Overcoming Organizational Challenges to Secure Knowledge Management

Eliot Rich, Finn Olav Sveen and Matthew Jager

Abstract—**Successful secure knowledge management requires consideration of both technical and organizational concerns. We use the example of existing industrial incident management systems to delineate a causal structure that represents these organizational challenges. A dynamic simulation illustrates the cumulative effects of rewards, learning, and retributions on the fate of a hypothetical knowledge management system designed to collect information about events and incidents. Simulation studies are part of an ongoing research project to develop sustainable knowledge and knowledge transfer tools that support the development of a security culture.**

Index Terms—**Knowledge Management, Security, Simulation, System Dynamics, Incident Management, Organizations**

I. Introduction

Concerns about protecting knowledge often focus on protecting the knowledge from undesired exposure. Mitigation of these concerns tends to focus on technological solutions, neglecting the organizational, interpersonal and individual challenges that must be overcome for successful design and implementation. Within the context of secure knowledge management, these non-technical concerns become even more important, as they often create or sustain undesired vulnerabilities.

In this paper we outline some of the economic, social, strategic and cultural pressures that may affect the success of secure knowledge management programs. Drawing examples from existing industrial incident tracking systems, we identify several characteristics that will influence success or failure of secure knowledge management efforts. These include the motivations to report events and incidents, the efforts to evaluate the reports, the learning that occurs from the reports, and the effects of possible recriminations, among others [1-3].

Eliot Rich is an Assistant Professor in the Department of Information Technology Management, University at Albany, State University of New York, Albany, NY 12222 USA. (phone: +1-518-442-4944; fax: +1-518-442-2568; e-mail: e.rich@albany.edu).

Finn Olav Sveen is an researcher and engineer with the Security and Quality in Organizations Research Cell, Agder University College, Grimstad, Norway (e-mail: finn.o.sveen@hia.no).

Matthew Jager is with the College of Computing and Information, University at Albany, State University of New York, Albany, NY 12222 USA (e-mail: matthew.jager@gmail.com).

Ultimately knowledge management efforts must be judged by their results over time: Does the combined technical and social system for secure data produce sustainable results, or does it fail? We present a causal model and simulation study of the pressures that influence information sharing in high vulnerability environments. The model considers what must be accomplished to create a "security culture", one where the perceived incentives for accurate reporting and sharing of a restricted set of secure information are greater than the direct or indirect risks for a large proportion of participants [4-6].

Finally we mention efforts underway to design information sharing architectures that provide insight while addressing the social barriers to knowledge management and maintain confidentiality. The first is the creation of a Virtual Computer Security Incident Reporting System, which contains real and constructed data about events and incidents. This reporting system in turn can be linked to the development of Dynamic Stories, training tools that identify the issues and concerns that turn routine activities into sources of vulnerability. Our long-term goal is to facilitate secure knowledge sharing in a way that promotes the needs of all participants.

II. The Duality of Secure Knowledge Management

The concept of secure knowledge management has a dual nature that arises when considering the purpose of security and secure information in organizations. For the purpose of this discussion, we suspend the differentiation between knowledge, data, information, and wisdom, and look specifically at a different question: Are we securing knowledge, managing security knowledge, or both?

The first part of the duality, securing the knowledge asset may be thought of as ensuring its correct and appropriate use in the mission of the owner [7]. At the same time, it also includes the prevention of misuse, intentional or not, from internal and external sources [8]. The collective concerns of information confidentiality, integrity, assurance and non-refutability (CIA-NR) are a cornerstone of secure operations [9]. The support of CIA-NR has been the traditional concern of much of information security technology: encryption, firewalls, intrusion detection, and myriads of other tools [7, 10]. A 'defense in depth' strategy, where multiple overlapping technologies are employed to improve the security profile of the firm, has been strongly recommended for some time [11].

