Toward a Generic Model of Security in an Organizational Context: Exploring Insider Threats to Information Infrastructure

Ignacio J. Martinez-Moyano
imartinez@anl.gov

Michael E. Samsa
msamsa@anl.gov

James F. Burke
jay@anl.gov

Bahadir K. Akcam[1]
bahadirakcam@gmail.com

Decision and Information Sciences Division
Argonne National Laboratory
9700 South Cass Avenue, Bldg. 900
Argonne, IL 60439-4832

Rockefeller College
University at Albany
1400 Washington Ave.
Albany, NY 12222

Abstract

This paper presents a generic model for information security implementation in organizations. The model presented here is part of an ongoing research stream related to critical infrastructure protection and insider threat and attack analysis. This paper discusses the information security implementation case.

1. Introduction

In this paper, we expand on previous work related to the behavioral and technical aspects of emerging insider threat identification that has the potential to explain successes and failures in detection of malicious insiders [22-24, 30] and on work that explores the dynamics of military operations from social and organizational perspectives [3]. The two bodies of work, although dealing with two seemingly disconnected domains, share fundamental elements related to the security dynamics. The work presented here is part of a larger effort to study critical infrastructure protection and to develop a decision support system for stakeholders in this area. This effort is termed Critical Infrastructure Protection Decision Support System (CIPDSS) and uses system dynamics as one of several modeling approaches [for an overview, see Ref. 4]. CIPDSS has been used to analyze several different situations; for example, the introduction of infectious diseases [28], the loss of multiple telecommunications assets [21], and the accidental release of toxic industrial chemicals [32].

The work presented here elaborates on aspects of the *dynamic trigger hypothesis* developed by Andersen et al. [1] in which they describe interacting feedback causal mechanisms in organizations that have the potential to create security risks and the emergence of malicious insiders ready to launch threats and attacks to organizational assets, including information systems.

Figure 1 shows a partial view of the causal structure of the *dynamic trigger hypothesis* as described by Andersen et al. [1] in which the detection trap (*R1*) and the trust trap (*R2*) are identified.

The detection trap and the trust trap are important in the model presented here, as these two mechanisms are prevalent in the military and information security contexts.

According to Andersen et al. [1], a detection trap arises when the organizational detection capability is low, leading to low levels of detected activity by insiders (threats and/or attacks). A low level of malicious activity lowers the organization's perceived risk, decreasing its desired investment in security measures and culminating in even lower levels of detection. In this sense, organizations create their own demise. Likewise, a trust trap can arise when lower levels of detected malicious activity increase managerial trust in the security

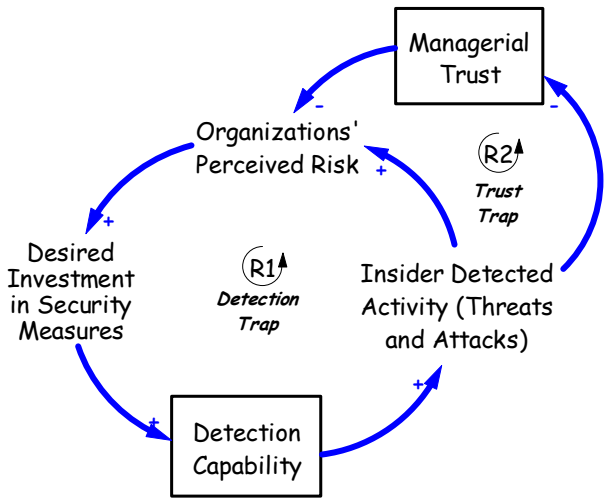

Figure 1. Dynamic trigger hypothesis

[1] Mr. Akcam's contributions to this paper were developed during a summer internship at Argonne National Laboratory in 2007.

1530-1605 2008 U.S. Government Work Not Protected by U.S. Copyright

of the system, pushing the perceived risk down and leading to underinvestment in security and eroded detection capabilities.

The core of the model presented here recognizes that when security operations are conducted, errors are made, and these errors trigger dynamics that can expose systems to increased risk and vulnerability. Additionally, the model embodies a theory of learning by doing and of dynamic decision making, used for the behavioral study of emerging threats.

2. Information security models

Information security has been explored by using the system dynamics approach to focus on a number of topics, including the insider threat and attack problem [1, 23, 26], understanding security risks [30], and increasing learning and risk perception [6, 14, 15, 22], among others [for a good collection of papers on the topic, see 13]. Specifically, our previous work related to insider threat identification and mitigation was based on empirical evidence collected by researchers of the CERT Coordination Center at Carnegie Mellon University's Software Engineering Institute with the U.S. Secret Service.

Following previous work on identification of insider activity [24, 25], we model learning by using a learning-by-doing mechanism. Learning models have been used in disciplines such as psychology, economics, and educational research [see Refs. 5, 10, 11, 16-20]. Learning by doing can be characterized as a reinforcement model of learning in which the premise is that people learn with experience [20]. In our research, however, it is salient that it can be difficult to directly experience the consequences of many of our decisions [24, 36]. In reinforcement learning models, learning is achieved by identifying the outcomes of actions and decisions and assigning utility that promotes improvement. For example, Martinez-Moyano et al. [22, 23], when studying insider-threat activities and vulnerabilities, use a reinforcement learning model to capture the mechanism used by security officers to determine the level of cutoff that maximizes identification of insider activity.

