Association for Information Systems
AIS Electronic Library (AISeL)

ICIS 2003 Proceedings

International Conference on Information Systems (ICIS)

December 2003

The Dynamics of Organizational Information Security

Amitava Dutta
George Mason University

Rahul Roy
Indian Institute of Management Calcutta

THE DYNAMICS OF ORGANIZATIONAL INFORMATION SECURITY

Amitava Dutta
School of Management
George Mason University
Fairfax, VA USA
adutta@gmu.edu

Rahul Roy
Management Information Systems Group
Indian Institute of Management Calcutta
Calcutta, India
Rahul@iimcal.ac.in

Abstract

In recent times, it has become evident that information security is not achieved through technology alone. Rather, it depends on a complex interplay among technology, organizational and managerial issues, and events in the external environment. Senior management attention, training, and sound operating procedures are just as important as firewalls and virtual private networks in arriving at a robust security posture. In this paper, we represent the interactions among these technical and organizational drivers using the system dynamics methodology, to develop a high level model of organizational information security. Since the basic system dynamics construct is the feedback loop, our model is able to expose the counteracting mechanics that work to reinforce and erode security, respectively. By doing so, it can inform the process of crafting an appropriate level of security—a problem facing most organizations. Since the model is based on simulation, it is also possible to test what-if *scenarios of how the security posture of the organization would fare under different levels of external threats and management policies.*

Keywords: Information security, system dynamics, policy modeling

Introduction

With the rapid diffusion of Internet-based commerce, accompanied by rising incidences of cybercrime, information security concerns have now reached the boardrooms of many, if not most, organizations. Losses from operational disruptions, loss of customer confidence, and liability resulting from information security incidents (Garg 2003; Sager and Greene 2002) are prompting management to investigate ways to craft an appropriate security posture that balances costs and benefits. In order to do so, it helps to understand the mechanics by which information security is eroded or reinforced in organizations. Management can then take steps to weaken the former and strengthen the latter to strike an appropriate balance. This paper takes a step in that direction by developing a high level model of information security that exposes the underlying mechanics.

It is useful to begin by noting that organizations' view of information security has evolved over time. For the longest time, information security was viewed by management as largely a technology issue (von Solms 2001). The solution was seen as one of selecting appropriate hardware and software components and designing an architecture to protect the information assets of the organization. Hence, it was seen as a responsibility of the IT department, and security expenditures were deemed a necessary evil. This emphasis on technology solutions still remains. However, over time, it became evident that technology solutions must be complemented with appropriate organization structure, management policies, and strategy in order to be effective (Hone and Eloff 2002). For instance, the best firewall offers little protection unless employee termination procedures include an *immediate* termination of all information access privileges. It is not uncommon for employee access rights to remain active long after they have left an organization, or for employees to divulge sensitive information over the phone, bypassing secure firewalls (Mitnick 2003). Proper background checks, ongoing security training and awareness programs, and senior management support are all needed in addition to technology (Nosworthy 2000). In short, the prevailing view of organizational information security is moving to a position that recognizes it to be an outcome of the interaction between technology and organizational factors.

That said, the practitioner literature also makes it clear that, independent of understanding the drivers of information security, deciding on an appropriate level of effort and making the business case for it continues to be a challenge for senior management (Gordon and Loeb 2002). By exposing the underlying mechanics, our model can help on both fronts: understanding how organizational and technology factors interact to help or hinder information security and examining the consequences of different management policy options and external conditions to help make the business case.

The remainder of the paper is organized as follows. The next section reports the structure of our model of information security as it currently stands and discusses some the mechanics that are inherent in its structure. The third section reports results of initial experimentation with the model and discusses the findings. Since this is work in progress, in the fourth section we conclude with a discussion of the directions in which the model will be enhanced and subsequent plans for experimentation in order to learn more about the dynamics of organizational information security.

A Holistic Model of Information Security

We now proceed to develop a model of organizational information security. As noted above, the model has at least one objective: exposing the underlying mechanics. In order to understand the mechanics underlying any behavior, we first need to capture the overall cause and effect structure among the variables that are deemed relevant to that behavior. Thus, to understand the mechanics of flight, it is necessary to know the cause-and-effect relationships among wing surfaces, airflow, weight, air pressure, and lift. In the same vein, we attempt to capture cause-and-effect relationships among variables relevant to organizational information security. As with any model, the level of detail is determined by the intended use. In our case, the model is targeted at senior management to aid in their decision-making. Thus, the variables are at a level that reflects relevant aggregate properties of organizations and the external environment.