The second part of the duality, managing security knowledge, concerns the collection, validation, and application of security-related information for the benefit of the firm. Many of the technologies mentioned above both protect and

report on their activities. The ability to use this knowledge to modify and proactively maintain a strong security profile is crucial for the ongoing success in the face of rapid threat changes. In addition, successful dissemination of the lessons from past security failures and near-misses is important to the development of a security consciousness within the culture of the firm. This consciousness may help defend against future unpredicted events and give employees a consistent touchstone for judging and evaluating their actions in the light of uncertain information.

The complexity of managing information about security is increasing apace with the security threat. The increase in attack volumes, sophistication, and possible reactions has been growing [12]. There is therefore great reason to expect that the need for both secure knowledge management and management of security information will continue to be important.

III. The Organizational Challenges

Non-technical issues often determine the fate of knowledge management programs [13]. We draw from reviews of knowledge management programs, security studies, and safety incident systems to identify important organizational influences. These reflect the reality of organizational behavior, which is imperfectly rational, economically sub-optimal, and driven in large part by satisficing the micro- and conflicting requirements of multiple stakeholders [14].

Managers must allocate limited economic and technical resources. Prior to a security breach, it is difficult to estimate the benefits of securing information relative to other investments. After a security breach, of course, the economic losses may be quite profound [12], and earlier decisions might well be questioned. While economic models exist to guide firms in their allocation decisions [15], firms do not always recognize the full economic or strategic value of preventing errors [16]. A system to manage secure knowledge for the benefit of the firm provides similar preventative value, but its perceived importance may not be clear in the absence of failures. Indeed, success in avoiding problems and deterrence of would-be attackers may create complacency.

A second concern arises around individual perceptions of the importance of security relative to other pressures in the firm. While the need for user training in support of a secure organization is discussed often, users may find strong security rules intrusive, cumbersome, or at odds with their contributions to profit. Studies of technology acceptance ([17, 18]) explicitly consider perceived usefulness as an important factor in successful implementation. If the collection and dissemination of security knowledge are not seen as contributing to the production-oriented goals of the firm, they will be de-emphasized. Resistance to knowledge sharing can also arise when internal competitive pressures within the firm create resistance to proper security controls [19]. Another possible motive for intentional interference with security and audit policies is covering the tracks of an attack, particularly when the source is an insider [20].

Successful secure knowledge management should consider the effects of disclosure on the individual and the firm, as disincentives may be difficult to eliminate. In safety reporting, for example, when incident reports have to pass upwards through a hierarchy to reach decision-makers, where they can be acted upon, superiors may stop a report that indicates their responsibility for neglect or wrongdoing [1]. Anonymous or confidential reporting systems demonstrate greater success, in terms of participation [21] but, in removing identifying information, important details of the problem can also be lost, reducing the effectiveness of the system.

From the firm's perspective, a collection of security breaches and near-misses might in itself become an important target for attack. Such sensitive knowledge might include incident reports that demonstrate an organization's awareness of some potentially dangerous situation, which, if not corrected, could lead to an accident. It has been observed that prior knowledge of a dangerous situation can be an important influence if punitive damages are assessed in litigation [1].

Personal relationships within the firm may limit compliance as well, as a employee's sense of loyalty to a coworker or superior may prevent them from sharing knowledge that could be harmful to their reputation or career [1, 6].

Finally, the reporting of incidents needs to reach beyond the traditional boundaries of the organization. The USSS-CERT/CC study of insider attacks in banking and finance institutions found that 83% of the breaches in their database were first noted by individuals outside the target firm, rather than by internal staff [20].

None of these problems are surprising, and none are insurmountable. The implementation of systems to manage secure information requires more than just strong technological solutions. It requires strong economic incentives, strong formal and informal support, clear linkage to business requirements and monitoring and enforcement to ensure compliance [8, 15, 22]. All of these must consider how managers, workers, and information technologists look at information security through their own lenses, and create a synthesis of needs and tradeoffs.