3. Methods

We use the system dynamics modeling approach to develop the model presented here [12, 31, 36, 37]. The system dynamics approach allows researchers to gain insight into dynamic problems by providing a framework to identify the causal structure that conditions the observed behavior of systems. System dynamics modeling has an orientation toward identifying feedback-rich endogenous theories potentially useful to explain the phenomenon of interest.

4. Model description

4.1 Model overview

The model focuses on the interaction that the implementation of security measures has with attackers' results, support of the user community, learning, and the emergence of excessive security measures over time. Figure 2 shows a sector view of the structure of the model.

Our model emphasizes social and organizational elements surrounding the implementation of information security measures in organizations. There seems to be agreement among researchers in the information security field that it is important to consider social and organizational issues in security models [8, 9, 33]. The inherent importance of social and organizational issues in the implementation of information security measures stimulates this trend.

Personnel in information security departments, malicious insiders, management, and the user community are actors in the model. The information security department embodies the effort and decision-making capacity for information security implementation. In this construct, we include the information technology department and other departments that oversee information security tasks and share responsibility related to ensuring that the information infrastructure is secure.

This model focuses on insider attacks. According to Schultz [34, p. 526], citing work by Schultz and Shumway [35, p. 189], an insider attack is "the intentional misuse of computer systems by users who are authorized to access those systems and networks." Research has been conducted to investigate the work leading to insider threats and attacks [2, 8, 9, 27, 33, 34]. Although some claim that insider security incidents occur far more frequently than externally-generated incidents [2], others characterize the claim as a misconception and myth, tracing it back to old FBI statistics [34]. Aside from this, however, it seems that "there is no debate that insider attacks pose a far greater level of risk than do outsider attacks" [34, p. 527]. Additionally, insights from our work in military operations are brought into this model. Particularly, we incorporate a structure that recognizes that, under certain circumstances, the people in charge of security-related operations might choose to use unwarranted force in order to accomplish their mission: to keep the infrastructure secure. In this model, stopping attacks and learning how to do this in a more efficient way without incurring excesses is the focus of the information security problem depicted.

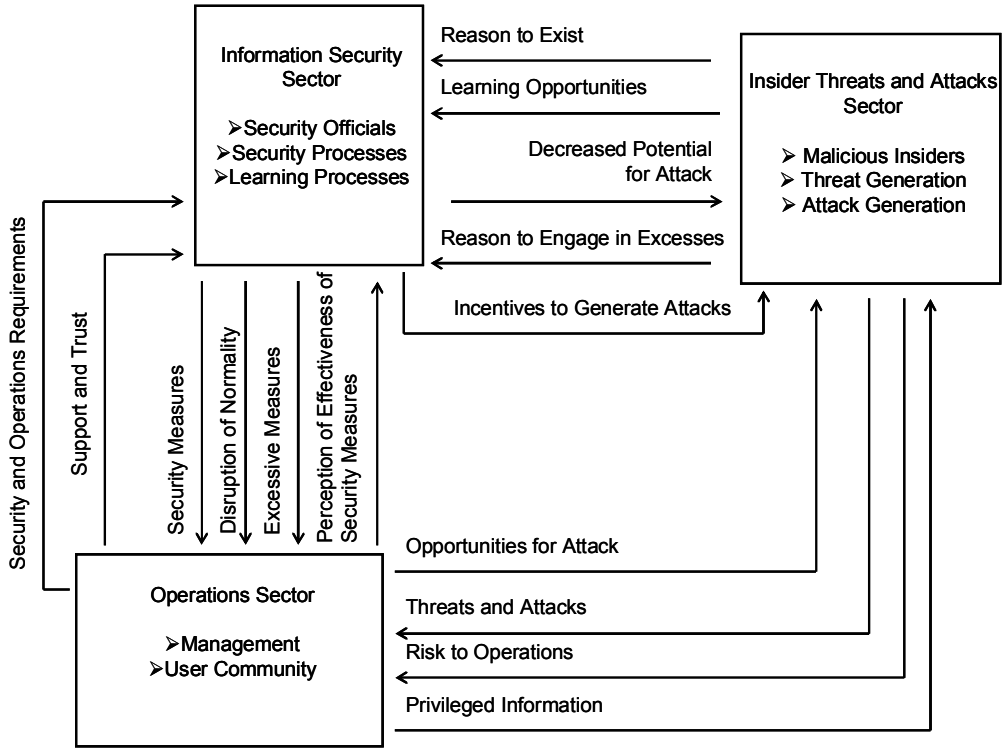

Figure 2. Sector overview

The model captures three main processes: the implementation of security measures, creation of excessive security measures, and gathering of knowledge about the system by the members of the security department in charge of implementing security measures to protect information assets (the learning process). These processes are interconnected and are part of the same complete causal structure that embodies the representation of a prototypical security implementation process.

4.2 Implementation of security measures

The first area of the model deals with the operation and implementation of security measures. Figure 3 shows part of the military operations model developed by Burke et al. [3], in which, as a result of conducting operations in the field, insurgents' potential for attacks is weakened, influencing the number of attacks that can be carried out by insurgents and, consequently, influencing the need for troops on the field and the ultimate number of troops available for operations.

