Simulating Insider Cyber-Threat Risks: A Model-Based Case and a Case-Based Model

Eliot Rich **University at Albany** **State University of New York** **e.rich@albany.edu**	**Ignacio J. Martinez-Moyano** **University at Albany** **State University of New York** **im7797@albany.edu**	**Stephen Conrad** **Sandia National Laboratories** **shconra@sandia.gov**
Dawn M. Cappelli **CERT/CC** **Software Engineering Institute** **dmc@cert.org**	**Andrew P. Moore** **CERT/CC** **Software Engineering Institute** **apm@cert.org**	**Timothy J. Shimeall** **CERT/CC** **Software Engineering Institute, USA,** **tjs@cert.org**
David F. Andersen **University at Albany** **State University of New York** **david.andersen@albany.edu**	**Jose J. Gonzalez** **Agder University College** **Norway** **jose.j.gonzalez@hia.no**	**Robert J. Ellison** **CERT/CC** **Software Engineering Institute** **ellison@sei.cmu.edu**
Howard F. Lipson **CERT/CC** **Software Engineering Institute** **hfl@cert.org**	**David Mundie** **CERT/CC** **Software Engineering Institute,** **dmundie@cert.org**	**Jose Maria Sarriegui** **TECNUN** **University of Navarra** **Spain** **jmsarriegui@tecnun.es**
Agata Sawicka **Agder University College** **Norway** **agata.sawicka@hia.no**	**Thomas R. Stewart** **University at Albany** **State University of New York** **t.stewart@albany.edu**	**Jose Manuel Torres** **TECNUN** **University of Navarra** **Spain** **jmtorres@tecnun.es**
Elise A. Weaver **Worcester Polytechnic Institute** **eweaver@wpi.edu**	**Johannes Wiik** **Agder University College** **Norway** **johannes.wiik@hia.no**	

Corresponding Author: Eliot Rich, Department of Information Technology Management, School of Business, BA-310, University at Albany, State University of New York, 1400 Washington Avenue, Albany, NY 12222.

The growing reliance on technological infrastructures has made organizations increasingly vulnerable to threats from trusted employees, former employees, current or former contractors, and clients. Recent research indicates that successful defense from these threats depends on both technical and behavioral controls. In this paper, we report on our work to identify seemingly reasonable organizational actions that may inadvertently lead to increased risk exposure. We also consider how potential internal attackers may be encouraged or discouraged by monitoring the organization's responses to probes of its firm's security systems.

Two interwoven work products are presented: A case study that presents a particular type of insider threat – long-term fraud – and a simulation model that supports the case, the underlying dynamic theory, and examination of policy options. The case and model combine to produce a motivating and useful exercise that illustrates the problems of insider cyber-threats. This material has been used in teaching of insider threat issues with satisfactory results.

Keywords: *Cyber-threats, Simulation, Computer Security, Signal Detection Theory, Insider Threats*

1 Introduction to the Insider threat problem

Insiders working against their employers and colleagues have been a concern as long as there have been employers. For example, during the Middle Ages double-entry accounting was invented as a defense against dishonest accountants (Davies 1996). Military commanders turning traitor on the battlefield are infamous (for example, Norwich 1993, discusses the battle of Manzinert in 1071). Today, government and commercial organizations increasingly rely on inter-networked information systems to carry out services that are critical to business mission success. With this increased reliance comes increased exposure to malicious actions, particularly by individuals employed by the organization who have, or previously had, authorization for access to all or part of the organization's computing systems or infrastructure.

Unfortunately, the ultimate effects of business policy decisions on insider threat risks are often complex and sometimes counterintuitive, with short-term effects very different from long-term effects. The potential cascading effects and long-term consequences of personnel, policy, and technology decisions on the organizational culture and security posture are not always immediately evident.

1.1 Recent studies of Insider Threats

Evidence from a joint U.S. Secret Service and CERT Coordination Center (CERT/CC) study on actual insider cyber crimes indicates that managers, at times, make decisions intended to enhance organizational performance and productivity, but with the unintended consequence of magnifying the organization's exposure to and likelihood of insider cyber attack (Andersen, Cappelli et al. 2004; Randazzo, Keeney et al. 2004). Evolving legislation rooted in the Sarbanes-Oxley Act of 2002 holds public companies increasingly responsible for the actions of its employees that violate applicable laws and regulations (U. S. Congress 2002). The lack of methods and tools for analyzing and communicating insider threat risks and mitigations exacerbates the problem faced by business managers.

1.2 Detecting Insider Threats is difficult

There are no simple approaches to detecting insider threats before attacks begin, and no simple profiles to potential attackers (Randazzo et al., op. cit.). There appear to be any number of potential vulnerabilities to exploit, ranging from detailed knowledge of internal systems and controls to bad "security hygiene" – leaving passwords posted on monitors, sharing access codes, and other activities that simplify work activities under the assumption of good behavior. A recent vendor survey indicates that 50% of respondents write down their passwords, and about 33% share them with others in the organization, independent of repeated reminders to avoid such actions (Sturgeon 2005).

In the Internet-enabled business environment, there is little time to review transaction data. Yet, inaccurate judgment of risk can lead to frustration over nit-picking, and lackadaisical review can create a crisis, with false alarms raising protection efforts and costs (Wilmer 2002). Time constraints pit the economic reality of work pressure against the historically proven needs for controls and risk mitigation.

Another complication in detection can arise because a seemingly routine business activity may actually be a subtle attempt to probe the defensive structure of a firm. For example, a transaction posted to the wrong customer may be an error or may be an attempt at fraud, an ambiguity that might only be settled after losses have been suffered.

Changes in worker morale can also be an early signal of risk. Alert managers may observe gross shifts in behavior, such as workplace disruptiveness. More subtle changes in attitude are simply not noticed or are characterized as personality quirks or adjustment difficulties. Indeed, scrutiny of individual activities for possible security lapses may be seen as intrusive and oppressive intervention in most business environments. It has only been through intense and confidential forensic evaluations of historical attacks that such signals were seen as portents to threats.

1.3 The problems of confidentiality

Good data is crucial to all empirically driven research, and such data would greatly advance our understanding and mitigation of the insider threat problem. Unfortunately, relevant data on cyber-threats does not always exist, nor is existent data available, nor is available data without error or bias. Accordingly, the modeling of cyber systems must use a research strategy that can still deliver valuable insights despite the holes and deficiencies in the data material.

One of the difficulties in systematic modeling of cyber attacks arises from the unavailability of data regarding these attacks. While such attacks are increasingly frequent on networked systems, systematically collected data on these attacks is not generally available. This lack of availability stems from three basic causes: Attackers generally act to conceal their attacks; defenders gather data on attacks for narrow purposes; and organizations controlling information assets rarely share or preserve data on attacks. First, successful information attacks depend to some degree on deception and surprise – networks that are prepared or forewarned for specific attacks generally suffer little or no damage from them. Thus, attackers must conceal as much information as possible on their attacks in order to preserve the utility of their methods – not a difficult task for them since the Internet was devised for information exchange between trustworthy users (Lipson 2002). This situation results in incomplete data capture on the methods and objectives of attacks on information assets – with the notable exception arising from work on honeypots and honeynets (Spitzner 2003; The Honeynet Project 2004) [1].

Second, defenders of information assets are often overburdened. As such, they have little motivation for large-scale data collection activities. Data are generally collected only if useful for a specific defensive task, for forensic purposes or to document relevant damage for legal proceedings. A wide range of data formats is used in such data collection. The data are organized, not in a generically accessible database, but rather in formats specific to the use for which they are collected, making systematic survey of the data collected quite difficult and time intensive.

Third, attack data are often shared only in vague terms, if at all, by affected organizations. Sharing of information may be precluded by the rules of evidence in a criminal

[1] Honeypots and honeynets are two types of controlled and monitored computing environments used to entice and monitor attacker activity.

prosecution. In other cases, data on attacks may be withheld due to concerns over publicity, reputation, or worries about copycat activities. When detailed data are shared, they often become available only under restricted-use agreements or guarantees of confidentiality. As such, data that characterizes attacks across a broad range of organizations are rarely available to the research community.

Beyond these three aspects, cyber data that is reported to computer emergency response teams, such as CERT/CC, cannot be shared freely with other researchers – not even with collaborating researchers from other institutions. Data concerning malicious activity may be stored for a limited amount of time. When the owner of such information perceives it as no longer necessary, collected information may be disposed of in a secure manner to avoid negative publicity if the information is disclosed to the wrong audience. Consequently, the information cannot be retrieved again, even if the owner would have been willing to do so.

2 The current research agenda

This paper presents our progress on insider threat research. This effort has taken form through the identification of a multi-institutional research agenda that brings together computer scientists working on the practical problems of cyber-threats, behavioral theorists thinking about motivation and decision-making of would-be attackers, and security experts looking to understand and mitigate threats to national infrastructures. The mix of technology, behavior, and dynamic feedback makes this problem quite amenable to the techniques of system dynamics.