IV. Incident Reporting Systems as a Model of Secure Knowledge Management

Incident reporting systems have been in use in aviation, chemical processing industry, nuclear industry and health care for many years. These systems have characteristics similar to those of secure knowledge management systems. They are concerned with a specific kind of sensitive data: mistakes, miscalculations, oversights, and shortcomings in an organization's practices that may affect current or future production outcomes. A significant incident exposes the firm to financial loss, possible regulatory scrutiny and loss of reputation and market share.

Incident reporting systems and secure knowledge management systems both exist in a context where technology, economics, and organizational theory combine. Users of these incident reporting systems are faced with the short-term exposure of mistakes, miscalculations, oversights, and shortcomings on themselves and their work environments, creating conflicts that affect their motivations to participate. In secure knowledge environments, users are tempted to take short-cuts and bypass security practice. A reporting system

would expose these decisions and create similar conflicts among desired practices and true behavior. This motivates an examination of incident reporting systems as a model for what might be expected in secure knowledge management.

Despite long experience with such systems, incident reporting systems continue to be plagued by reporting and quality problems [1]. An interesting observation is that the same kinds of problems recur across these different industries. This indicates that there may be a general dynamic structure that is valid for many of these situations.

The model presented below is a synthesis of many cases from several different industries. The model was created using the feedback approach of System Dynamics, and implemented in Vensim DSS[1] software. System Dynamics views systems as governed by feedback, information and material delays, and accumulations. It provides insight into complex problems by considering how the structure of a system influences its behavior over time [23].

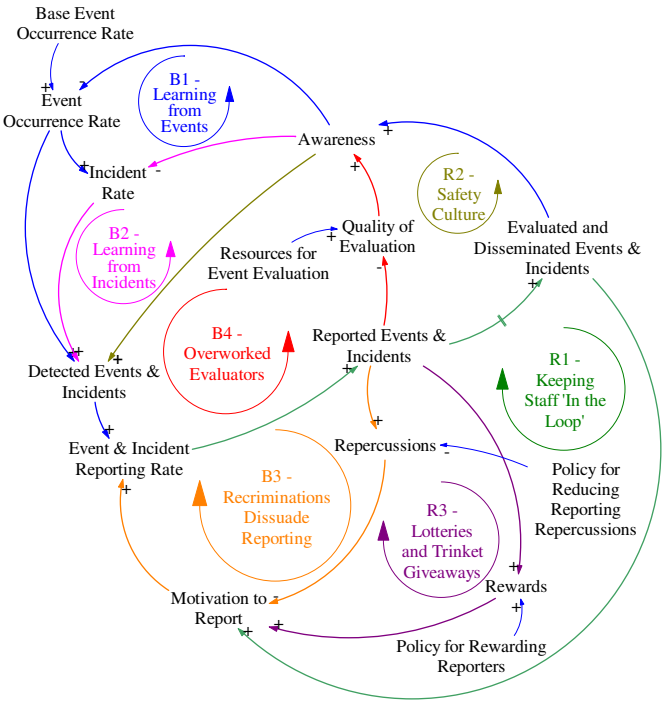

Figure 1 - Causal Loop Diagram of a generic Incident Reporting System[2]

The model consists of a set of causal loops that depict how events and incidents are reported, evaluated, and used for organizational learning. Note the distinction between incidents and events. Here an event is defined as an unanticipated situation or near miss, managed with little or no short-term cost. If an event is not mitigated it turns into an incident which has an immediate cost or result, such as an injury. We have assumed that the incidents and events are reduced according to a power law experience curve: with each doubling of properly investigated incidents, the incident and event occurrence rate is reduced by a certain percentage, reflecting gradual learning from experience about incidents and events.[3]

The general goal of an incident reporting system is to share information on incidents to avoid recurrence or minimize damage. When an incident (or an important near-miss event) occurs, someone, typically an operator, a nurse or a pilot, detects and reports it. At that stage an investigative team is presumed to take over and attempt to find the root causes of the incident. When the root cause has been found, safeguards can be put in place; personnel can be made aware of the danger and can be made aware of the problem, thus avoiding future occurrences of the same incident (B2) or in the case of an event, avoiding that it in the future turns into an incident (B1). As personnel become more safety aware, they become better at spotting potential incidents and more events and incidents are reported (R2).