Figure 4 shows the causal structure that captures the implementation of security measures and its social impact in the case of insider threat and attacks in the context of security operations. As can be observed in Figure 4, the structure follows that of the military operations model, as

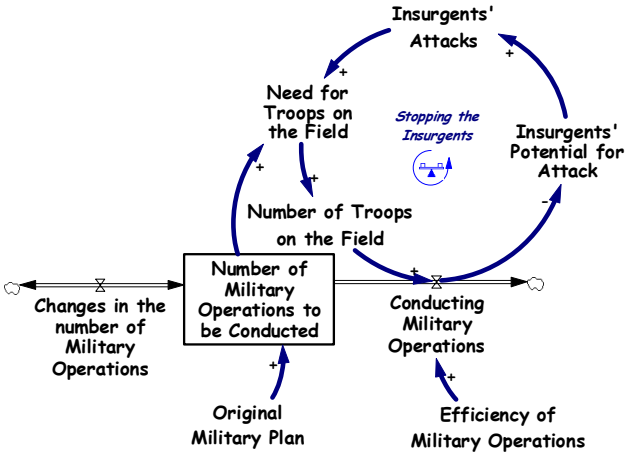

Figure 3. Partial insurgency model structure

these two contexts share the same underlying mechanisms related to how attacks are stopped by means of conducting and implementing special operations adequate for those contexts.

The main focus of information security is to ensure the order and stability of an organization or a system by minimizing attacks, coming from both inside and outside sources, which may lead to disruptions. Although the ideal case is to prevent all attacks, this can be difficult and

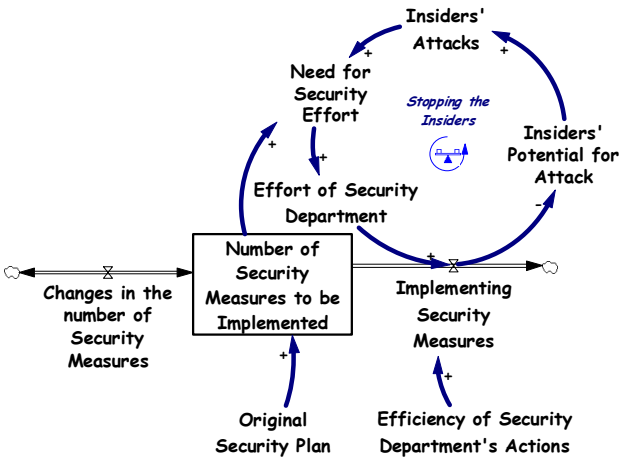

Figure 4. Implementation of security measures

not cost effective since the cost of security might be greater than the likely consequences of small-scale attacks. Organizations have either implicitly or explicitly stated thresholds that guide their efforts to discern when action is warranted [22-24]. A joint U.S. Secret Service and CERT Coordination Center study on actual insider crimes [29] discusses how managers' decisions geared to enhancing productivity and performance in organizations unintentionally increase the risk of insider attacks [1, 29].

In our model, the organization has a security plan. This security plan describes the number and types of measures needed to be taken to prevent insider attacks. In some cases, these plans include provisions mandated by law. For example, legislation such as the Sarbanes-Oxley Act of 2002 and the Health Insurance Portability and Accountability Act of 1996 mandate that organizations implement measures to ensure security and privacy of information [38-40].

In the model, the information security department implements security measures to decrease the level of insider attacks by decreasing the attackers' potential for attack or the exploitable vulnerabilities of the system (see "stopping the attacks" loop in Figure 4). As more security measures are implemented, less potential for inside attack is available, so the number of actual insider attacks is decreased.

As insider attacks decrease, the perceived need for security-related effort decreases, bringing the implementation of security measures down. The inherent need for security-related effort, however, is not likely to change. This feedback mechanism has a balancing effect because the result of implementing security measures, when successful, is a decreased perceived need for them over time. Security measures decrease the potential for inside attack; for example, the ability to have unauthorized access to files or systems and the possibility to guess other users' access codes can be counted as resources for insider attacks. Security measures restrict these abilities or decrease the possibilities of using these against the organization. Decreasing the potential for insiders to attack decreases the number of insider attacks. Additionally, Figure 5 shows that the implementation of security measures is a function of the effort exerted by the information security department (people) and their efficiency in the use of resources.

Increased insider attacks require more security measures to be taken, which can be done by having more information security professionals or higher efficacy in the use of resources. Increase in effort will help the organization implement more measures, resulting in less successful attacks over time. In addition, as insider attacks create disruptions in the order and stability of the information infrastructure of the organization, making the perceived level of threat to the system higher, new security measures are taken to close the information security gaps in the system. In successful cases, added security measures are of capable preventing insider attacks and additional disruptions in the system.

The implementation of security measures, however, also disrupts the normality of the operations in the organization, decreasing the support of management and the user community.

As Davis and Silver [7] identified in their post-9/11 investigations, high perceived levels of threat to the system increase the support of management and users for security departments' actions when a high level of trust in the security department exists. Since information security is the responsibility of the whole organization, not just the information security department, keeping this support level high is crucial for the department.

