started to emerge. For instance, frameworks proposed by Carnegie-Mellon Software Engineering Institute (CERT) are targeted to address the reality of risk management in complex and distributed operational environments, characterized by interoperable networked technologies and interrelationships and dependencies among technologies, data, tasks, activities, processes, and people. One such approach, called the Mission Assurance Analysis Protocol (MAAP), has been developed as an advanced, systematic approach for analyzing operational risk and gauging mission assurance in complex work processes (Alberts and Dorofee, 2005).

But problems of exploiting fear, playing the blame game, and dealing with silos in operations, as well as the need for a holistic approach to managing in complex and networked operational environments are not new challenges to organizations. In fact, they have been the focus of management attention for the past several decades (in modern business history) as firms have tried to produce quality products on a consistent basis in a highly competitive environment. Such parallels between

information security and quality motivate us to study the philosophy and methods of quality management, in the hope that we can draw from lessons in quality to develop a process approach to the management of information security.

QUALITY AND SECURITY: A COMPARISON

In this section, we explore some of the parallels that can be seen between quality management and information security management. In so doing, we draw some broad lessons for managing information security from the more than two decades of theory development and implementation experience in quality management. The discussion of this section is summarized in Table 1.

External environment

In manufacturing industries such as automobiles and consumer electronics, external competitive pressure by foreign firms, most notably Japanese, since the 1970s has exposed many vulnerabilities of U.S. manufacturing, ranging from poor product design, to manufacturing systems and suppliers, to organizational and industry structures. These manufacturing vulnerabilities were "exploited" by Japanese companies to leapfrog, gain market shares from, and sometimes almost annihilate their U.S. competitors in intense market competition. Similarly, vulnerabilities of information systems are being exposed and exploited through security attacks. Hackers and intruders exploited these systems vulnerabilities to achieve adversarial objectives and/or obtain monetary gains against the attacked firms. In comparison, while the former case is typically legally acceptable activity among organizations that are aimed at winning competitively (arguments of protectionism aside), the latter is an illegal or criminal activity done by individuals (or, more recently, organized crimes) against firms with malice and hostility. On the other hand, both have a common genesis in that they are activities that expose and exploit certain types of vulnerabilities of the target firm. The phrase "get better or get beat" was a message to U.S. manufacturing in the context of quality in an increasingly competitive environment in the 1980s. The same message can be applied in the context of information security today.

Historical development

Early (say, in the first half of the twentieth century) efforts at quality in the U.S. were focused on improving quality by removing defects through inspection as part of the production process. Gradually, this simple inspection function separated from production to form quality departments, isolating senior managers from being aware of quality problems and thus prepared for any resulting crisis. Eventually, around World War II, statistical quality control—a statistical approach to addressing manufacturing and production vulnerabilities—emerged as a discipline that focused on identifying and eliminating the problems that cause defects. But it was not until the late 1970s and early 1980s, driven by international competition, that quality assurance and control were brought to the forefront of management attention. It was later recognized that quality in organizations was everyone's business, not just the quality department's, and this realization brought about a broad drive to educate all employees of their roles and responsibilities as related to quality. This thinking of quality management that brings it to its source—the person who does the work—continues to this day (Box, 1995; Goldman, 2005; Juran, 1995).

Given this backdrop, compared with the history of quality management, the development of information security seems to be at an earlier stage. It has risen to gain significant managerial attention, due to events such as 9/11, the ubiquity of information systems in organizations today, and the high level of publicity from any large-scale security failure. However, due to a dominant focus on technical solutions, information security is still largely the preserve of experts, similar to the early days of quality management through specialized inspection function. So we find a disconnect in that while we have management attention on security, the responsibility for its delivery is still with the specialists, not everyone in the organization. High level of security awareness through comprehensive information security education of all employees in organizations seems to be an important step in the maturation of information security management (Hu and Dinev, 2005). Another disconnect is that, just as quality management evolved to focus on identifying and eliminating the problems that cause defects through the use of statistical techniques, fixing information security problems has to go beyond an event-based response to using statistical methods.