In the parlance of System Dynamics, B1 and B2 are balancing feedback loops, where an exogenous pressure will tend to be balanced over time. In this case, B1 and B2 describe how an increase in the rate of new events increases knowledge, which increases awareness and reduces the rate of events in the future. R2 is a reinforcing feedback loop, describing how a strong safety culture creates pressures that further strengthen it. Later in the paper we will see that there are powerful balancing feedback loops, B3 and B4, which counteract the effect of R2.

As personnel experience that their reports are being taken seriously and that their participation leads to safety improvements, their motivation to report increases (R1). Vice versa, if their reporting is not perceived as leading to improvements, staff may be dissuaded from reporting. Johnson termed this *keeping staff 'in the loop'* [1]. The issue may not only be of staff feedback, but also of feedback to organizations. An example is Taiwan's use of mandatory aviation incident reporting to the Taiwanese Civil Aviation Administration (CAA). [21] reports that the CAA's aviation incident database contains considerable amounts of incident data, but due to lack of funding, the data has not been used for trend analysis. Furthermore, the data has been inaccessible in nature and thus have not been used by Taiwanese air carriers or Taiwan's Aviation Safety Council (a Taiwanese aviation incident investigation group).

Many organizations use incentives to increase the reporting rate (R3). However, another strong force that has detrimental effects on the motivation to report are various recriminations that exist inside and between organizations (B3). Reprimands from management, co-workers seeing the reporter as disloyal, media exposure, legal prosecution and culture are some of the factors that can dissuade reporting [1, 6, 21, 25].

[1] http://www.vensim.com/

[2] + and - denote polarity. A causal link from A to B is positive if A adds to B, or if a change in A produces a change in B in the same direction. Decreasing A leads to a decrease in B or an increase in A leads to an increase in B. A causal link from A to B is negative if A subtracts from B, or if a change in A produces a change in B in the opposite direction. See [23] for more on polarity. The // marks denote a time delay.

[3] See [24] for more on learning/experience curves.

The last part of the model concerns the quality of the investigations. If the quality is too low, i.e. if the systemic root causes of the incidents are not found, the organization's awareness will not increase and safeguards, if put in place, will not be efficient. In the words of Johnson, "Incident reporting systems can provide important reminders about potential hazards. However, in extreme cases these reminders can seem more like glib repetitions of training procedures rather than pro-active safety recommendations. Over time the continued repetition of these reminder statements from incident reporting systems is symptomatic of deeper problems in the systems that users must operate." [1]

Several simplifying assumptions apply at this point. In the model, quality of evaluation is simplified to a function of the amount of resources available and the workload. In reality, the investigator's level of training and level of experience will also contribute. All events and incidents have the same severity; in the real world, serious incidents would most likely receive additional resources for investigation. However since the model works on averages over time rather than discrete events, this is a reasonable simplification.

The effects of management commitment to the reporting system are not explicit in the causal model. This is because we believe that if management commitment is not strong enough, none of the individual parts of an incident reporting system will function satisfactory. Sporadic management emphasis and management fear of liability [6] may hinder the functioning of an incident reporting system. If management is not totally committed and lead by example, subordinate staff will not follow either.

V. Simulation Runs

The causal model was adapted to a difference equation structure through Vensim and simulated under four different scenarios to examine the effects of different organizational policies concerning incident reporting. As a synthetic model, a set of parameters are used that that illustrate the problem, rather than claim to represent a specific reality. In all the scenarios an incident reporting system is introduced at time 0. The **Base Run** is a scenario where incentives and recriminations are not present and adequate resources for investigation are provided. In **Recriminations** and **Incentives**, recriminations against reporting and incentives towards reporting are respectively introduced. Scenario **Inadequate Resources** has 12.5 % fewer resources assigned to investigation than what is actually needed to evaluate, causing an accumulation of unanalyzed incidents. [4]