When the system is threatened due to insider attacks, and the level of trust in the security department is low, the support of management and of the user community can decline and create potential security risks and system vulnerabilities [7]. A decline in support for information security initiatives may lead users to neglect their roles in information security and engage in actions such as not locking their computer systems while away from them, sharing passwords with others, opening unsafe attachments to emails, etc. (like sharing their passwords with others). A recent survey indicates that 50% of users write down their passwords and 33% share them with others in the organization on a regular basis.

Management and users who support the information security department increase the likelihood of success against insider attacks by not allowing opportunities to arise for malicious insiders to exploit.

The support of the user community influences the trust in the security department's actions, which, in turn, positively influences the support of the user community,

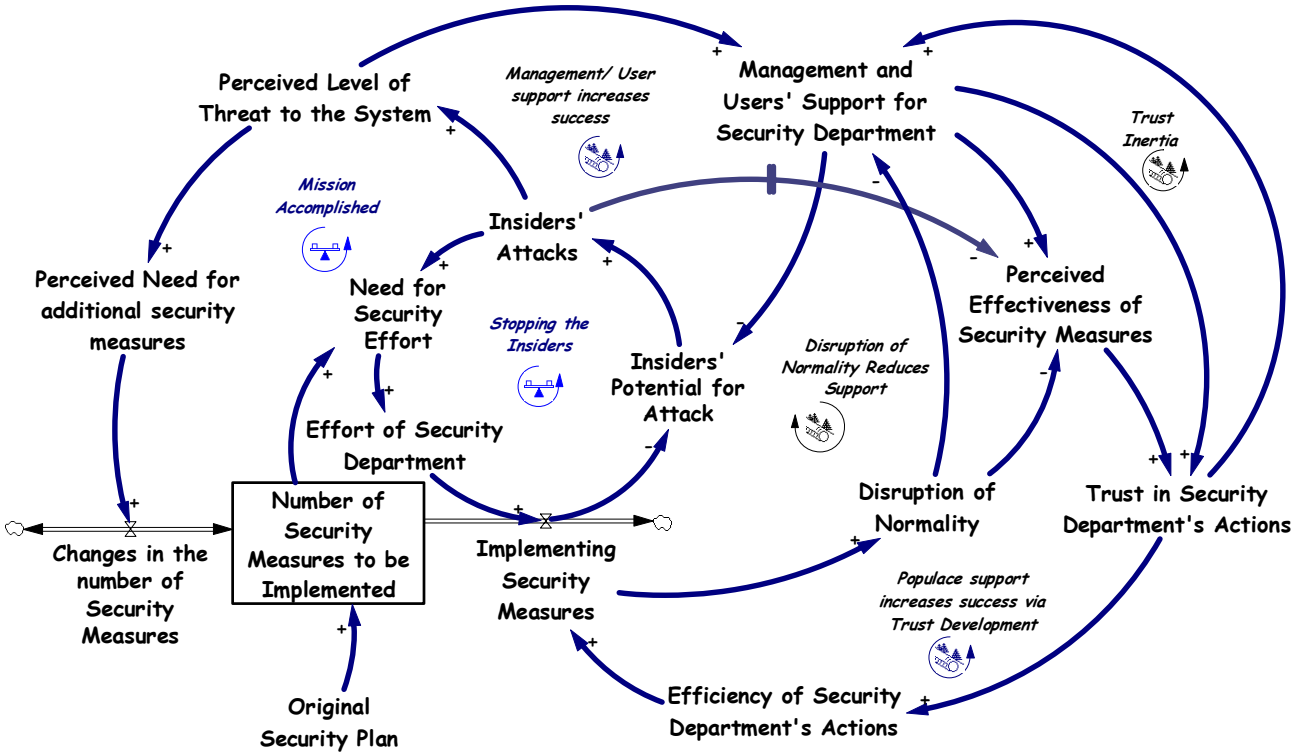

Figure 5. Expanded causal mechanisms

creating a reinforcing cycle of increasing trust. However, this same cycle can turn into a spiral of declining trust under adverse circumstances in the organization. Management and users' support will increase trust in the department's actions, yielding higher efficiency in the implementation of security measures.

4.3 Excessive security measures

Increases in insider attacks lead to decreased order and stability in the organization and to higher perceived levels of threat to the system. Increased insider attacks also decrease the perceived effectiveness of the security measures implemented, which has an effect on the level of trust in the security department actions that management and the user community have. Decreased levels of perceived effectiveness of security measures influence the perceived need and willingness to engage in excessive security measures to be able to contain the attacks experienced, which increases the number of excessive security measures. When excessive security measures grow, the perception of security measures in use as being excessive also grows, decreasing management and user support as well as trust in the security department. This creates the conditions for increased risk and vulnerability. However, under conditions of high trust and a high perceived level of threat to the system, the use of excessive security measures can potentially be perceived by management and the user community as necessary, and measures will be implemented adequately, creating more secure conditions in the system. Figure 6 shows the causal structure that potentially explains the existence of excessive security measures in organizational systems.

Requiring multiple passwords to access data, forcing users to have complex password combinations, and long procedures to gain access to different levels of data can be counted as normal security measures. Excessive measures could be conceived as applying the previously listed measures in an unnecessary, extremely burdensome, coercive manner. For example, instead of having one letter, one character, and one number in an eight-character-minimum password, forcing users to have more complex and longer passwords, such as 20 characters minimum, can be identified as excessive.