Evolving Definitions

The definition of quality has itself evolved and matured through many stages. These include quality defined on the basis of judgmental criteria of goodness of the product, product-based criteria involving quantities of some specific product attribute, user-based criteria as being what the customers wanted and how well the product performs its intended function, value-based criteria that relates usefulness or satisfaction to price, and manufacturing-based criteria derived from conformance to specifications (Evans and Lindsay, 2005). To manage and reconcile this diverse set of definitions of quality, ultimately an

integrated perspective that defines quality as being multi-faceted emerged. These quality facets or dimensions for goods are performance, features, reliability, conformance, durability, serviceability, aesthetics, and perceived quality (Garvin, 1984); and for services include reliability, responsiveness, assurance, empathy, and tangibles (Parasuraman et al., 1985). Further, the definition of goods and services quality has now evolved to mean the ability to satisfy given needs (ANSI definition). More commonly, this is stated as quality being the ability to meet or exceed customer expectations. This customer expectation approach has the advantage of being based on a long history of customer experiences with goods and services.

In the case of information security, we find a product-based definition in use today. A common way of defining information security is through the use of the key characteristics of information, namely, confidentiality, integrity, availability, privacy, identification, authentication, authorization, and accountability (Whitman and Mattord, 2004). This approach to defining security parallels the approach used to define the dimensions of quality; and these dimensions are similar to quality characteristics of service. For instance, the integrity and availability dimensions are associated with the information itself and parallel the tangibles dimension of service quality. Identification, authentication, authorization and accountability provide assurance. But confidentiality and privacy are related concepts that deal with access, something that is typically not considered in service quality. However, a customer-expectation-based definition of information security does not exist today.

Costs

The concept of cost of quality (COQ) centers on the costs associated with avoiding *poor* quality or those incurred as a result of *poor* quality (Evans and Lindsay, 2005). COQ is typically classified into four categories (Feigenbaum, 1983, Tatikonda and Tatikonda, 1996): appraisal costs (e.g. inspection, testing), prevention costs (e.g. training, redesign, new equipment), internal failure costs (e.g. rework, repair, scrap), and external failure costs (e.g. loss of customer goodwill, complaint handling, repair and replacement). Such cost analyses are justified because of the assumptions that failures are intrinsic in any system, prevention is cheaper than fixing, and performance is measurable (Chase et al. 2006).

In the case of information security, however, it is more common to talk about return on investment (ROI) of spending on security measures than the cost of (poor) security itself (Gordon and Loeb, 2002). More often than not, security investment, instead of the poor state of security, is often regarded as costs that need to be justified. Further, the ROI of security investment is particularly difficult, due to the fact that the success of such investment is measured by "nothing happens." As a result, companies tend not to invest in information security optimally (Schechter, 2005). The lack of such understanding of the importance of measuring the cost of (poor) security can be understood by examining the assumptions for analyzing COQ in the context of information security. The first assumption that failures are caused in any system is directly applicable to information security, because vulnerabilities always exist in any information system. But, while quality assumes such a failure *will* happen, the commonly adopted risk-management approach to security has instilled a probabilistic view that is often mistakenly interpreted as a failure "may or may not" occur. (In truth, the probabilistic view should be interpreted as "it will occur at some point in time.") When the security events are deemed not necessarily happening, the assumption that prevention is cheaper than fixing no longer holds even for potential disasters, because doing nothing is always cheaper than spending on security. The final assumption that performance can be measured is also hard to justify, because, as we argued earlier, the performance of security is not easily determined due to its nature of negative achievement. This comparison points out to a need for a definition of the cost of (poor) quality, perhaps in a fashion similar to COQ, that includes operationalized categories such as appraisal costs, prevention costs, internal failure costs, and external failure costs, that will lead to a better understanding of the return on and effectiveness of security investments.

Deming's Theory

Some of Deming's principles such as "drive out fear" and the need to "improve constantly and forever the system of production and service" are being recognized in information security management, as indicated earlier. But the fundamental principles in quality management are best summarized by Deming's "Theory of Profound Knowledge." This theory has four elements: systems thinking, understanding variation, the theory of knowledge, and human psychology (Deming, 1990; Hillmer and Karney, 1997, 2001; Rungtusanatham et al., 2003). All for are equally fundamental to, what we can paraphrase as, the "theory of profound security knowledge."

The need to "think systems" is natural to IT management, where systems and subsystems interact to create cause-and-effect relationships that are disconnected in time and space. The element of psychology to understand human nature is only beginning to be explored with respect to information security (Hu and Dinev, 2005). As the number of internal threats and incidents to information security rises, the need to understand intrinsic and extrinsic motivation of individuals is gaining significance. Further, the challenges of nurturing and preserving innate positive attributes will continue to be faced by companies in order to maintain information security. In interpreting the theory of knowledge, Deming's view was that experience alone does not establish theory. Experience is useful only in describing what occurred, and thus there is a need

for developing a theory of information security to be able to incorporate the knowledge to help management in the prediction or explanation of events.