Through this collective agenda, we are working on instruments to understand and teach the lessons of insider threats, grounded both in behavioral theory and practical knowledge of industry practice and weakness. In this section we discuss the approach we have taken to develop our agenda. Later, we present the case study that was developed by this collective group, followed by the dynamic hypothesis that it supports, and a discussion of the simulation model.

In November 2004, CERT/CC hosted a three-day workshop on modeling insider threats that brought together experts in computer security and dynamic modeling. One of the goals for this meeting was finding a technique to integrate the real-world insights of the CERT/CC domain experts into a set of prototype models of threat dynamics. These insights were developed through analysis of insider attack data by CERT/CC staff, but the source data could not be released to the modeling team, for the reasons noted in section 1.3. Thus, we needed to consider a protocol to develop a model that was based on anecdotal evidence, sanitized and summarized by the domain experts. We also recognized that to advance our research there should be some single "story" for the model design; in the absence of real data, but with real stories, we could craft a case study that would illustrate the issues of insider threats and the dynamic hypotheses we suspected were in play.

On the second day of the workshop, the CERT/CC staff in attendance were asked to tell anecdotes about one class of insider threats which seemed to hold promise for modeling – long-term fraud perpetuated by insider efforts – based on their earlier review of dozens of attack cases. After some story telling, several key elements of the anecdotes emerged. The presence of an explicit, solitary attacker, who exploited known gaps in the information system; the lack of organizational response to initial tests of security, which in turn emboldened the attacker; the introduction of new actors into the organization that upset the interpersonal relationships and exposed the insider attacks. This approach preserved the confidentiality of the actual data and still preserved the dynamic insights surrounding insider attacks.

With these few concepts agreed on, the next step was to create a compelling, synthetic case that was based on real insights and motivations, The team broke up into four groups that independently advanced the "story", integrating elements of the dynamic theory that we had previously developed and reviewed, adding depth to the story that would make an engaging case. Each team presented their version of the case, and the group performed another synthesis exercise to decide exactly which dynamics the case should illustrate, and how these dynamics should be presented in a simulation model.

After the workshop ended, members of the team worked to develop both the case and the model. We realized that we had created two products: First, a "model-driven case," suitable for introducing security personnel to the organizational and behavioral issues that were critical to insider threats, and, second, a "case-driven model, " that helped expose the dynamics and structures that are the basis for our working hypothesis on the reasons that organizations remain vulnerable to these threats.

3 The case study: Insider Risks at AgPEX

This section outlines the fictional AgPEX case underlying the model: how three senior managers failed to detect and guard against the insider threat all the while seeming to pay proper attention to cyber-security measures at AgPEX.[2] It sets up the important conflicts that set the stage for the emergence of a disgruntled employee, the different perspectives of managers in the firm about security requirements and risks, and an attack vector that took advantage of insider knowledge to do harm.

> ***The AgPEX Situation***
>
> AgPEX, the Agricultural Product Exchange, is thriving on a simple idea. Modeled after the commercially successful eBay, AgPEX provides farmers, retailers, and wholesalers with geographically distributed market information that allows them to make arbitrage sales to maximize the efficiency of their overall inventory management[3]. AgPEX creates a market potential with an electronic presence and charges a small, but profitable, fee for this service.
>
> AgPEX is experiencing growing pains as it strives to move from its regional base in the mid-west to a national market. The company's founder hires both a new CEO and CIO to prepare the firm for its national debut. The new CEO understands that the integrity of AgPEX operations and the transactions that it facilitates are vital to keeping customers happy. If fraud or the suspicion of fraud were to become widespread or even rumored, AgPEX could suffer loss of volume and market share, making the whole business unprofitable. AgPEX's continued success relies on maintaining customer confidence

[2] The current version of the case is available from the corresponding author.

[3] Arbitrage is a market mechanism where sellers and buyers are brought together by a third party to negotiate immediate transactions. Typically, the facilitator receives a small percentage of the transaction as a fee for providing the information linking the parties.

through a corporate culture of teamwork to achieve very low rates of transaction error and fraud.

Sue Miller, the new CIO, has been trained to think in terms of risk assessment and management within the context of networked information systems. She understands that the greatest threats to AgPEX's long-term profitability may come from high impact but low probability attacks latent in the firm's environment. Unfortunately, analysis shows that AgPEX is infected with low but persistent levels of transaction errors and customer fraud. High rates of fraud and errors appear especially in transactions that contain (1) a high volume of product transfer, (2) high complexity as measured in number of customers involved in a split order, or (3) a high number of new customers. AgPEX's automated transaction monitoring system alerts managers of transactions involving any of these three indicators so that fraudulent and erroneous transactions are caught and handled before they cause problems.

Ian Thompson, the insider, has been with AgPEX working with the founder from the very start. For the past 8 years, he had managed the largest customer accounts, had shown the lowest rates of shipment and transaction error, and had set the standard for performance within the firm. Thompson was embittered by the course set for AgPEX by the newly hired CEO and CIO. Rather than being recognized for his many years of loyal and stellar performance, the CEO's much vaunted team-based approach had the basic effect of turning highly effective senior employees into tutors for inexperienced juniors. In turn, the most skilled employees were in essence penalized because their bonus performances depended on how well the least trained and least skilled members of an ineffective team performed. The new senior management had ripped off his ideas to develop their "security strategy" and tried to implement them through ineffective team models. Worst of all, his bonus pay had actually declined under these new and allegedly improved systems.

Attack on AgPEX

Thompson's disgruntlement turned especially harsh when he came under pressure at home due to medical expenses in his family and the need to meet college tuition payments for his twin sons. Thompson realized that the CIO's new security system contained the seeds of its own demise. Because it drew attention in a rigid way to large transactions with complicated order splits most often involving new customers, the system was wide open to anyone who used small orders split between only a few customers, none of whom were new to the system.

All he had to do was to set up a small number of "loyal" customers who would take and send a large number of small split orders and no one would ever bother to look at their transactions. Using his access to system level information, he could easily modify orders being sent to real customers so that their own audits of transactions would not easily identify the shortages in shipments and cross-payments. It would not be hard to set up a permanent skimming operation using a few simple rules that "slipped in under the radar" of this new automated and not-so-smart security system.

Operationally, here is what Thompson did. He set up "false firms" that served as intermediaries between legitimate sellers and buyers. These false firms received shipments of one size and purported to make shipments of a slightly larger size, skimming the receipts from these bogus phantom shipments. Many small skimming operations added up over time to a considerable amount of fraud. Thompson only had to make certain that a comprehensive audit of one of these bogus firms did not take place. Since AgPEX policies and procedures usually looked only at single transactions, there was little chance of this happening. In order to accomplish this fraud, Thompson used his access to the transaction monitoring systems to set up the bogus firms and to design the multiple

> skimming operations that poured cash in relatively small amounts into these firms. He had an illegal cash cow of sorts.
>
> Thompson did not launch illegal operations right away. Before beginning actual attacks, he systematically introduced errors into the statements and transactions of bona fide customers, waiting to see if the auditing and follow up procedures used by AgPEX could capture these innocent-looking errors. As more and more of his "errors" went undetected, he gained confidence in his overall scheme. He waited to launch real insider attacks until he had used precursor "pseudo attacks" to make sure that real attacks were more or less safe. In addition, Thompson had inside knowledge of the CIO's automated transaction monitoring system and what cues most line workers were using to signal possible cases of fraud being triggered by outsiders. He used his inside knowledge to steer his attack behavior away from those transactions most likely to be viewed as suspicious by his co-workers.
>
> As time wore on, Thompson became increasingly confident in his scheme. His initial careful attention to every detail of his skimming operation may have begun to slip somewhat as he became increasingly successful. In addition, the sheer volume of illegal activity began to pile up, leaving behind a larger pile of clues and evidence that would be harder and harder to cover up. Apparently, he was leaving some clues that were noticed by his co-workers. An alert co-worker made a report to management that ended Thompson's scheme.
>
> The senior managers at AgPEX were left with some difficult damage control. Not only did they have to prevent a repeat of this insider Cyber-fraud. They had to prevent additional losses by damage to their future reputation.

The case sets up a common problem, drawn from the fieldwork done by CERT/CC and other members of the Security Dynamics Network. Thompson, the hypothetical would-be attacker, finds a vulnerable spot in the organization's existing techniques for identifying risky transactions. He tests the organization's environment before striking. The strike goes undetected for some time, and the attacks continue until there is some change (either endogenous or exogenous) that stimulates a suspicion of malicious behavior. Using a synthetic case to organize our thoughts, we were able to operationalize our theory of insider threats, without breaching the confidentiality of the actual data.

4 The model and a behavioral theory behind Insider Threats

There are many possible models of why insider threats continue to exist, even in face of compelling evidence of their cost to organizations and the prescriptions of many security experts. Our perspective attempts to illuminate the behavioral aspects of the insider threat. For the AgPEX corporation case study, the firm's performance is due exclusively to implementing different policy decisions based on an improved understanding of cognition and resultant behaviors.