A variety of methods are available for representing dynamic processes. We have chosen system dynamics (Richardson 1999) for the following reasons. The main structural element in a system dynamics model is the feedback loop, making it well suited for capturing the interaction among different drivers of security. System dynamics can represent quantifiable as well as "soft" variables, which is useful since the security context has both social and technical aspects. Delays can also be modeled, and this is needed to represent certain social mechanisms. Moreover, system dynamics models can be simulated, providing a platform on which to test scenarios for policy analysis.

The basic premise in system dynamics is that system behavior results from interaction among its feedback loops. Model building begins with development of a causal loop diagram that consists of a collection of causal links, each having a certain polarity. A positive (negative) link implies a reinforcing (balancing) relation where a positive change in the cause results in a positive (negative) change in the effect. A double line intersecting a link represents delays in an effect. A causal loop is formed by a closed sequence of causal links. A negative feedback loop has an odd number of negative polarity links, while a positive loop has an even number of negative links. The causal loop graph can be mapped to a mathematical model consisting of a system of difference equations, which can be simulated under different parametric conditions.

Figure 1 shows our causal loop diagram for organizational information security. For visual convenience, when variables from Figure 1 are referenced in the narrative, they will be shown in italics. Space constraints prevent us from discussing every causal link in Figure 1. Only the major links and feedback loops will be discussed. The main variable of interest here is *security preparedness*. One can, conceptually, score an organization on a continuum of preparedness, the lowest point representing a situation where the organization has not taken even the most basic steps to ensure information security. There is no awareness of information security issues, no policies in place, no resources allocated to information security, and the technology infrastructure for information security is minimal. The highest score represents a situation where the organization has the proper people, technology, procedures, and policies in place, resulting in the strongest level of preparedness. For modeling purposes, the lowest and highest scores can be anchored at zero and one, respectively. Note that a preparedness level of one does not imply immunity to information security breaches. Total security is a myth. It is neither technologically possible nor economically viable (Quinn and Brill 2002). There will be breaches from time to time. Hence, notice the two causal links inbound to *rate of security incidents* in Figure 1 from *security preparedness* and *external threat level*. Their polarities are negative and positive, respectively, for reasons that are obvious from the definitions given above (e.g., as preparedness increases, rate of information security incidents should decrease, other factors remaining constant).