Criteria	**Quality**	**Information Security**
Exposing system vulnerabilities	Done through competitive actions and is legal	Done with malice and is illegal
Managerial attention	Took competitive "defeats" in the market place to get it	Took large breaches and losses in the public eye to get it
Employee roles and responsibilities	Quality is everyone's business	Security is the responsibility of the technical experts
Employees education	Employees educated in technical issues such as statistical quality tools	Employees still treated as unable to grasp the technical intricacies involved, and so need to follow instructions of experts
Identifying and eliminating problems	Statistically-driven root cause analysis	Event-driven root cause analysis
Characteristics or dimensions	There are eight dimensions of goods quality and five dimensions of service quality	There are eight dimensions of information security
Dominant definition	Outcome-based definition of meeting or exceeding customer expectations	Process-based definition of providing protection along specific dimensions
Costs	Cost of quality is a well established concept	Cost of Security is limited to what is spent for appraisal and prevention but needs to be expanded to include internal and external losses
Deming's Theory of Profound Knowledge	Forms the basis of quality management	Can be extended to address information security management
Variation	Common cause and assignable cause variation well understood	Common cause variation recognizes ever present system vulnerabilities and assignable cause variation recognizes the intentional or unintentional exploitation of these vulnerabilities

Table 1: Summary of Quality vs. Security Comparison

The last element, variation, is present in all systems. In Deming's theory, variation actually consists of two elements, namely common cause variation and assignable cause variation. Simply put, common cause variation is a natural part of any process due to the complex interactions of various subsystems and the environment. Such combined effect is omnipresent, stable, and can be predicted statistically. It is simply a result of the design of the system. The concept of common cause variation can be translated into the information security context to mean that all information systems, being designed systems, always have a variety of vulnerabilities, which could surface during routine operations but do not disrupt the relatively stable information handling process for which they are designed. These variations (or intrinsic vulnerabilities) are out of the control of users, and are typically addressed in redesign that occurs in future versions of the system during upgrades.

Assignable causes are special causes of variation that arise from external sources not inherent in the established process. These causes result in unnatural, unpredictable variation that disrupts the random pattern of common cause variation. Assignable causes are detectable by statistical means and can then be corrected to restore the system to its previous stable state of common cause variations. In an information security context, intrusions are clearly an assignable cause. Even internal attacks are an assignable cause, because they emanate from individuals conducting activities that are not inherent to the designed purpose of the process or system. Unintentional but risky behaviors by individuals that may degrade security,

such as using "password" as log-in password, are also assignable causes, because those individuals are not acting as intended and are introducing external variation into the systems they are interacting with.

In summary, we find that adopting a variation approach to information security helps distinguish two areas that may cause information security problems. Common cause variation recognizes the ever-present system vulnerabilities, and assignable cause variation recognizes the intentional or unintentional exploitation of these vulnerabilities. Common cause variation in security due to vulnerabilities created by interacting subsystems should be addressed through system design and redesign efforts. This is beginning to happen in organizations that now require security-related issues to be addressed in the product design and be an integral part of the product development process. It is also important to note that not all common cause variation, or intrinsic vulnerabilities, can be expected to be removed, although progress can be achieved and should be maintained. On the other hand, an important part of the information security efforts should be directed to the reduction of assignable cause variation, because it is often more controllable by the users of the systems than common cause variation. This can be actively addressed through root-cause analysis (discussed below) and failure mode analysis methods. Finally, due to the "built-in" nature of common cause variation, an understanding of control limits of acceptable safety, or the notion of adequate security, becomes necessary.

In the next section, we explore these concepts of Deming's theory of variation further and develop a framework to address assignable cause variation in information security. A process-centric approach is developed as opposed to the event-centric approach that is generally used today. In such an approach, managing security is a process that involves both reactive and proactive analyses. This leads to recognizing information security management as a business process.