We focus on the long-term fraud threat, and use this as the basis for examination of the motives and tradeoffs that organizations and individuals make in thinking about their internal security systems. The case and the model combine to countervail the common presumption that firms are playing a zero-sum game where increased security comes at the expense of production (and vice versa). This erroneous view leads to systematic under-investment in security. Through experimentation with a simulation tool, the user may find that increased expenditures on security can also lead to increased profitability.

4.1 Description of model structure

In an earlier paper we presented the constructs of the "Dynamic Trigger Hypothesis" (Andersen, Cappelli et al. 2004). This hypothesis led us to believe that an organizational focus on external threats can lead to complacency. This in turn allows an insider to gain confidence by exploiting knowledge of weaknesses in organizational defenses.[4] Defending against both internal and external threats involves considering a combination of policies to institute: (1) technological controls; along with, (2) policies that explicitly acknowledge the role of cognitive and behavioral traits for the firm's information workers – as well as common behavioral traits of a potential inside attacker. In other words, an effective defense against cyber attack equals technology plus behavior. Since best-practices guidance to date has focused almost exclusively on implementing technological controls, we focus on the typically neglected portion of the defense equation.

In this simulation, we look at a single organization that needs to protect itself against both insider and outsider attack. Within the organization, there are three endogenous "roles": **information workers** perform the routine tasks of business and are responsible for the generation of profits. As line staff, they also use their judgment to sense if a particular transaction might be fraudulent. A second role is assigned to the firm's **security officer,** who is responsible for developing the strategy and tactics to protect the organization from fraud. In the ideal world, these techniques are enacted by the information workers. In this model, as in the real world, there is no assumption that information workers obey the directions of the security officer, even though both constitute the defenders of the firm. The third role in the model is the **inside attacker**, or insider. The attacker has some access to the defensive response of the firm, and has to choose when and how often to attack.

In describing the model structure, we begin by depicting the defenders' cognitive and behavioral framework as articulated in the model, followed by a depiction of the behavioral traits associated with the inside attacker. We then describe how production and staffing is handled in the model, and conclude by describing how profit and loss is calculated for the firm.

4.2 The Defenders' World

Transactions come into AgPEX and the information workers must process these transactions. The defenders' world, depicted in Figure 1, summarizes how the firm maintains defenses against attack during the course of processing the incoming transactions. Transactions that come into the firm are either "good" (nothing improper) or "bad" (indicating the presence of either fraud or error). If there were an absolute test for impropriety, a "positive" result on the test would indicate something was amiss, while a "negative" result would indicate that all was well. We use the terms "positive" and "negative" in this sense, rather than one of absolute value.

[4] Organizations that have invested in security systems to protect against outside attack will likely find some value against insider ones as well. The proposed dynamic here is that investments in security which are not followed up will eventually become vulnerable, and will be more vulnerable to individuals inside the firm than outside. This remains an area for study, and there is little data available to support or contest it.

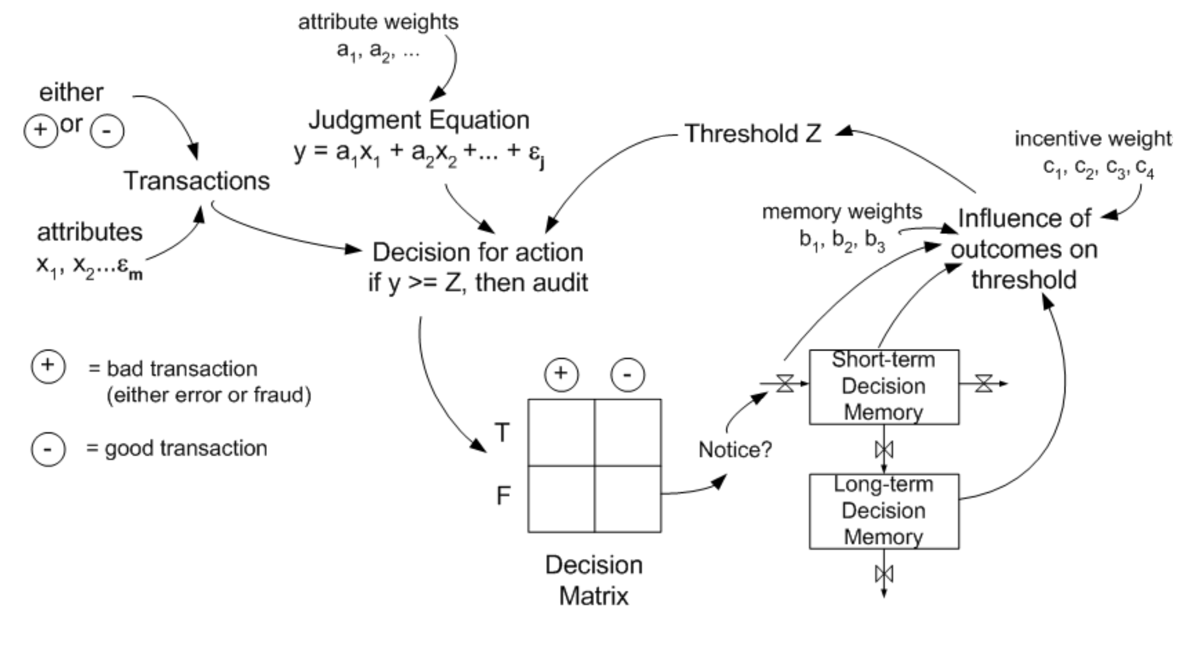

Figure 1 - Defender's World

Unfortunately, there is no such absolute, unbiased test. One task of the information workers (beyond simply processing the transaction) is to make some judgment as to whether the transaction looks suspicious and warrants closer inspection. That is, they need to use their knowledge to consider whether a transaction, with an unknown positive or negative state, should be investigated.

Each transaction has a set of descriptive attributes, $x_1 \ldots x_{n,}$ along with an error term $\varepsilon_{m,}$ capturing variability in attribute measurement. As recounted in the case description, the likelihood of an external fraud associated with a given transaction could be associated to some subset of these attributes. The values of these attributes may be binary, continuous, or qualitative, and found through either an automated screen or a manual review.

The information worker processing each claim must make a judgment as to whether or not the transaction looks as if it could be fraudulent. The aggregate skill that the information workers bring to this task is represented by the weights ($a_1 \ldots a_n$) placed on the attributes in the judgment equation. An additional and distinct error term, ε_j, represents the variability in judgment that occurs when an information worker evaluates the value of identical attributes at two different times.[5]

Information workers make their judgments about each transaction by comparing their (mental and individual) judgment equation calculation, $y = f(a_1x_{1,} \ldots a_nx_n; \varepsilon_j)$ against some threshold, Z. If $y > Z$, then the transaction is considered to be suspicious. Suspicious transactions trigger further inspection in the form of an internal control audit, a contemporaneous verification of the transaction. Such audits are useful, but they cost time and money, which affects the

[5] A third type of error, resulting from variability in the environment, is not included in the model at this time.

financial performance of the firm. When selected for audit, the information worker is judging a transaction as positive, that is, potentially fraudulent. The act of actually performing the control audit, in turn, reveals whether or not they were in fact fraudulent. The transactions that were judged to have been positive, and in fact turned out to have been positive are termed *true positives* – these are intercepted attacks. *False positives* are false alarms, where the transaction was judged to have been positive but the follow-up control audit showed that it was not. Of those transactions judged to have been negative, *true negatives* are normal transactions, and *false negatives* are undefended attacks. These undefended attacks end up creating significant losses for the company.

Without some other kind of auditing, such as random audits or external audits (to be described later), it is not possible to distinguish between true and false negatives. In random auditing, some (usually small) fraction of those transactions judged to have been negative is selected at random for a contemporaneous verification of the transaction.

This technique of judging an ongoing stream of uncertain data (the transactions) against a set of weighted attributes by comparing against some threshold and then, over time, aggregating the results to populate a decision matrix, has been well studied and described within the field of cognitive psychology as judgment theory and decision analysis (Hammond, McClelland et al. 1980; Stewart 1988; Hammond 1996; Weaver and Richardson 2002).

The defenders (the information workers and the security officers) wish to maximize profits by minimizing the fractional costs associated with false positives while simultaneously attempting to avoid fraud losses from undefended attacks. One way to do this is by readjusting the suspicion threshold, Z, based on the set of noticed results as reflected through the decision matrix of accumulated results – true vs. false, positive vs. negative.

Two processes allow adjustment of the threshold. The first relies on a three-mode model of memory, a simplified view of how events move from immediate sensation and reaction to a state of more or less permanent recollection. In the psychology literature, sensations are filtered by attention, which permits some subset to move to a short-term memory store. Some short-term memories are revisited and rehearsed, which provides the impetus to move them to a long-term store (Atkinson and Shiffrin 1968).

In this paper, decision outcomes are analogous to sensations that are noticed when they occur. These are expected to have direct effect on the next set of decisions. In addition, these outcomes accumulate in short-term decision memory, a stock of events that has its own influence on the threshold. Some portion of the contents of short-term decision memory may become long-term decision memory through further integration with existing information, represented as a flow to a second stock or it may not be retained and leak out of the system. Long-term decision memory also contributes to the adjustment of the threshold, and the stock leaks as well, representing the decay of the effect of events that happened long ago that may not be reinforced through inflow from short-term decision memory.