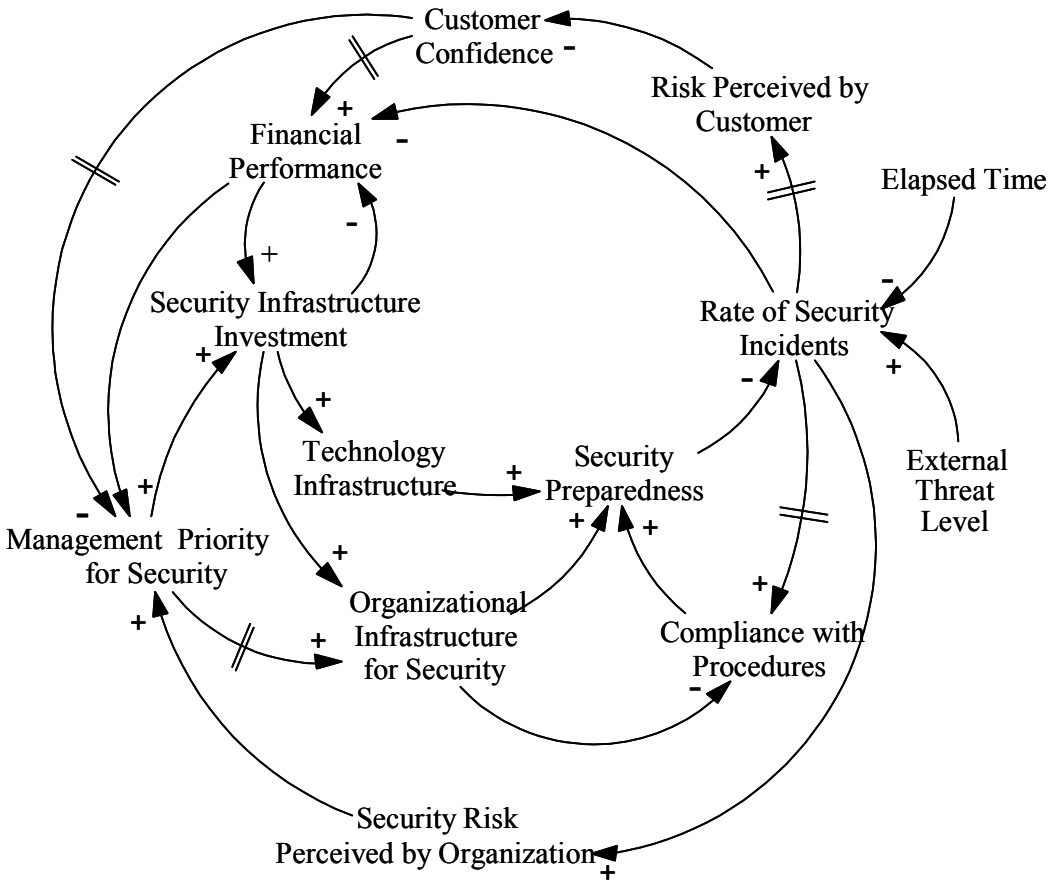

Figure 1. A Causal Model of Organizational Information Security

Customers have no way of knowing the internal security preparedness of an organization. Their perceptions of how vulnerable an organization might be are shaped by actual incidents of information security compromises. The more frequently they occur, the greater the perception of risk. However, by the same logic, when the frequency of incidents is low, the perception of risk is low. In fact, as more time elapses after an incident, the public's perception of risk also tends to wane. In other words, there is a natural decay in perceptions of risk, in the absence of security incidents. This perceptive decay is well documented in the literature (Battman and Klumb 1993; Gonzalez and Sawicka 2003), hence the negative link from *elapsed time* to *rate of security incidents*.

This risk perception on the part of customers has immediate effects that ultimately impact information security. First, increased *customer perception of risk* leads to reduced *customer confidence* (negative polarity link), which in turn leads to reduced *financial performance* (positive polarity link). This sequence of causal effects can be traced in Figure 1. The impact on financial performance is important for two reasons. First, it directly affects the organization's ability to allocate resources for information security, hence the positive link from *financial performance* to *security infra investment*. Second, financial performance is known to have a significant impact on *management priority for security*. In particular, during lean times, management is inclined to lower their priorities for information security. In short, *security infrastructure investment* is a function of the firm's ability to do so (financial performance), as well as the priority accorded to information security by management, hence the two inbound links into this variable in Figure 1. Apart from financial performance, there is also a positive link from actual *rate of security incidents* to the *security risk perceived by organization* and another positive link on to *management priority for security*. This is because information security breaches have the immediate effect of its increasing priority.

The remainder of the causal structure separates information security investments into technology and organizational infrastructure investment components, reflecting the contemporary realization that both are important for information security effectiveness.

Besides these two components, however, notice that the issue of compliance has also been explicitly represented. In general, a higher incidence of information security incidents makes organizational members more aware of vulnerabilities and results in a higher level of compliance with established security procedures. However, more stringent organizational security measures usually institute more burdensome procedures, which users tend to circumvent or ignore. Hence there are inbound links to *compliance with procedures* having both positive and negative polarities.