A PROCESS APPROACH TO INFORMATION SECURITY

The systems thinking element of Deming's Theory is adopted to define an intuitively appealing security management *system* with the following main elements:

Environmental Context: Security Regulation, Security Threats, Security Related Performance of Competitors, Security

Solutions

Organizational Context: Security Strategy, Policies, Culture

Security Delivery Process: Evaluate and Promote awareness, Assess and Analyze Risk, Apply or Implement Security Controls, Audit and Monitor Effectiveness

Individual Actions: Actions of Individual Participants

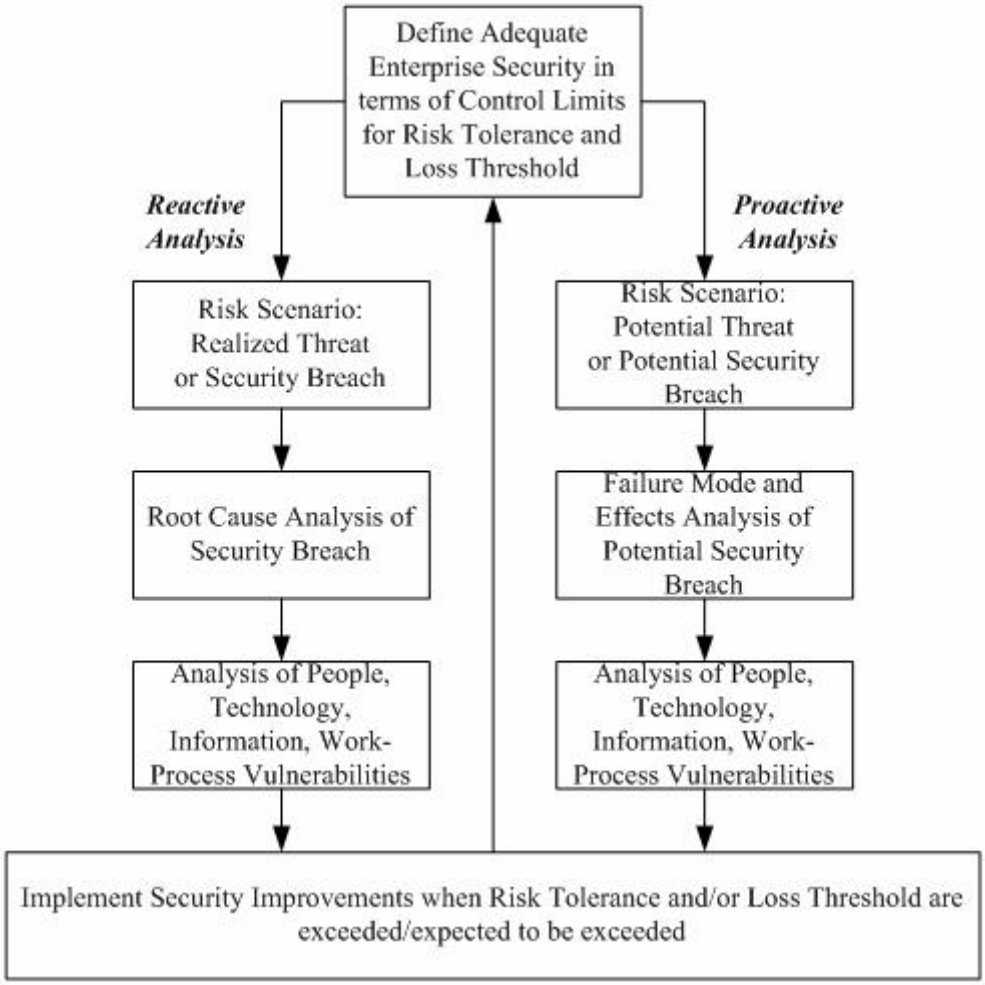
The combination of individual actions that exist within security processes and policies form the basis of an information security system that exists as an open systems interacting with a complex operational, technical and regulatory environment.

From the above, it can be recognized that ensuring information security is an ongoing process. Therefore, an enterprise-level information security analysis begins with an evaluation of loss threshold and risk tolerance, as opposed to assessing and analyzing threats to, and vulnerabilities of, assets. This is the starting point of a process-centric information security management framework, as shown in Figure 1 (adapted from Behara and Bhattacharya, 2006). It in direct contrast to the event-centric risk management approach that is the dominant paradigm today.