We postulate that information worker perception is dominated by recent events – thus increasing the propensity for the threshold to oscillate between heightened vigilance immediately after observing a true positive outcome and laxity in between. The memory weights (b_1, b_2, b_3, in our three mode case) are front-loaded toward outcomes that have just happened and reducing the influence of long-term memory.

A second mechanism for influencing the decision threshold comes from the incentives that drive the decision maker. In this paper, we assume these effects are largely economic, reflecting the costs and benefits of each of the four possible outcomes: true positive, true negative, false positive, and false negative. For example, a firm's focus on production goals relative to operational security would de-emphasize detection (which would tend to interrupt the generation of product), and drive the threshold higher. A reputation-conscious firm might stress the need to protect against any undefended attacks – false negatives – and lower the detection threshold. Each of the four outcomes has a corresponding weight (in our model, c_1, c_2, c_3, c_4), which articulates the relative importance of each outcome in the decision matrix on the setting of the threshold[6].

This feedback system representing defender behavior is arrayed in two dimensions. First, each transaction is judged for suspicion of attack, whether from external as well as insider attack. Second, the equations are arrayed to represent both the aggregate characteristics of the information workers, and also to represent the characteristics of the security officer, played in the AgPEX case by Sue Miller, the new CIO.

Information worker judgment is ultimately what matters since they directly process (and identify suspicious) transactions. They tend to be dominated by recent events, and their judgments can be subjective, in that their weights can be significantly off from optimal, and the variability in judgment between information workers can be quite high. Moreover, they have little appreciation for the insider threat, meaning their attribute weights for judging the possibility of insider attack are initially very low. However, all this can be improved through training in the procedures designed by the security officer.

In contrast, because of the security officer's training and access to company and industry data, the judgment of the security officer tends to be grounded in both inside and outside sources and more focused over the longer term (and less prone to oscillating, especially if the company maintains an enduring security commitment). Still, the security officer's judgment is imperfect. For example, since the security officer has no production responsibilities, she can tend to overweight the impact of identifying true positives and avoiding false negatives.

The security officer's own judgment can be improved from the analyses performed as part of external audits. We assume there is a capacity for retrospective review, consisting of some combination of:

- A look back at past audits
- A process audit, examining the suitability of the control procedures
- A compliance audit, to verify that the control procedures are being implemented

[6] See Sawicka, A. (2004). Dynamics of Security Compliance: Case of IT-based Work Environments. Kristiansand, Norway, Agder University College. for more on modeling compliance and laxity in security.

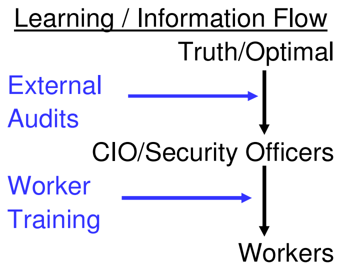

Figure 2 – A Security-Learning Environment

- Analytical review focusing on security risks to the company and looking for patterns in the transactions

These audits are akin to outside accounting audits that examine a company's financial records, except these audits examine how well the company handles its IT processes against error and attack. Depending on the degree of rigor, audits may be very expensive, but they can impart improved knowledge about the performance of the company's IT system to the security officer. Operationally, a commitment to performing external audits allows the security officer to align and converge on the true/optimal weights.

Figure 2 summarizes this two level security-learning environment for the company. The security officer learns about security vulnerabilities and how to improve detection of attackers by commissioning external audits. The security officer transmits her knowledge to the information workers through training. In this way, an effective security program requires both external audits and training. Auditing without training tends to result in little security improvement because the insights from audits are not passed on to the information workers who must ultimately implement any new policies. Training without audits can yield some security improvements, but without the detailed analysis provided by the external audit, the lessons will, necessarily be more generic to an industry and not very company specific. Audits with training typically provide the best combination for cost-effective security improvement (as long as management is smart and stays beneath point of diminishing security investment returns).

Figure 3 shows the effect of security training on the information workers. Training transfers the system knowledge of the security officer (who is expected to be more attuned to the firm's security position) to the information workers. In the model, the attribute weights of the information worker's judgment equation (a_1, $a_2 \ldots a_n + \varepsilon j$) come into alignment with that of the

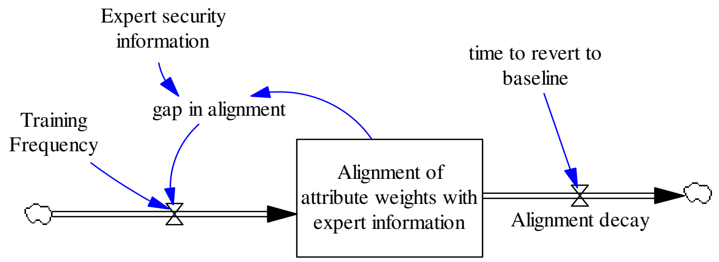
Expert security information
time to revert to baseline
gap in alignment
Training Frequency
Alignment of attribute weights with expert information
Alignment decay

Figure 3 - Effect of Training on Alignment

security officer. The information worker's decision threshold, Z, also changes as both the memory weights ($b_1 \ldots b_3$) and the incentive weights ($c_1 \ldots c_4$) improve and come into alignment with those of the security officer. Changing the memory weights shifts the responsiveness to memory toward the longer term (thereby reducing the yo-yoing in the threshold for invoking control audits). However, the effects of training decay over time and information worker weights can revert towards their initial values. Recurrent training can help retard this decay while continuing to reduce the knowledge gap between the information workers and the security officer.

4.3 The Attacker's World

In this model, we assume that a motivated inside attacker already exists within the firm at the beginning of the simulation. The attacker's behavioral profile as articulated in the model is that of an employee attempting to defraud the company without getting caught – as opposed to, say, an attacker wishing to vandalize the company's IT assets with little concern about detection.

In this case-based model, the insider begins his activity by launching precursors, probes that test the organization's defenses against attack. CERT/CC, in their work examining case studies of successful insider attacks has recognized several types of precursor activities including: stepping stone activities that increase the insider's ability to launch an attack, activities that lower the detection capability of the firm, and precursors that test and probe the firm's defenses (Randazzo et al., op. cit.). In the current incarnation of the model, we consider only precursors that test the firm's defenses.

A schematic illustrating the attacker's decision process with regard to launching precursors is given in Figure 4. Each precursor transaction is characterized by attributes that, when analyzed through the defender's judgment equation, indicates a low likelihood of external attack. Remember, the insider has some knowledge about the attributes that tend to arouse suspicion of a possible external fraud attempt and he piggybacks his precursors onto transactions that will most likely conceal them.

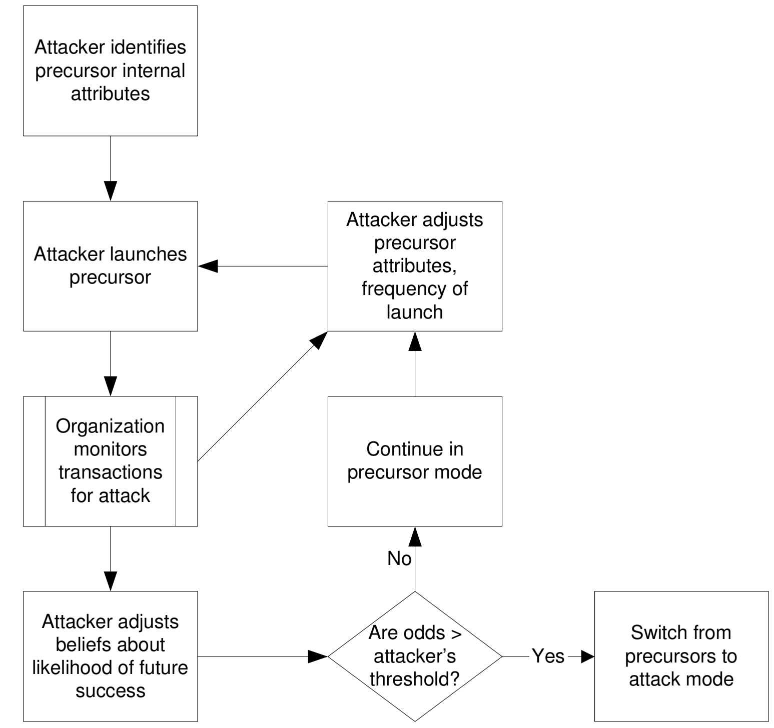
Attacker identifies precursor internal attributes
Attacker launches precursor
Attacker adjusts precursor attributes, frequency of launch
Organization monitors transactions for attack
Continue in precursor mode
No
Attacker adjusts beliefs about likelihood of future success
Are odds > attacker's threshold?
Yes
Switch from precursors to attack mode

Figure 4 - Internal Attacker's Decision Process (Precursors)

If the attacker's precursor is detected by the organization, the attacker receives feedback of the detection, and subsequent precursors are delayed or cancelled. Conversely, if the precursor goes undetected, some emboldening occurs, and the likelihood of a subsequent launch increases. With the launching of each precursor, the insider updates his odds of attack success. If at any decision point these odds don't yet exceed the insider's threshold for success, another precursor probing the system is launched. However, once the odds exceed the insider's threshold, then precursor activity is completed and the insider begins to launch attacks.