Humans are very good at identifying localized causal effects, but their ability to understand the behavior of long causal chains is limited (Richardson 1999). Therefore, having discussed cause-and-effect relations one at a time, it is useful to now step back and view the causal loop diagram more holistically in order to see the mechanics underlying information security. This can be done by identifying associated feedback loops, since it is the interaction among feedback loops that generates system behavior. To illustrate how the model can be used in this way to uncover mechanics, assume that *management priority for security* were to increase—due to an internal policy decision, for instance. Tracing the following loop in Figure 1, *management priority for security* $\Rightarrow^{+}$ *organizational infrastructure for security* $\Rightarrow^{+}$ *security preparedness* $\Rightarrow^{-}$ *rate of security incidents* $\Rightarrow^{-}$ *financial performance* $\Rightarrow^{+}$ *management priority for security,* and seeing the even number of negative links shows it to be a positive feedback loop. This loop shows a mechanism where management decision to increase priority unleashes a mechanism that encourages further increase in priority. However, consider the following loop *management priority for security* $\Rightarrow^{+}$ *security infrastructure investment* $\Rightarrow^{-}$ *financial performance* $\Rightarrow^{+}$ *management priority for security.* This is a negative feedback loop since there are an odd number of negative links. This loop says that management's decision to increase priority for security results in mechanics that discourage that move. So we can see counteracting forces at play here, and it is possible to identify additional feedback loops in the model of Figure 1. Nevertheless, the preceding exercise is sufficient to establish the ability of this modeling approach to expose some of the complex mechanics by which technology and organizational parameters interact to affect security. The practitioner literature contains ample evidence that while managers are keenly aware of the need to maintain customer confidence in their security measures, they are also under pressure to maintain financial performance of the firm—and security expenditures do not help on that dimension. Figure 1 exposes how these opposing forces affect information security through their respective feedback loops.

Experimental Results

A causal model such as Figure 1 is good at exposing the different feedback loops affecting information security. However, it is hard to informally reason through their interacting effects. This is where the simulation capability of system dynamics models becomes very useful. The causal loop structure of Figure 1 was converted to its equivalent structure using standard stock and flow constructs of system dynamics (Richardson 1999). In the remainder of this section, we report the results of initial simulation experiments with the model. The main intent is to show how the simulations give insights into the dynamics of organizational information security, i.e., how an organization's security posture changes over time in response to external conditions and/or management policies.

Figures 2 through 4 show graphical functions used in the model.

At this initial stage of research, we have chosen model parameters based on our intuitive understanding of the problem domain. Rather than numeric validation, the objective has been to validate the model in terms of the dynamics exhibited by its key variables. Note that in the causal loop diagram we have shown *external threat level* as an exogenous variable. We used a step function with volume of 0.4 for this variable to capture a situation where the external threat level suddenly increases, and watch how the organization—i.e., system—adjusts to the situation. Figure 6 shows variables representing system performance measures. Figure 7 shows behavior of key variables affecting the dynamics of the organization's security position.

In Figure 6, note that the external threat level remains steady at a constant level. *Security preparedness* of the organization, however, fluctuates over time. The *rate of security incidents* shows periods of sharp rise followed by periods of stabilization. As expected, the high rate of security incidents coincides with low security preparedness. *Customer confidence* levels fluctuate as well. It appears that even when *external threat level* is constant, the organization cycles through periods of high preparedness and vulnerability.

Figure 7 provides a peek into the inner mechanics of the system. It shows that while *organizational infrastructure* increases to a steady level, *compliance by employees* fluctuates in phase with security preparedness and *technology infrastructure* fluctuates with a phase lag. Note also the declining peak of *technology infrastructure* levels due to decreasing *financial performance* of the firm in the face of dwindling customer confidence.

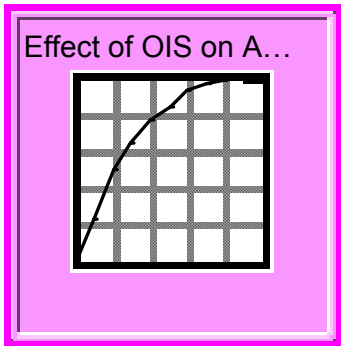

Figure 2. Relationship between Organizational Infrastructure for Security with Security Preparedness

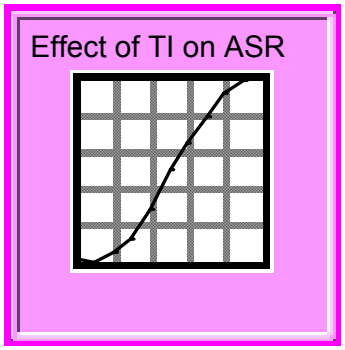

Figure 3. Relationship between Technology Infrastructure with Security Preparedness

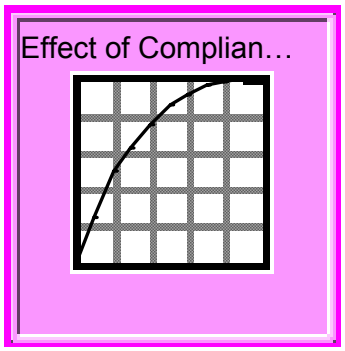

Figure 4. Relationship between Compliance with Procedure with Security Preparedness