A security management process-centric framework is built upon the process management concepts that are established in quality management. Here "delivering security" is considered a process. As such, since all processes have variation, it is a foregone conclusion that there will always have some "variation," or vulnerabilities, in the extent of security afforded to users. Such variation in security can be due to assignable causes (that can be identified and removed) or common causes (that have to be designed out). This framework focuses on the identification and elimination/reduction of both causes for poor security. This, in turn, can be achieved by analyzing when a security breach has occurred to eliminate assignable causes by using a root-cause analysis, or proactively using failure mode and effects analysis to address common causes.

Based on our argument about the parallel between quality management and information security management, we adopt the widely used fishbone or cause-and-effects diagram approach to analyze the root-causes of security breach. This approach can be applied to a security breach in any part of an information network, that is, information processing in storage, applications, and/or transmission.

Figure 1: Process Approach for Information Security Management



As can be seen in Figure 2, the root-causes of any security breach (effect) can be classified into four categories (causes):

- Technology vulnerabilities
- People vulnerabilities
- Information vulnerabilities
- Work-process vulnerabilities

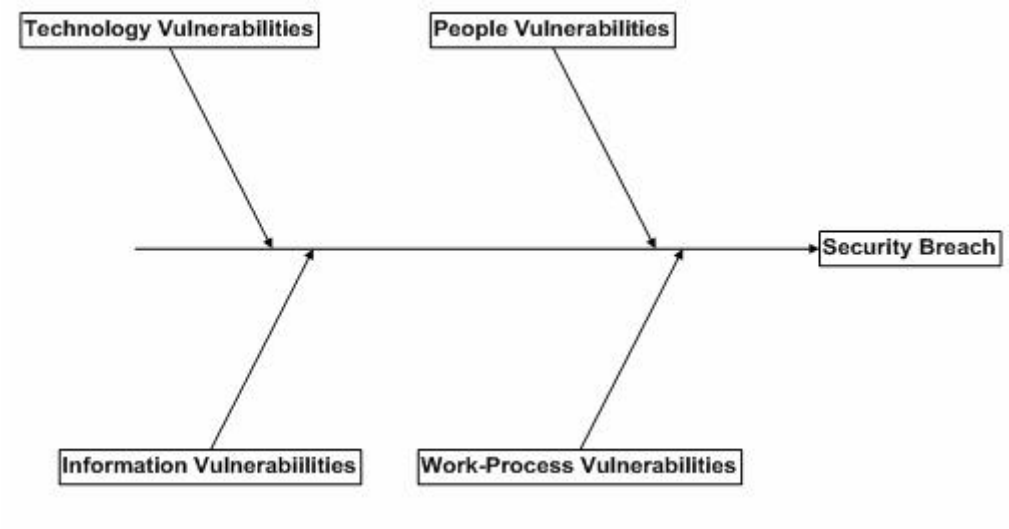
The traditional "solutions" that dominate the current security debate involves addressing the *technology vulnerabilities* of hardware, software or network components. Studies are beginning to recognize the need to address the *people vulnerabilities*, especially as the scope and scale of internal security breaches have increased in organizations. However, this framework specifically draws attention to the other two components that are typically ignored.

Information vulnerabilities are related to the intrinsic vulnerabilities associated with the attractiveness of the information that is being protected. By redefining the information structure and requirements, this vulnerability can be mitigated or resolved by reducing its attractiveness to attack. It is only after that, that solutions such as encryption may be considered.

Work-process vulnerabilities are inherent in the way work is accomplished in any domain. Of specific interest, however, is the way information is handled in the work process. Further, this distinction is increasingly non-discernable as much of the work today is information-intensive. Hence information security is not something that has to be done in addition to doing work (as it is now conceived), but an integral part of the work and its design. A useful process to benchmark would be the

nuclear materials handling processes in the nuclear power and nuclear reprocessing industries. Considering information to be "radioactive" would be a useful metaphor that can highlight the importance of integrating safe practices into work routines in a systematic and ubiquitous manner.

Figure 2: Root-Cause Analysis for Risk Management



Hence the new framework being proposed is process-centric and is focused on preventing repeat breaches by closing gaps identified through a root-cause analysis, and by closing potential gaps identified through a possibility-based failure mode and effects analysis (FMEA). FMEA is a structured method to identify, estimate, prioritize, and evaluate risk of possible failures, and then provide recommended actions to eliminate failures along with identifying those responsible for them. As such, the framework with both reactive and proactive analyses, is action-oriented and addresses technical and organizational issues. Concepts of adequacy, thresholds and tolerances are byproducts of managing this process within acceptable "control limits". It begins with an understanding of the causes, followed by solution options, and finally by control mechanisms to ensure consistent or reduced variability in the delivery of security.