In all four scenarios the introduction of an incident reporting system causes an initial reduction in incident rate (Figure 2). However, in the **Recriminations** scenario *incident rate* increases again after about month 42, reflecting the effects of strong recriminations on reporters and on their propensity to report in the future (loop B3). In the three other scenarios, *incident rate* eventually reaches equilibrium. The **Incentives** scenario, where employees are encouraged to report, shows a substantial improvement in incident rates over **Base Run,** with incentives and trinkets (loop R3), increasing the motivation to report. **Inadequate Resources,** where there is insufficient evaluation and feedback to reporters about the effects of their contributions, provides some level of protection from incidents, but less than **Base Run**.

While the true incident rate is an important metric, it is not what managers see. Managers can only estimate the rate of incidents from the data that is actually reported. This difference has an important effect on how the actual safety and security profile of the firm is understood.

In the **Base Run** and **Inadequate Resources** scenarios *incident reporting rate* behavior (Figure 3) is similar to *incident rate* behavior. However in the **Recriminations** scenario *incident reporting rate* is substantially lower than the other scenarios. The recriminations create a problem of underreporting which can lead managers to believe that they have a safe system when it is actually not the case. In the

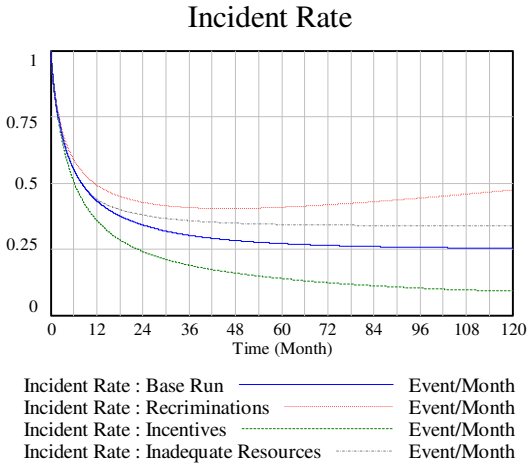

Figure 2 - Incident Rate

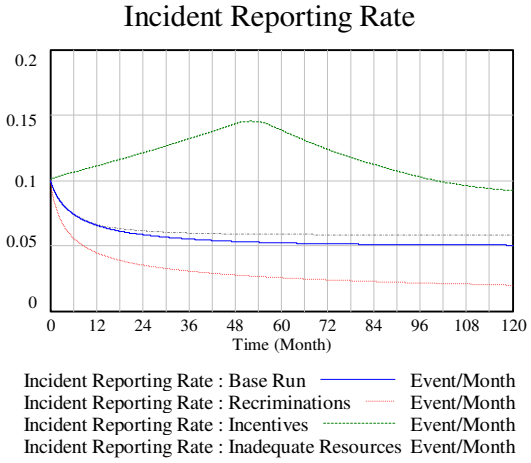

Figure 3 Incident Reporting Rate

[4] The details of the model are available from the corresponding author (Rich).

Incentives scenario *incident reporting rate* actually increases for the first 44 months. However when we compare with *incident rate* the system is actually becoming safer. There is an initial problem of underreporting and the incentives are strong enough to substantially improve the situation, especially in the absence of recriminations. [1, 3, 5, 26] all point to underreporting as a major problem in incident reporting systems.

The last graph shows the *event reporting rate* (Figure 4). As previously explained, events are near misses. They are thus perfect opportunities to learn from without incurring heavy penalties in incident costs. An important observation here is that there is an inverse relationship between *incident rate* and *event reporting rate*. This has been shown empirically by [5]. Thus the number of reported events can be an indicator for the number of incidents.