Although to many, excessive security measures provide sound solutions to the insider threat, this type of measure also may become part of the problem by decreasing the efficiency of the organization, disrupting normal operations, and making management and user support for the department dubious. Excesses by themselves disrupt the order of the organization and inconvenience management and users. Losing credibility

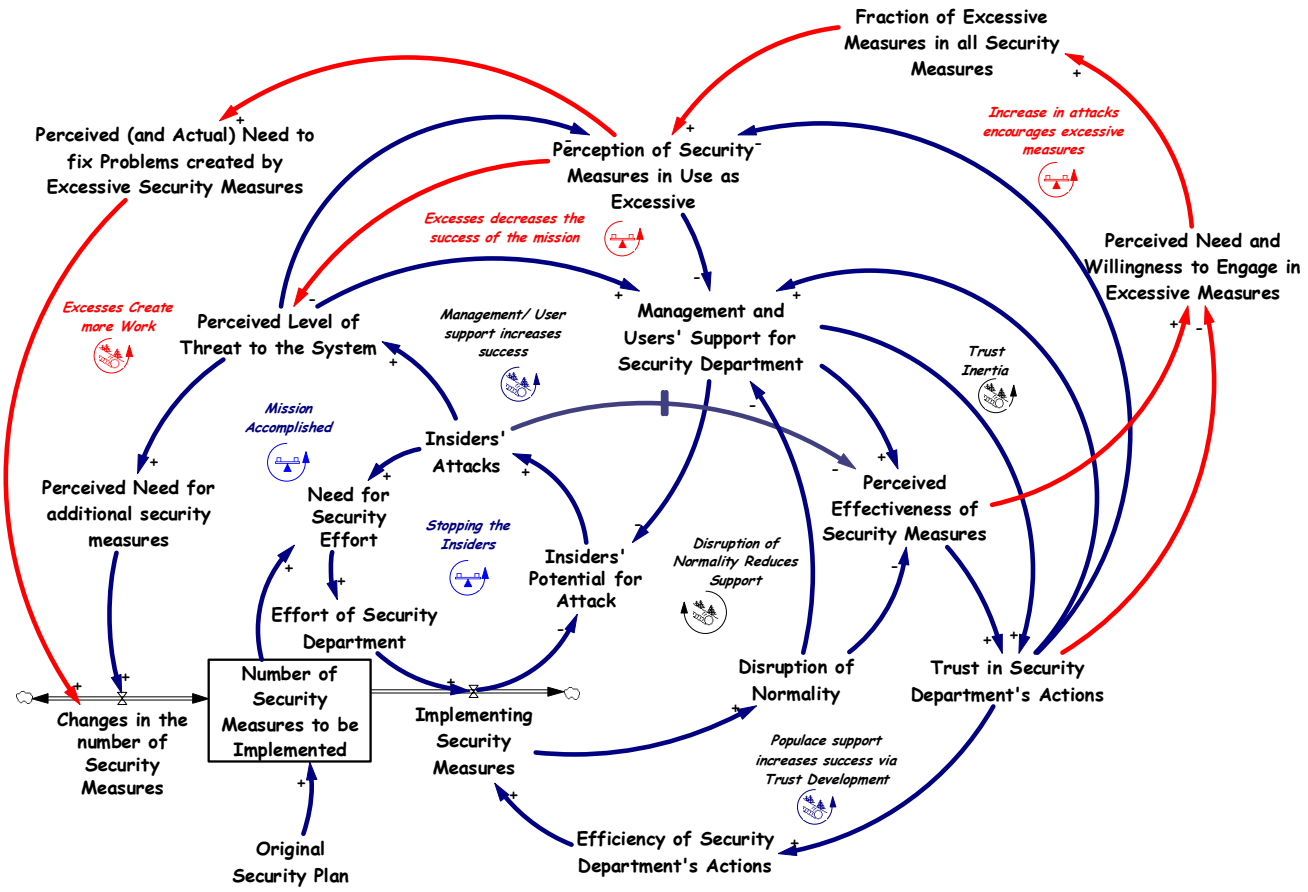

Figure 6. Excessive security measures

and trust will lead members of the information security task force to make mistakes, reducing their efficiency in the use of resources and causing implementation failures that lead to a higher risk of insider attacks. Furthermore, reduced efficiency in implementing security measures can lead to a higher risk of system vulnerability and to additional excessive security measures to try to solve the problems generated.

Excessive security measures, in combination with low levels of trust in the security department's actions, have the potential to create problems, such as users leaving their systems open while unattended or users writing their extremely complex passwords in papers and putting them next to their monitors, allowing for eroded system security and higher system vulnerability. In order to fix these problems created by excessive security measures, changes in the security plan are warranted, requiring additional effort in the design and implementation of new security measures.

4.4 Knowledge gathering

Implementing security measures allows knowledge to be generated via experience. Our model captures this learning process with a learning-by-doing mechanism. The right-hand side of Figure 7 shows the causal structure of this process.

A crucial element of an efficient information security process is the accumulation of the necessary knowledge about the system and about the problems existent in it.

Implementing security measures gives information security specialists opportunities for gathering knowledge through experience. As more implementations are conducted, more knowledge can potentially be gathered. This process is the basis of learning-on-the-job and of learning-by-doing theories of organizational training and improvement.