Figure 5. Relationship between Security Incidents with Organizational Perception of Security

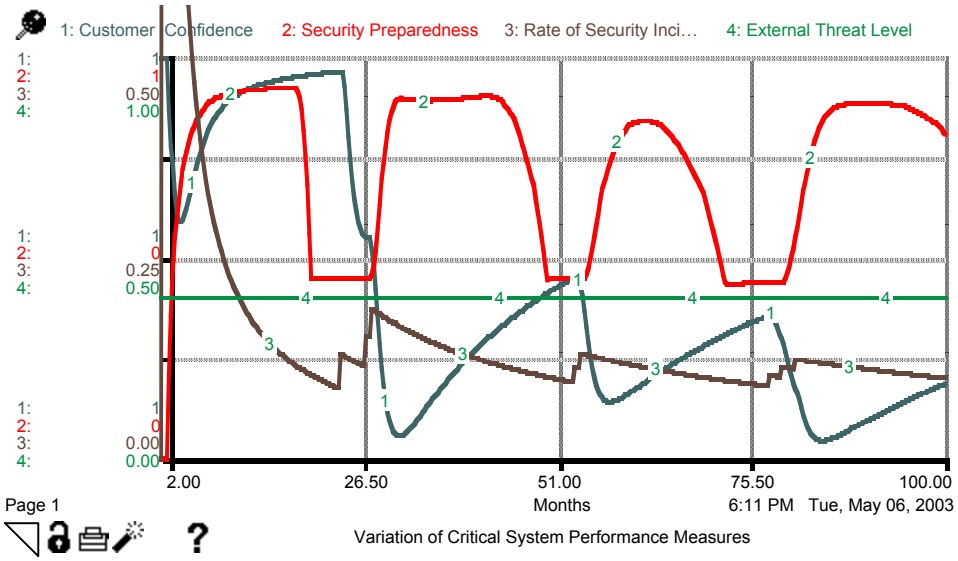

Figure 6. Behavior of System Performance Variables

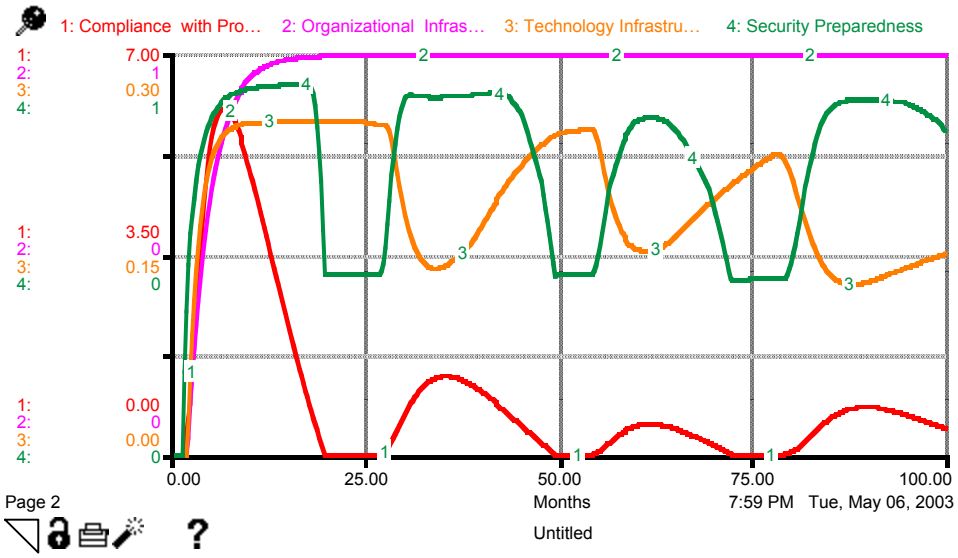

Figure 7. Behavior of Some Variables Affecting Security Preparedness

Given this kind of basic behavior, the model can be used for sensitivity analysis. In Figure 8 we show one such test, carried out under parameters representing closer monitoring of security incidents, better technology investment policy, and higher incentive to employees for adhering to organizational procedure. The results show definite improvement in *security preparedness*.