These four runs illustrate the potential for a successful incident reporting system, but they also show that there is potential for partial or even complete failure if important factors such as quality of investigation and motivation to report are not handled well. There is also the possibility of misjudging the number of incident and events, if one believes that the true number of incidents and events are equal to the number of reports. The simulation scenarios indicate that the creation of a safety culture is possible. A safety culture arises when a stream of reports feeds organizational awareness (R2), increasing it or keeping it at a high enough level to allow for the detection of new dangerous situations or of relapse to old unsafe practices. However, this is only possible if recriminations against reporting are minimized or completely removed.

VI. Incident Reporting and Information Security

Many industries and individual companies have successfully initiated safety reporting systems. An example is the aviation industry, with NASA's Aviation Safety Reporting System as the best known, although there are numerous others. The chemical processing industry has a host of reporting systems. Most of these systems are on a local factory level. Norsk Hydro is one company that has introduced such systems with good results [27]. In recent years the health care industry has seen a wave of safety reporting systems, although with mixed results [28-30]. Still, there is little doubt that safety reporting systems have contributed significantly towards safety improvements in many of these industries.

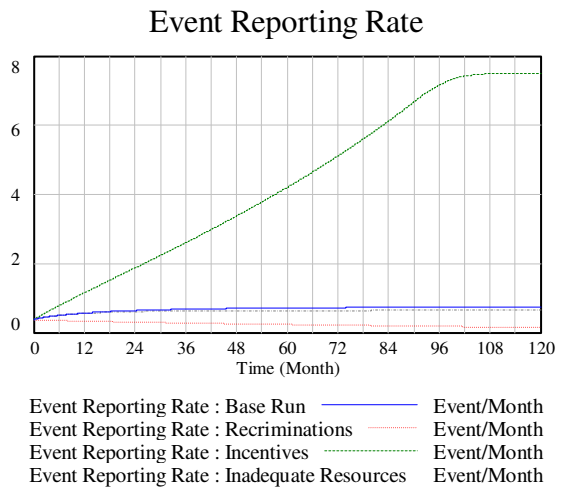

Figure 4 Event Reporting Rate

Is such an industry-wide reporting system necessary for successful information security? A particular and passionate statement [31] compares the frustrating situation for cyber data reporting with the success of 'Air Safety Reporting Systems'. [32] provides further argument towards the need for such a system, focusing on incident reporting as a quality improvement process.

Both the model developed in this paper and the literature on which it is based illustrate the potential of an incident reporting system to significantly reduce incidents [1-6, 21, 25, 26, 32-35]. This leads us to believe that such a system, if implemented correctly, would also be useful within information security. It would be an integral part of creating a prevention-based approach to information security, rather than a reactive or punitive one.

Our current fieldwork focuses on two aspects of the secure knowledge management:

1) At present, individual organizations gather security effectiveness data for narrow operational purposes, making scientific research on incidents difficult [32].

2) Establishing an effective incident reporting systems and appropriate incentives by identifying conflicting priorities and barriers to information sharing.

To overcome these two problems, the AMBASEC project of which the authors are part has been using Group Model Building (GMB) to create System Dynamics (SD) models of particular security problems within the Norwegian offshore oil & gas sector [36]. GMB circumvents the usual problem of sensitive data by allowing for a high degree of aggregation while at the same time retaining the most important lessons. These SD models can then be used *'in reverse'* to generate narratives, what we call "Dynamic Stories". Parameter variation of the SD model allows for computation of multiple Dynamic Stories. These dynamic stories are in a sense *virtual incidents,* which can then be used to initially populate an incident reporting system. This provides grounded and secure data for organizations who wish to protect themselves and for scientists who wish to conduct research on the problem. Although a proper Cyber Security Reporting System still seems but a distant vision, a *virtual incident* reporting system can be rapidly established since it circumvents the problem of sensitive data.

VII. Conclusion

This paper argues for serious consideration of the effects of organizational and individual factors in support of secure knowledge management systems. The similarities between industrial incident reporting and computer security problems give a direction and important analogy to consider. The literature reviewed clearly points to aspects of organizational

culture that have significant effects on the use and utility of integrated information systems that is plainly ignored in the development and implementation of these systems.