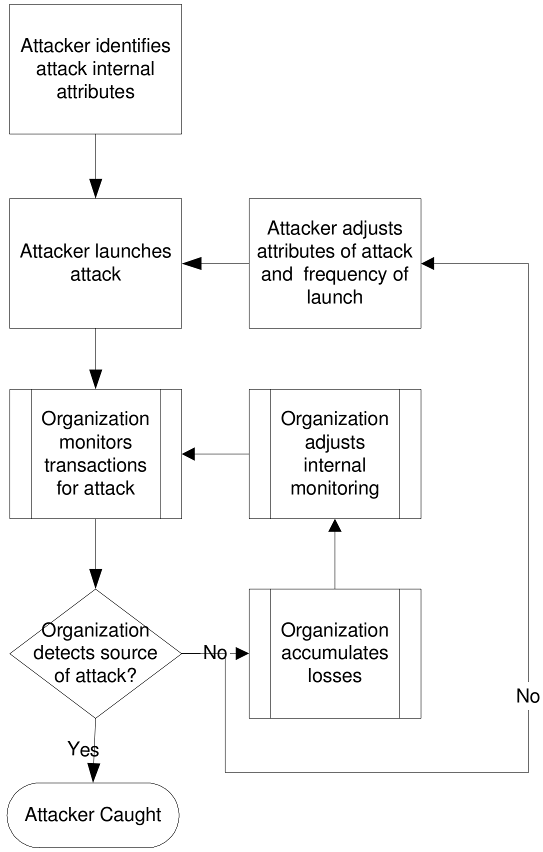
Attacker identifies attack internal attributes
Attacker launches attack
Attacker adjusts attributes of attack and frequency of launch
Organization monitors transactions for attack
Organization adjusts internal monitoring
Organization detects source of attack?
No
Organization accumulates losses
No
Yes
Attacker Caught

Figure 5 - Internal Attacker's Decision Process (Attacks)

If precursor-probing activities are successful, the insider begins launching true attacks. A schematic illustrating the attacker's decision process with regard to launching attacks is given in Figure 5. As with the precursors, the attacker piggybacks on transactions unlikely to arouse suspicion with regard to external fraud. As successful attacks accumulate over time, the attacker becomes emboldened in two ways. First, the attack frequency escalates over time. Second, the attacker can begin leaving behind more clues with each attack, increasing the internal attributes that could be detected by an observant defender and increasing the likelihood of detection.

Note, however, that insider attacks against the firm are not inevitable. Consider what might occur if the managers at AgPEX recognized the potential for insider fraud and instituted adequate controls to defend against it. Their defenses may detect a significant proportion of the insider's precursors. The odds of success would never reach the threshold needed for the insider to begin attacking. Further, with each detected precursor, the frequency of subsequent precursors is reduced.

Figure 6 illustrates how increased attention to security issues affects production and staffing, and ultimately affecting the firm's profitability. Our model expands on a previously published structure (Oliva 2001; Oliva and Sterman 2001; Martinez-Moyano 2004) describing transaction flows and effort and resource allocation mechanisms in firms. In this model, new work in the form of transactions to be processed comes in exogenously. That work accumulates in a backlog that needs to be cleared within a stipulated time frame. The production rate is a direct function of the time to complete each transaction. This completion time depends on the fraction of the transactions undergoing an audit. This fraction, in turn, depends on the degree of commitment to security together with the skill with which the information workers identify suspicious transactions (as improved through training). Also, note that the production rate indirectly depends on the required production capacity, which depends on the transaction completion time. As attention to security slows the rate of production and increases the required capacity, production pressures intensify and productivity increases for a time until fatigue nullifies these productivity gains. This increased workload on the staff could adversely affect staff retention rates. Ultimately, the increase in the required capacity must be dealt with by hiring new staff.

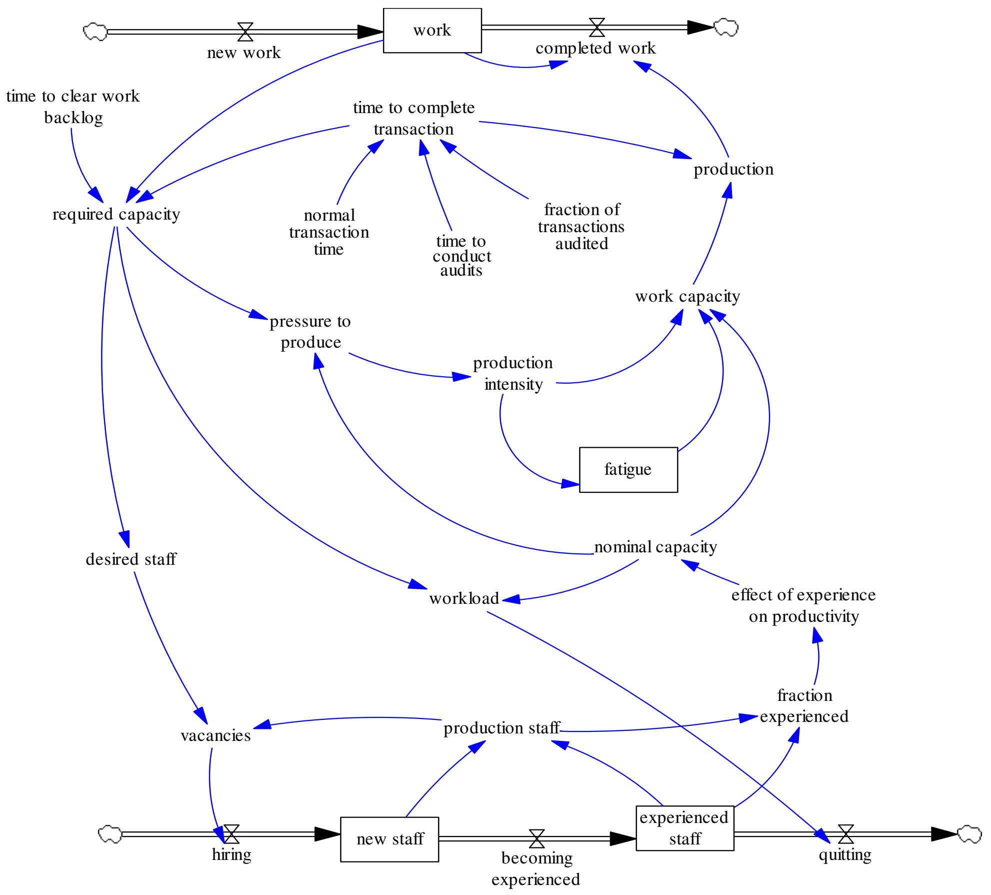

Figure 6 - Process Dynamics

Additionally, in the model, revenues, expenditures, profits and losses are tracked. Each processed transaction generates fixed revenue. Total revenue is simply the quantity of processed transactions times the revenue per transaction. Total expenditures consist of production costs (described above), auditing costs, losses from both insider and external attacks, and training costs. This accounting process is summarized in Figure 7.