Accumulated knowledge about the system, its vulnerabilities, and its inherent problems helps increase

the efficiency of the security department's resources, leading to enhanced implementation of security measures. Better implementation of security measures leads to an even higher level of knowledge, closing a crucial reinforcing cycle that can be an engine of continuous security improvement over time.

Management and users play a crucial role in knowledge generation by providing adequate and timely feedback to information security officers. Most of the time, there are champion users who are proactive in informing system administrators about system issues and problems. Increased user support increases the availability of user knowledge to the information security department making knowledge gathering and accumulation an easier endeavor. This important source of knowledge helps the security department gather knowledge about the process of implementation and about actual and potential problems and vulnerabilities in the system. Cooke [6] stresses the crucial role of learning in security systems (specifically from incidents) when he indicates that "failure to learn from precursor incidents is a ubiquitous trait in all kinds of safety and security problems" [6, p. 140].

The existence of trained security specialists is a very important element of the knowledge gathering process. Trained specialists have better chances to recognize critical success factors and, due to their training, are likely to be more responsive to the available information and communicate better with management and users than other professionals.

Even excessive security measures contribute to the knowledge gathering process. Implementation of excessive security measures generates knowledge about the results of such implementations that contributes to the overall knowledge about the system available for future implementations. Excessive security measures, however, decrease management and user support, hurting the security department's credibility and thus decreasing its efficiency. Additionally, declining levels of support from managers and the user community decrease their availability and willingness to provide actionable knowledge and feedback, thereby hurting the knowledge gathering process.

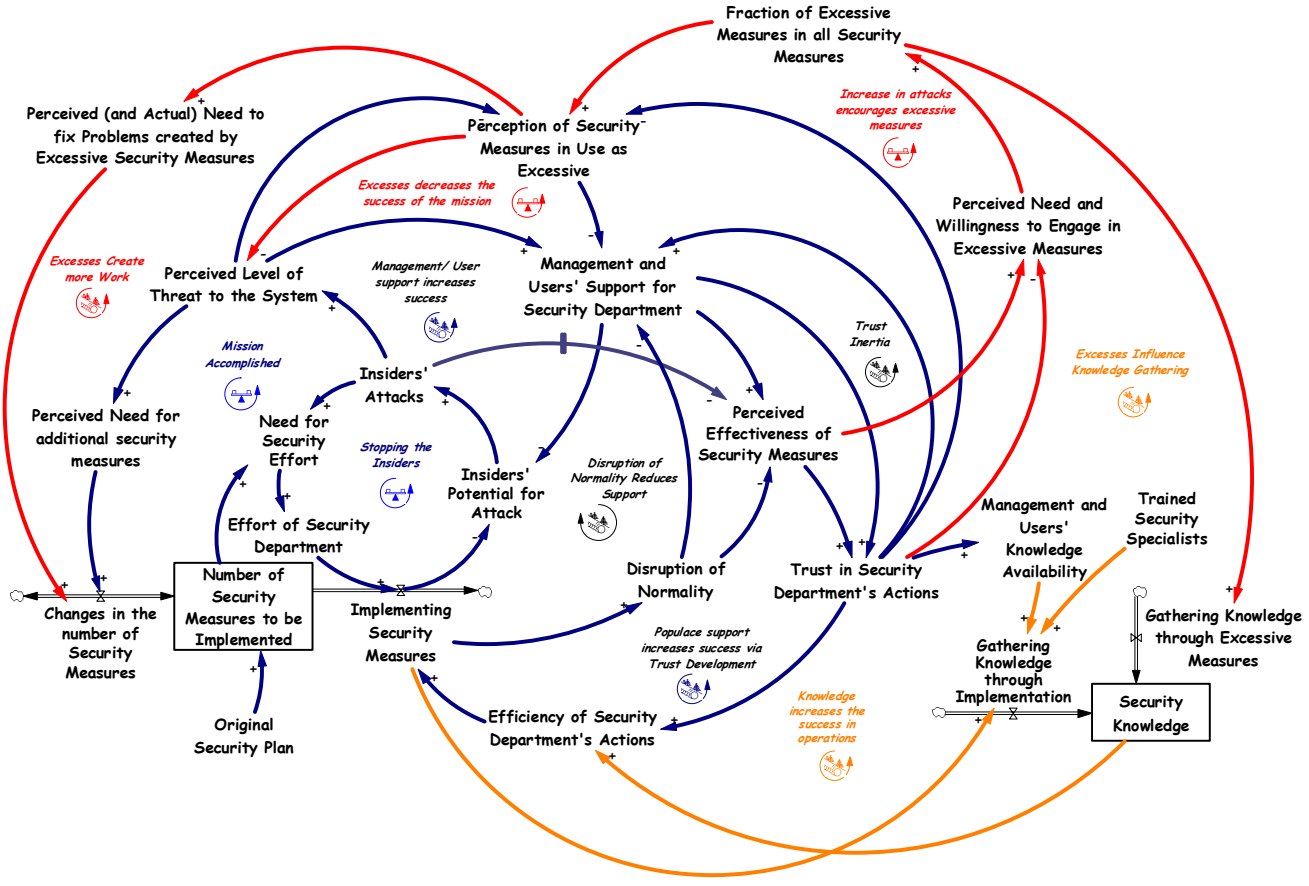

Figure 7. Knowledge gathering

5. Conclusions

Protecting the information infrastructure in organizations is embedded in a feedback-rich set of interactions. In our work, the existence of reinforcing mechanisms in management and user support and in knowledge gathering and accumulation as sources of success in implementing security initiatives seems central. Additionally, the realization that the implementation of security measures is embedded in an extremely rich social environment that triggers reactions that can lead to excesses in security measures is illuminating. Excesses in security measures can cause minor problems or become major roadblocks for productivity and security. Additionally, a reinforcing process of excessive security measures that generates added problems and work and lead to the addition of more excessive security controls could explain the experience of several organizations that resorted to adding security, with disastrous results.