Through a simulation study the difference among incident rates, incident reporting rates, and event rates are explored. Under different assumptions the same system may generate sustainable management of knowledge at different levels of effectiveness, or a program that loses its value.

Our ongoing research program with different industry and research groups works to understand and reduce barriers to information sharing through group modeling and development of archetypical stories that transfer the essence of security lessons without exposing specific vulnerabilities and competitive information. We hope to demonstrate that the key to a secure firm does not rest solely in the use of technological tools alone, but in the proper implementation of these tools, and their alternatives, that is made possible through cultural and social analysis of organizations.

VIII. Acknowledgements

This research has been financed in part by the Research Council of Norway under grant 169809/D15, Improving Security by Improving Data (ISECBIDAT), and grant 164384/V30, A Model Based Security Culture (AMBASEC) project, both under the direction of Prof. J. J. Gonzalez, Agder University College, Norway. The authors greatly appreciate the support of the Research Council and Prof. Gonzalez.

IX. References

[1] C. Johnson, *Failure in Safety-Critical Systems: A Handbook of Incident and Accident Reporting*. Glascow, Scotland: Glascow University Press, 2003.

[2] J. Reason, "Human Error Models and Management," *British Medical Journal* vol. 2000(320), pp. 768-770, 2000.

[3] N. Stanhope, M. Crowley-Murphy, C. Vincent, A. M. O'Connor, and S. E. Taylor-Adams, "An Evaluation of Adverse Incident Reporting," *Journal of Evaluation in Clinical Practice*, vol. 5(5-12), 1999.

[4] D. L. Cooke, "The Dynamics and Control of Operational Risk," Unpublished PhD Dissertation. Haskayne School of Business University of Calgary, Alberta, 2004.

[5] S. Jones, C. Kirchsteiger, and W. Bjerke, " The Importance of Near Miss Reporting to Further Improve Safety Performance," *Journal of Loss Prevention in the Process Industries*, vol. 12(59-67), 1999.

[6] J. R. Phimister, U. Oktem, P. R. Kleindorfer, and H. Kunreuther, "Near-Miss Incident Management in the Chemical Process Industry," *Risk Analysis*, vol. 23(3), 2003.

[7] ISO/IEC, "Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model," Geneva, Standard ISO/IEC 15408-1:2005(E), October 2005.

[8] C. B. Haley, J. D. Moffett, R. Laney, and B. Nuseibeh, "A framework for security requirements engineering," presented at the 2006 international workshop on software engineering for secure systems, 2005, Shanghai, China

[9] ISO/IEC, "Information technology - Security techniques - Evaluation criteria for IT security — Part 2: Security Functional Requirements," Geneva, Standard ISO/IEC 15408-1:2005(E), October 2005.

[10] National Institute of Standards and Technology, "An Introduction to Computer Security: The NIST Handbook," US Department of Commerce, Special Publication 800-12, July 2000.

[11] National Institute of Standards and Technology, "Engineering Principles for Information Technology Security (A Baseline for Achieving Security)," US Department of Commerce, Gaithersburg, MD, Special Publication 800-27, June 2001.

[12] L. A. Gordon, M. P. Loeb, W. Lucyshyn, and R. Richardson, "2004 CSI/FBI Computer Crime and Security Survey," Computer Security Institute, Technical Report 2004.

[13] L. Damodaran and W. Olphert, "Barriers and facilitators to the use of knowledge management systems," *Behaviour & Information Technology*, vol. 19(6), pp. 405-413, 2000.

[14] J. G. March, *A primer on decision-making: How decisions happen*. New York: Free Press, 1994.

[15] L. A. Gordon and M. P. Loeb, "The economics of information security investment," *ACM Transactions on Information and System Security*, vol. 5(4), pp. 438-457, 2002.

[16] N. Repenning and J. Sterman, "Nobody Ever Gets Credit for Fixing Defects that Didn't Happen: Creating and Sustaining Process Improvement," *California Management Review*, vol. 43(4), pp. 64-88, 2001.