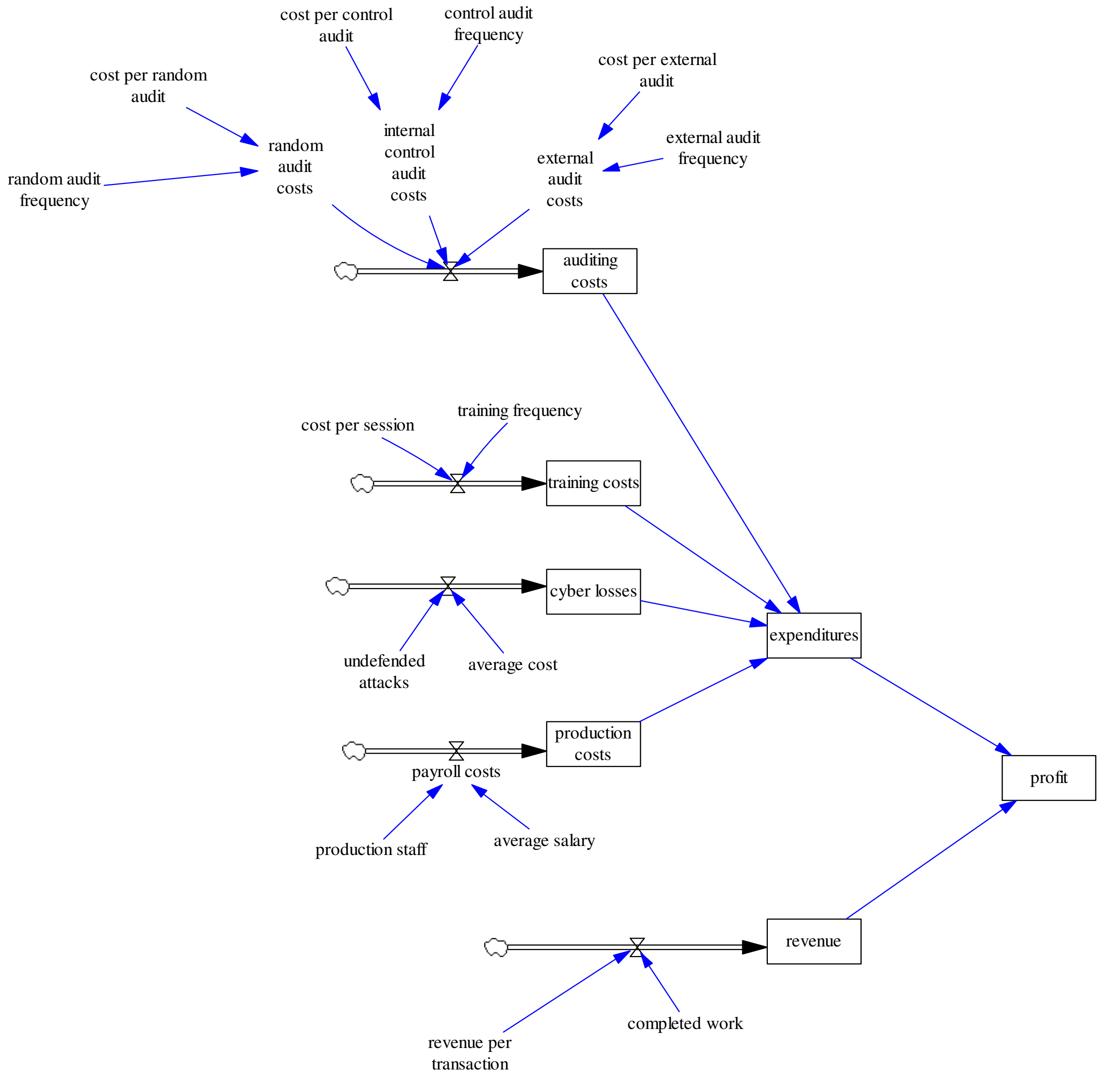

Figure 7 - Business Dynamics

4.4 Description of Model Behavior

4.4.1 The Base Run

The base run presents a situation in which a firm guards against an insider attacker unsuccessfully. The inside attacker generates a series of successful attacks that go unnoticed by the firm's defenders, shown in Figure 8, causing the firm financial harm. In the simulation, the average expected yearly profit presents an oscillatory behavior from an assumed seasonality of operations and product demand with an upward trend until the internal attacker starts to attack frequently (approximately at time 91) when the average profit drops to approximately half its value. At the same time, protection cost remains relatively stable until the repeated attacks from the emboldened insider trigger operational audits, and increasing the cost of protection.

In the base run, under a fixed base rate of external attacks of 0.05[7], the firm is subject to 47 external attacks[8]. Out of the 47 attacks, 32 are intercepted by the control system (via operational audits) and 15 are successful external attacks on the corporation.

The internal attack rate is generated endogenously. The internal attack rate is a function of the decision of the internal attacker to go into attack mode (when his assessment of the likelihood of success goes above the pre-established, and fixed, threshold) and, when in attack mode, of the frequency of the attacks. In the base run, the internal attacker goes into attack mode at time 74,

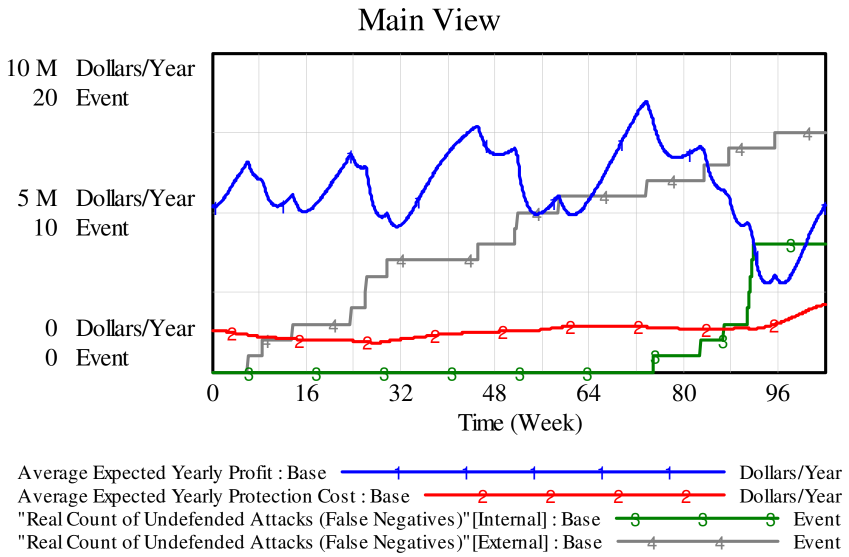

Figure 8 - Base Run Dynamics – Main View

[7] This base rate was selected to portray the case in which firms are subject to low base rate attacks that make learning and defending more difficult. The external attacks base rate remains constant during the length of the simulation (104 weeks).

[8] In 832 transactions yielding a true base rate for the external attacker of 0.056

and starts attacking at a relatively low frequency until time 92, when the frequency of the attacks go up, as shown in Figure 9. In this run, with the existence of an internal attacker that goes into attack mode, the firm is subject to 56 internal attacks. Out of the 56 endogenously generated internal attacks, 51 are unsuccessful and just 5 make it through the control system creating financial damage to the corporation[9].

In the base run, the decision threshold of the information worker with respect to internal attacks remains relatively constant during the first 74 weeks of the simulation. When the internal attacker starts to attack, and the defender can gather evidence that an attack is underway, the firm reacts by lowering the decision threshold, raising the possibility of catching the internal attacks. The defender modifies the level of the decision threshold (both internal and external) based on intelligence about the outcomes of his decisions. However, as mentioned earlier, the intelligence that the defender has is based on information that is both imperfect and incomplete about the outcomes.

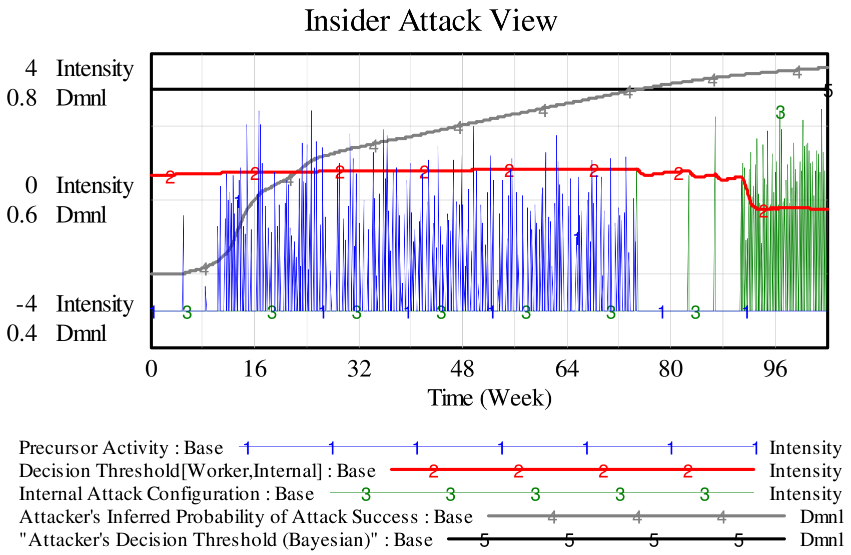

Figure 9 - Base Run Dynamics – Insider Attack View

[9] The true base case for the internal attacker in the base run is 0.24 (56 out of 234 transactions), which is 4.3 times the external attacks base rate.

The defenders—the information workers and the security officers — react differently to information about the outcomes due to differences in their behavioral profile. In the base case, the information worker adjusts his threshold in an oscillatory pattern that remains approximately at the original level while the security officer, responding to the evidence gathered, adjusts his threshold down reaching equilibrium at the lower end of the possible continuum[10] after 50 weeks, as seen in Figure 10.