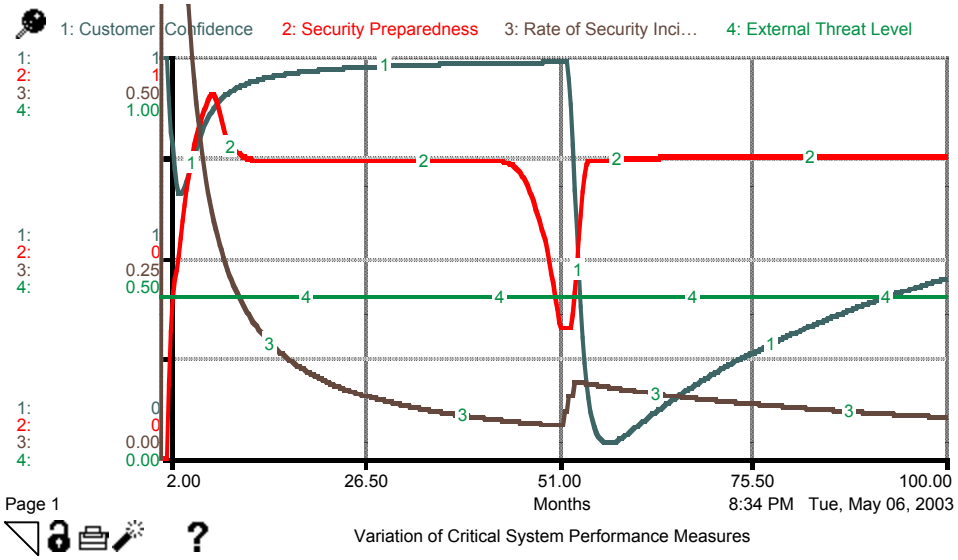

Figure 8. Results of Sensitivity Analysis

Extensions and Concluding Remarks

This paper reports on work in progress. The model in Figure 1 is our initial effort at capturing the major forces affecting organizational information security, from the standpoint of senior management. At this stage, some of the variables are, necessarily, coarse. Therefore, the first refinement will be to disaggregate some of the variables. For instance, *organizational infrastructure*

for security can be further refined into policy and structure components. Similarly *security infrastructure investments* can be disaggregated into investments in technology and organizational change. Apart from model refinement, we plan to compare the information security behavior predicted by the model to that in an actual organization. Independent of this modeling effort, we are conducting in-depth interviews with selected firms in the service sector to collect senior management's perceptions and plans in the area of information security. We plan to use the findings from our interviews to further refine model structure to lend greater confidence to the information security behavior it generates.

References

Battmann, W., and Klumb, P. "Behavioral Economics and Compliance with Safety Regulations," *Safety Science* (16), 1993, pp. 35-46.

Garg, A. "What Does an Information Security Breach Actually Cost: Evidence and Implications," *Information Strategy* (19:4), 2003, pp. 21-25.

Gonzalez, J. J., and Sawicka, A. "Origins of Compliance: An Instrumental Conditioning Perspective," *Proceedings of the 36th Hawaii International Conference on System Sciences*, IEEE Computer Society Press, Los Alamitos, CA, 2003.

Gordon, L. A., and Loeb, M. "Return on Information Security Investments: Myths vs. Realities," *Strategic Finance* (84:5), 2002, pp. 26-31.

Hone, K., and Eloff , J. H. P. "Information Security Policy: What Do International Security Standards Say," *Computers & Security* (21:5), 2002, pp. 402-409.

Mitnick, K. "Best Practice: Are You the Weak Link?," *Harvard Business Review* (81:4), 2003, pp. 18-20.

Nosworthy, J .D. "Implementing Information Security in the 21st Century: Do You have the Balancing Factors," *Computers & Security* (19:4), 2000, p. 337.

Quinn, L. R., and Brill, A. E. "Risky Business," *Journal of Accountancy* (193:6), 2002, pp. 65-70.

Richardson, G. P. "Reflections for the Future of System Dynamics," *The Journal of the Operational Research Society* (50:4), 1999, pp. 440-449.

Sager, I., and Greene, J. "Commentary: The Best Way to Make Software Secure: Liability," *Business Week*, March 13, 2002 (available online at **http://lists.microshaft.org/pipermail/dmca_discuss/2002-March/001238.html**).

Von Solms, B. "Information Security: A Multidimensional Discipline," *Computers and Security* (20:6), 2001, pp. 504-508.