[17] F. D. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology," *MIS Quarterly*, vol. 13(3), pp. 319-340, 1989.

[18] V. Venkatesh and F. D. Davis, "A theoretical extension of the technology acceptance model: Four longitudinal field studies," *Management Science*, vol. 46(2), pp. 186-204, 2000.

[19] H. K. Moon and M. S. Park, "Effective reward systems for knowledge sharing," *Knowledge Management Review*, pp. 22-25, 2002.

[20] M. R. Randazzo, M. M. Keeney, E. F. Kowalski, D. M. Cappelli, and A. P. Moore, "Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector," U.S. Secret Service and CERT Coordination Center / Software Engineering Institute, Pittsburgh, PA, Technical Report August 2004.

[21] P. I. Lee and T. R. Weitzel, "Air Carrier Safety and Culture: An Investigation of Taiwan's Adaptation to Western Incident Reporting Programs," *Journal of Air Transportation*, vol. 10(1), 2005.

[22] J. M. Stanton and K. R. Stam, *The visible employee*. Medford, NJ: Information Today, 2006.
[23] J. D. Sterman, *Business dynamics: Systems thinking and modeling for a complex world*. Boston: Irwin McGraw-Hill, 2000.
[24] W. Zangwill and P. Kantor, "Toward a theory of continuous improvement and the learning curve," *Management Science*, vol. 44(7), pp. 910-920, 1998.
[25] D. J. Anderson and C. S. Webster, "A System Approach to the Reduction of Medication Error on the Hospital Ward," *Journal of Advanced Nursing*, vol. 35(1), pp. 34-41, 2001.
[26] P. Barach and S. D. Small, "Reporting and Preventing Medical Mishaps: Lessons from Non-medical Near Miss reporting Systems," *British Medical Journal*, vol. 320, pp. 759-763, 2000.
[27] S. Jones, C. Kirchsteiger, and W. Bjerke, "The Importance of Near Miss Reporting to Further Improve Safety," *Journal of Loss Prevention in the Process Industries*(12), pp. 59-67, 1999.
[28] R. H. James, "1000 Anaesthetic Incidents: Experience to Date," *Anaesthesia*, vol. 58, pp. 856-863, 2003.
[29] N. Stanhope, M. Crowley-Murphy, C. Vincent, A. M. O'Connor, and S. E. Taylor-Adams, "An Evaluation of Adverse Incident Reporting," *Journal of Evaluation in Clinical Practice*, vol. 5(1), pp. 5-12, 1998.
[30] A. S. Nyssen, S. Aunac, M. E. Faymonville, and I. Lutte, "Reporting Systems in Healthcare From a Case-by-Case Experience to a General Framework: An Example in Anaesthesia," *European Journal of Anaesthesiology*(21), pp. 757-765, 2004.
[31] B. Schneier, *Secrets & Lies: Digital Security in a Networked World*: Wiley, 2000.
[32] J. J. Gonzalez, "Towards a Cyber Security Reporting System -- A Quality Improvement Process," in *Computer Safety, Reliability, and Security*, *Lecture Notes in Computer Science 3688*, B. A. G. Rune Winther and G. Dahll, Eds. Heidelberg: Springer, 2005.
[33] R. H. James, "1000 anaesthetic incidents: experience to date," *Anaesthesia*, vol. 58(856-863), 2003.
[34] A. S. Nyssen, S. Aunac, M. E. Faymonville, and I. Lutce, "Reporting systems in healthcare from a case-by-case experience to a general framework: an example in anaesthesia," *European Journal of Anaesthesiology*, vol. 21, pp. 757-765, 2004.
[35] J. Reason, "Combating omission errors through task analysis and good reminders," *Journal of Quality and Safety in Health Care*, vol. 11, pp. 40-44, 2002.
[36] S. A. Hillen, F. O. Sveen, and J. J. Gonzalez, "Using Dynamic Stories to Communicate Information Security," presented at International System Dynamics Conference, Nijmegen, The Netherlands,, 2006.