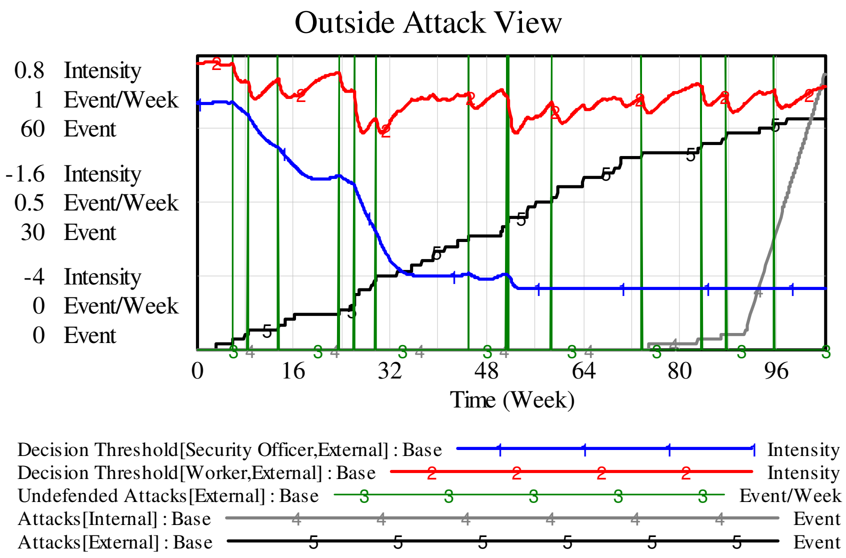

Figure 10 - Base Run Dynamics - Outside Attack View

In summary, the base run shows that after a series of precursor attacks the inside attacker senses the organization's vulnerability through lack of detection. The insider then switches to attack mode, causing financial harm to the organization.

4.4.2 The Alignment through Training Run.

A likely response of management in the firm is to increase the ability and skills of the information worker via training. In the training case, the organization decides to invest in training to help information workers understand and implement the security officer's guidance. This policy successfully suppresses insider attacks. Precursors are detected and the attacker's

[10] The decision threshold varies from +3 to -3 (standard deviations) representing the inverse of the standard normal cumulative distribution (has a mean of 0 and a standard deviation of 1) of the possible outcomes. For example, a decision threshold of +3 is above 99.87% of transactions and generates a response rate of 0.13%, a decision threshold of 0 is above of 50% of transactions and generates a 50% response rate, and a decision threshold of -3 is above 0.13% of transactions generating a response to 99.87% of transactions. The ideal decision threshold is aligned with the actual base rate of the attacks, how much each audit costs (in both direct costs and in worker time) and the average loss to the company from each undetected attack. In the case of the external attack base rate, the ideal response rate would be near 5% (or 1.64 SD). However, the real problem is to determine to which 5% of transactions should the control system respond to (this is the signal detection problem contained in the judgment process of the defender).

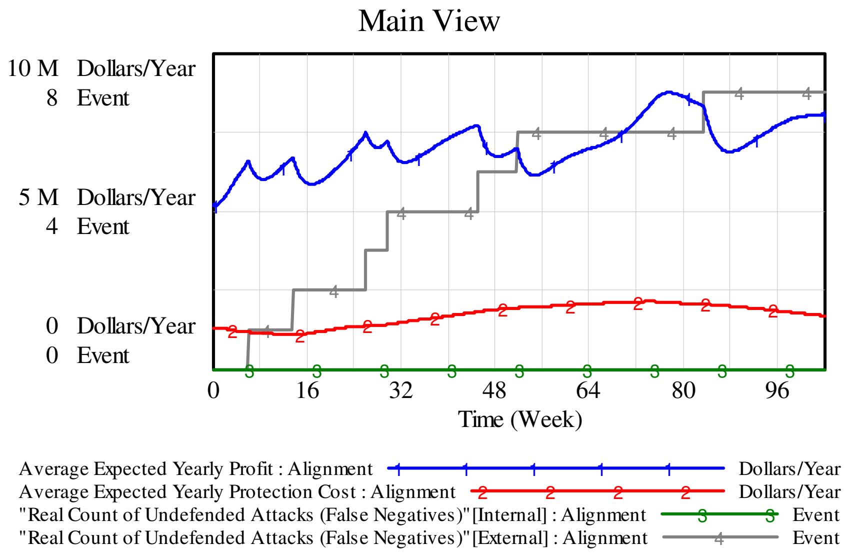

Figure 11 --Alignment Run Dynamics—Main View

belief of possible success stays low. The attacker never goes into attack mode. This policy, labeled the Alignment Run, includes the implementation of a training policy in which the information workers are trained on how to follow the security polices that the security officer has determined. In the base run, the information worker determines the level of his decision threshold (both internal and external) solely on his outcome-related intelligence (or his own perceptions and experience). In the Alignment Run, both the security officer and the worker are trained on how to follow a corporate information policy more consistent with data provided from sources that are more knowledgeable. In the case of the security officer, training aligns his decision threshold to an external (and presumably better) decision threshold standard. In the case of the worker, the training aligns his decision threshold to the policy established by the internal security officer. This alignment causes the information worker to change the way in which he is adjusting the level of the decision threshold.

The new capability to adjust the decision thresholds of the workers and security staff defending the organization creates a new security conscious environment, one that deters the internal attacker from going into attack mode preventing internal attacks from happening. This environment generates zero internal attacks, a decreased number of successful external attacks, and a more robust financial behavior, shown in Figure 11. In this run, the firm is subject to the same 47 external attacks[11] but is able to intercept (defend against) 40 of the attacks allowing only 7 undefended (successful) external attacks to hit the organization, presented in Figure 12.

[11] Same external attack base rate of, approximately, 0.05

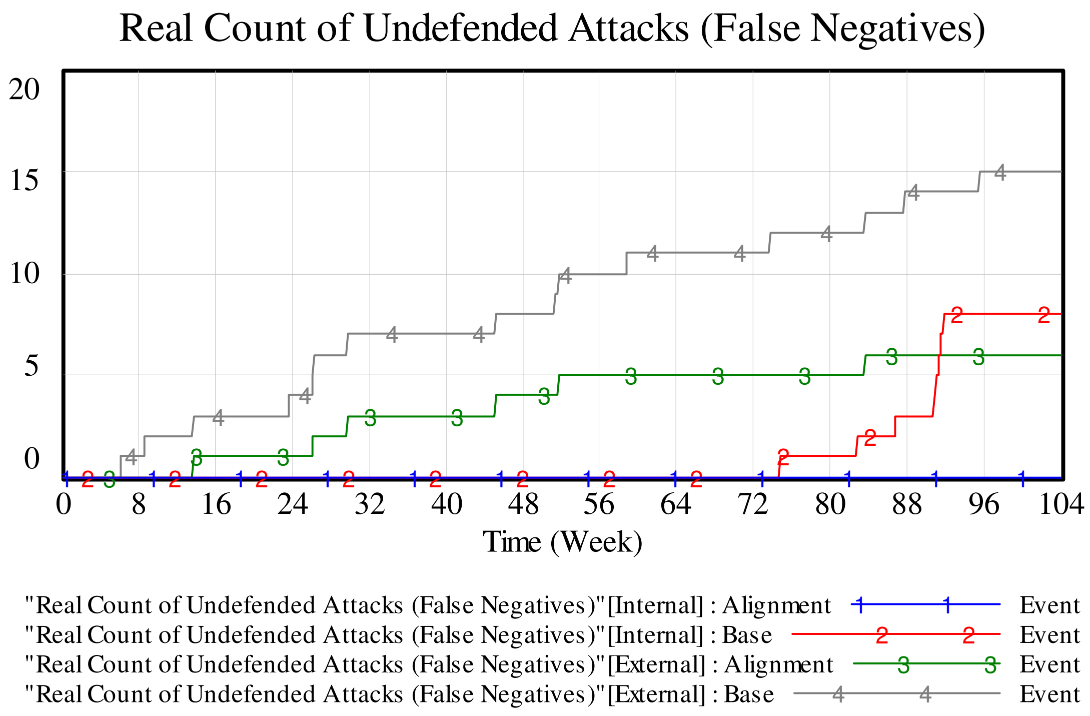

Figure 12 -- Comparative Dynamics—Real Count

The internal attacker, due to the increased vigilance of the information worker and security officer, never reaches the point in which his assessment of likelihood of attack success is above his attack threshold and, therefore, never goes into attack mode. The precursors, generated to test the control system, never produce enough confidence to start launching attacks. Because the precursors are consistently being detected, the internal attacker inferred probability of attack success goes down from its starting point[12] until week 50 when it starts to build up, shown in Figure 13.

The alignment policy not only discourages the internal attacker from attacking but also creates a better financial outlook for the company. Under the alignment policy, the protection cost grows significantly because of the number of operational audits launched[13]. However, at the same time, the alignment policy reduces fraud, fosters increased net profit and creates a better overall financial situation (see Figures 14A and 14 B)—protection pays.

The results of the runs show that the alignment policy was found to be a better option for the firm than the base run scenario. Several other policies are going to be tested to investigate their effectiveness in the overall behavior of the system, including:

- Training information workers and officers on how to become better judges of fraud threats by better integrating available information cues.