CONCLUSION

This paper reviews some key concepts in quality management and draws lessons for information security management. This approach extends the theoretical basis for information security domain beyond its current focus on risk management. In doing so, it makes a contribution by consciously stepping away from the traditional technology-oriented event-centric view of risk management, and develops a process-centric framework with which to better understand the information security process and eventually to improve information security management practices in organizations. The framework is further explored to provide a guideline for root cause analysis to reduce assignable cause variation in the security process. Future research should involve the extension of this framework to apply failure mode and effects analysis to information security. In addition, since the framework developed in this study is a theoretical one, it provides opportunities for empirical validation and refinement through applications in specific cases.

REFERENCES

1. Alberts, C.J. and A.J. Dorofee (2005), "Mission Assurance Analysis Protocol (MAAP): Assessing Risk in Complex Environments," CERT: Networked Systems Survivability Program, Technical Note CMU/SEI-2005-TN-032, September 2005.
2. Behara, R.S. and S. Bhattacharya (2006), "Process-Centric Risk Management Framework For Information Security," in *National Security*, H. Chen, T.S. Raghu, R. Ramesh, A.Vinze and D. Zeng (Eds.), Elsevier.
3. Berinato. S., D. Duffy, S. Scalet, T. Wailgum and M. Wheatley (2004), "The ABCs of New Security Leadership," http://www.csoonline.com/fundamentals/abc_leadership.html, accessed on 28 February 2005.
4. Box, G. (1995), "Total Quality: Its Origins and Its Future," *Total Quality Management-Proceedings*, Chapman & Hall: London.

5. Chase, R.B., F.R. Jacobs, and N.J. Aquilano (2006), *Operations Management for Competitive Advantage*, McGraw-Hill Irwin, Boston.
6. Deming, W.E. (1990), "A System of Profound Knowledge," *ActionLine*, August, pp. 20-26.
7. Evans, J.R. and W.M. Lindsay (2005), *The Management and Control of Quality* (6th Edition), Thomson South-Western Press.
8. Feigenbaum, A.V. (1983), *Total Quality Control*, New York: McGraw-Hill.
9. Garvin, D.A. (1984), "What Does Product Quality Really Mean?" *Sloan Management Review*, 26 (1), pp. 25-43.
10. Goldman, H.H. (2005), "The origins and development of quality initiatives in American business," *The TQM Magazine*, 17 (3), pp. 217-215
11. Gordon, L.A., & Loeb, M.P. (2002) "The Economics of Information Security Investment," *ACM Transactions on Information and Systems Security*, 5 (4), pp. 438-457.
12. Hillmer, S. and Karney, D. (2001), "In Support of the Assumptions at the Foundation of Deming's Management Theory," *Journal of Quality Management*, 6 (2), pp. 371-400.
13. Hillmer, S. and Karney, D. (1997), "Towards Understanding the Foundation of Deming's Theory of Management," *Journal of Quality Management*, 2 (2), pp. 171-189.
14. Hu, Q. and Dinev, T. (2005) "Is Spyware an Internet Nuisance or Public Menace?" *Communications of the ACM*, 48 (8), pp. 61-66.
15. Juran, J.M. (1995), A History of Managing for Quality: The Evolution, Trends, and Future Directions of Managing for Quality, ASQC Quality Press: Milwaukee, WI.
16. Parasuraman, A., V.A. Zeithaml and L.L. Berry (1985), "A Conceptual Model of Service Quality and Its Implications for Future Research," *Journal of Marketing*, Fall.
17. Rungtusanatham, M., J.A. Ogden, B. Wu (2003), "Advancing Theory Development in Total Quality Management: A 'Deming Management Method' Perspective," *International Journal of Operations & Production Management*, 23 (7/8), pp. 918-936.
18. Schechter, S.E. (2005), "Toward Econometric Models of the Security Risk from Remote Attacks," *IEEE Security & Privacy*, 3 (1), pp. 40-44.
19. Tatikonda, L.U. and R.J. Tatikonda (1996), "Measuring and Reporting the Cost of Quality," *Production and Inventory Management Journal*, 37 (2), pp. 1-7.
20. Whitman, M.E. and H.J. Mattord (2004), *Management of Information Security*, Course Technology: Boston, Mass.