Success in implementing security measures leads to decreased insider attacks and to a decreased perceived need for security, which creates a balancing mechanism that prevents continued investment in security measures and vigilance in organizations unless attacks are evident. This process can lead to an organizational trap—a success trap—that, if left unchecked, can potentially drive organizations to higher levels of vulnerability [for a description of other security-related organizational traps identified, see Ref. 1].

The model presented here integrates operations, decision making, and learning theories to provide an integrated framework with which to behaviorally approach the study of insider threats in the context of information security implementation.

Acknowledgments

This work was funded in part by the U.S. Department of Homeland Security. This article has been created by UChicago Argonne, LLC, Operator of Argonne National Laboratory (“Argonne”). Argonne, a U.S. Department of Energy Office of Science laboratory, is operated under Contract No. DE-AC02-06CH11357. The U.S. Government retains for itself, and others acting on its behalf, a paid-up, nonexclusive, irrevocable worldwide license in said article to reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, by or on behalf of the Government.

References

[1] Andersen, D. F., D. Cappelli, J. J. Gonzalez, M. Mojtahedzadeh, A. Moore, E. Rich, J. M. Sarriegui, T. J. Shimeall, J. Stanton, E. Weaver, and A. Zagonel. "Preliminary System Dynamics Maps of the Insider Cyber-threat Problem". Paper read at the *Proceedings of the 22nd International Conference of the System Dynamics Society*, Oxford, UK, 2004.

[2] Briney, A. *The 2001 Information Security Industry Survey* 2002 [cited October 20 2002. Available from http://www.infosecuritymag.com/archives2001.shtml#october2001.

[3] Burke, J. F., I. J. Martinez-Moyano, and B. K. Akcam. 2007. Modeling National Security Changes from Military Operations: CT Scan Overview. In *75th Military Operations Research Society Symposium*. Annapolis, MD.

[4] Bush, B. W., L. R. Dauelsberg, R. J. LeClaire, D. R. Powell, S. M. DeLand, and M. E. Samsa. 2005. Critical Infrastructure Protection Decision Support System (CIPDSS) Project Overview. In *Proceedings of the 23rd International Conference of the System Dynamics Society.* Boston, MA.

[5] Camerer, C., and T.-H. Ho, "Experienced-Weighted Attraction Learning in Normal Games", *Econometrica*, 67 (4), 1999, pp. 827-874.

[6] Cooke, D. L., "A System Dynamics Analysis of the Westray Mine Disaster", *System Dynamics Review*, 19 (2), 2003, pp. 139-166.

[7] Davis, D. W., and B. D. Silver, "Civil Liberties vs. Security: Public Opinion in the Context of the Terrorist Attacks on America", *American Journal of Political Science*, 48 (1), 2004, pp. 28-46.

[8] Dhillon, G., "Violation of Safeguards by Trusted Personnel and Understanding Related Information Security Concerns", *Computers and Society*, 20 (2), 2001, pp. 165-172.

[9] Dhillon, G., and S. Moores, "Computer Crimes: Theorizing about the Enemy Within", *Computers and Society*, 20 (8), 2001, pp. 715-723.

[10] Erev, I., "Signal Detection by Human Observers: A Cutoff Reinforcement Learning Model of Categorization Decisions under Uncertainty", *Psychological Review*, 105, 1998, pp. 280-298.

[11] Erev, I., D. Gopher, R. Itkin, and Y. Greenshpan, "Toward a Generalization of Signal Detection Theory to N-Person Games:

The Example of Two-Person Safety Problem", *Journal of Mathematical Psychology*, 39, 1995, pp. 360-375.

[12] Forrester, J. W., *Industrial Dynamics*, Productivity Press, Cambridge MA, 1961.

[13] Gonzalez, J. J., ed. *From Modeling to Managing Security: A System Dynamics Approach*. Høyskoleforlaget / Norwegian Academic Press. Kristiansand, Norway. 2003.

[14] Gonzalez, J. J., and A. Sawicka. "Modeling Instrumental Conditioning -- The Behavioral Regulation Approach". Paper read at the *36th Hawaii International Conference on System Sciences (HICSS 36)*, Big Island, Hawaii, 2003.

[15] ———. "The Role of Learning and Risk Perception in Compliance". In *From Modeling to Managing Security: A System Dynamics Approach*, edited by J. J. Gonzalez. Høyskoleforlaget / Norwegian Academic Press. Kristiansand, Norway. 2003.

[16] Hammond, K. R., *Judgments under Stress*, Oxford University Press, New York, NY, 2000.

[17] Klayman, J., "Learning from Feedback in Probabilistic Environments", *Acta Psychologica*, 56, 1984, pp. 81-92.

[18] ———, "Cue Discovery in Probabilistic Environments: Uncertainty and Experimentation", *Learning, Memory, and Cognition*, 14 (2), 1988, pp. 317-330.

[19] ———. "On the How and Why (Not) of Learning from Outcomes". In *Human Judgment: The SJT View*, edited by B. Brehmer and C. R. B. Joyce. Nort-Holland. Amsterdam. 1988.

[20] Kolb, D. A., *Experiential Learning: Experience as the Source of Learning and Development*, Prentice-Hall, New York, 1984.

[21] LeClaire, R. J., and G. O'Reilly. 2005. Leveraging a high fidelity switched network model to inform a SD model of the telecommunications infrastructure. In *Proceedings of the 23rd International Conference of the System Dynamics Society*. Boston, MA.

[22] Martinez-Moyano, I. J., S. H. Conrad, and D. F. Andersen. "An Outcome-based Learning Model to Identify Emerging Threats: Experimental and Simulation Results". Paper read at the *40th Annual Hawaii International Conference on System Sciences (HICSS'07)*, Hawaii, HI, 2007.

[23] Martinez-Moyano, I. J., E. H. Rich, S. H. Conrad, and D. F. Andersen. "Modeling the Emergence of Insider Threat Vulnerabilities". Paper read at the *Winter Simulation Conference*, Monterrey, CA, 2006.

[24] Martinez-Moyano, I. J., E. H. Rich, S. H. Conrad, D. F. Andersen, and T. R. Stewart, "A Behavioral Theory of Insider-Threat Risks: A System Dynamics Approach", *Transactions on Modeling and Computer Simulation*, Forthcoming, pp. 1-36.

[25] Martinez-Moyano, I. J., E. H. Rich, S. H. Conrad, T. Stewart, and D. F. Andersen. 2006. Integrating Judgment and Outcome Decomposition: Exploring Outcome-based Learning Dynamics. In *International Conference of the System Dynamics Society*. Nijmegen, The Netherlands.

[26] Melara, C., J. M. Sarriegui, J. J. Gonzalez, A. Sawicka, and D. L. Cooke. "A System Dynamics Model of an Insider Attack on an Information System". In *From Modeling to Managing Security: A System Dynamics Approach*, edited by J. J. Gonzalez. Høyskoleforlaget AS - Norwegian Academic Press. Kristiansand, Norway. 2003.

[27] Mitnick, K. D., and W. L. Simon, *The Art of Deception : Controlling the Human Element of Security*, Wiley Publishing, Indianapolis, IN, 2002.

[28] Powell, D. R., J. Fair, R. J. LeClaire, L. M. Moore, and D. R. Thompson. 2005. Sensitivity Analysis of an Infectious Disease Model. In *Proceedings of the 23rd International Conference of the System Dynamics Society*. Boston, MA.

[29] Randazzo, M. R., M. Keeney, E. Kowalski, D. Cappelli, and A. Moore. 2004. Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector: CERT and the National Threat Assessment Center.

[30] Rich, E., I. J. Martinez-Moyano, S. Conrad, A. P. Moore, D. M. Cappelli, T. J. Shimeall, D. F. Andersen, J. J. Gonzalez, R. J. Ellison, H. F. Lipson, D. A. Mundie, J. M. Sarriegui, A. Sawicka, T. R. Stewart, J. M. Torres, E. A. Weaver, J. Wiik, and A. A. Zagonel. "Simulating Insider Cyber-threat Risks: A Model-based Case and a Case-based Model". Paper read at the *International Conference of the System Dynamics Society*, Cambridge, MA, 2005.

[31] Richardson, G. P., and A. L. Pugh, III, *Introduction to System Dynamics Modeling with DYNAMO*, Productivity Press, Cambridge MA, 1981.

[32] Samsa, M. E., D. R. Powell, R. LeClaire, Y. Chang, P. Klare, I. J. Martinez-Moyano, S. Folga, and S. M. DeLand. 2007. CIPDSS Chemical Threat Capabilities Case Study: Summary Report. In *LA-UR-07-2382*. Los Alamos, NM: Los Alamos National Laboratory.

[33] Schneier, B., *Secrets and Lies: Digital Security in a Networked World*, John Wiley & Sons, New York, NY, 2000.

[34] Schultz, E., "A Framework for Understanding and Predicting Insider Attacks", *Computers and Society*, 21 (6), 2002, pp. 526-531.

[35] Schultz, E., and R. Shumway, *Incident Response: A Strategic Guide to Handling System and Network Security Breaches*, New Riders, Indianapolis, IN, 2001.

[36] Senge, P. M., *The Fifth Discipline: The Art and Practice of the Learning Organization*. Revised edition, Currency Doubleday, New York, NY, 2006.

[37] Sterman, J. D., *Business Dynamics: Systems Thinking and Modeling for a Complex World*, Irwin McGraw-Hill, Boston MA, 2000.

[38] United States House of Representatives, *Health Insurance Portability and Accountability Act*, United States Government Printing Office, Washington, 2002.

[39] United States House of Representatives Committee on Financial Services, *The Corporate Accountability, Responsibility, and Transparency Act of 2002*, United States Government Printing Office, Washington, 2002.

[40] ———, *Sarbanes-Oxley Act*, United States Government Printing Office, Washington, 2002.