[12] 50% in this simulation
[13] Between 30% and 50% overtime

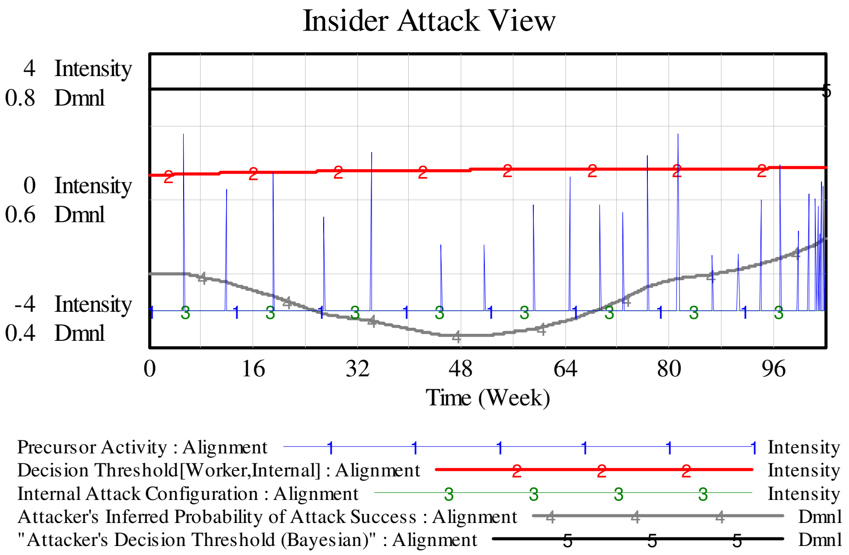

Figure 13 -- Alignment Run Dynamics—Insider Attack View

- Training information workers and officers on how to acquire better information for the judgment process.
- Training information workers and officers on how to become more reliable judges of fraud threat.

5 Using the case and model

The case and model may be used in two training settings. The first is the training of executives and security officers who need tools to understand the risks and trade-offs surrounding insider threats. The second is for instruction in systems thinking as a way of approaching problems that include learning behaviors, uncertain information, and organizational conflicts.

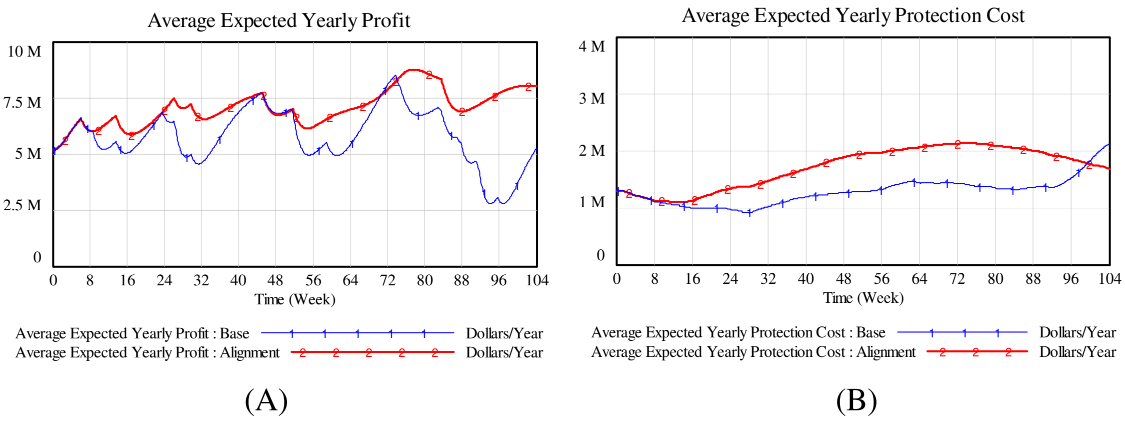

Figure 14 -- Comparative Business Dynamics—Base and Alignment Runs

An initial evaluation of the teaching case was made during a short-term graduate course in information warfare at Carnegie Mellon University. The fifty students involved were a mix, working toward technical and managerial degrees at the master's level. The materials used were a preliminary version of the case study and a greatly simplified model. The methods of system dynamics and the case study were introduced during a lecture, working at a very high level of abstraction. The case study then formed the basis of a subsequent homework assignment, which required application of systems thinking to the problem of dealing with insider threat.

There were several confirmatory and cautionary results from this initial experience. First, the students were able to make use of even the incomplete case study and draw from it sufficient concepts to complete the associated homework. The "Dynamic Trigger Hypothesis," showing how organizations may be lulled into a false sense of security while a potential attacker is preparing to strike, formed a cohesive and helpful framework for students to view the insider threat problem, and to understand the difficulties of dealing with the risks associated with malicious insiders (Andersen, Cappelli et al. 2004). Second, the students often did so without reference to the model or by using simulation. The introduction provided in this initial experience was too brief for them to feel comfortable using the simulation in a course setting. Third, the students were interested in learning more of the technique. Comments to the instructor recommended expansion on the initial experience with a more complete introduction to system dynamics modeling and simulation. Using this pilot experience, further development of the case study and associated models can be integrated further.

6 Next steps: More thoughts about Insider Threats

6.1 Extension of the case and curriculum

The project to develop theory and practice support for insider threats continues. At previous International System Dynamics Conferences several important cases were presented, including ones that presented the risks associated with the lack of professional oversight, indifference to uncertain signals of unusual behavior, misuse of trust, and other gaps in management and oversight (see, for example, Melara, Sarriegui et al. 2003). The AgPEX case adds to this literature by integrating a rich case with a simulation model suitable for class use.

This case study represents one type of insider threat profile. Another common form of insider attack came from organizations that hire very young individuals at low salaries (For example, minimum-wage data entry clerks) to perform functions that require great trust in handling company assets. These attacks are not technically sophisticated attack, but the frequency of these types of attack merits further investigation and modeling.

Appropriate extensions of this work include: Attacks that may have been prevented through some training about the trust that the organization has in their performance; organizational development procedures that increase the levels of commitment on the part of employees; auditing procedures to detect abuses; and, warnings about prosecution of violations of that trust. One other thread that seems to occur in many cases is not integrated in the model: romance. A specific example is a young insider, whose personal relationships have created a vulnerability to emotional pressures, which in turn are manipulated by an outsider to extract or falsify internal information. It's not clear from our research how this training curriculum would be applied here. In addition, there is another common form of attack, based on beliefs of "personal entitlement" on the part of the would-be attacker, which culminates with the theft of proprietary information, sometimes with the intent of creating a competitive service.

A second promising research stream would examine more closely why more companies give relatively little attention to insider threats relative to those starting from outside their perimeter. Even when simple security best practices are identified, such as password expiration, why do many organizations choose to neglect them? Is there a conflict with larger business imperatives, or, as we speculate in our model, is this a case of a short-term profit focus on immediate economic effects?

A third stream looks at improving security policies for firms facing potential insider threats. Of particular interest is identifying the critical policy levers that might suppress the dynamics that embolden potential attackers before they decide that an attack is both feasible and safe.

6.2 Advancing an integrated behavior / technical defense against insider threats

Our current model includes a particular approach to operationalizing the decision processes of managers and would-be attackers, based on Signal Detection Theory (Swets 1992). While this approach is well understood as a viable structure, it has been criticized as prescriptive rather than descriptive of how decision makers react to uncertain information. There are other interesting and alternative ideas, such as instrumental conditioning that might serve the purposes of the model (Gonzalez and Sawicka 2003a; Gonzalez and Sawicka 2003b; Sawicka 2004).

6.3 Extension of the basic model structure to other infrastructure defenses

Our work to date has been focused on insider cyber-threats, largely because the first concerns about this topic were voiced by CERT/CC and their particular agenda. We have observed that many of these same issues may be in play for other industries. One particular Ph.D. project investigates how Computer Security Incident Response Teams (CSIRTs) can effectively handle, detect and prevent incidents from both insiders and outsider in such critical infrastructures (Wiik, Gonzalez et al. 2004). A broader collaborative effort funded by the Norwegian Research Council is underway to conduct research with respect to CSIRTs in the offshore oil industry that is increasingly dependent on computer networks in their daily operations. Some of the decision-making and defense strategies presented here might well apply in parallel domains.

Gonzalez (2005) argues that the outsourcing of security processes – particularly of incident response handling – might be a first step toward a Cyber Security Reporting System (CSRS) in the spirit of 'Air Safety Reporting Systems'. A necessary condition for this to happen is that providers of outsourced security services improve their capability to do proactive work and to provide security quality management services. Successful quality improvement processes might result in a significant improvement of CSIRT performance and release the potential of CSIRTs in security prevention and their ability to evolve toward Cyber Security Reporting Systems. Outsourcing might provide a level of distance, oversight, and standardization, which, if managed correctly, would establish a higher level of trust in process and control than single organizations currently have.

6.4 Teaching Systems Thinking to Security Personnel

This work has induced members of the SDN to apply systems thinking and system dynamics to other problems in security. Recent work is illuminating the critical role that robust change management controls have toward achieving IT operational excellence (Behr, Kim et al. 2004). These same controls are proving to be critical to managing organizational security, particularly in the area of enterprise patch management, which is considered by high performing organizations to fall within the scope of IT change management. A recent CSO survey reported enterprise patch management to be one of the most relied on, but least effective, of the security disciplines (CSO Magazine 2004). Unfortunately, even with this strong evidence, organizational adoption of these controls is hampered by the difficulty of developing a compelling and credible business case.

The CERT/CC is developing system dynamics models that capture the problem as seen by low performing organizations and the mitigations that robust change management controls produce, based on data previously collected by analyzing low and high performing organizations (Taylor, Allen et al. 2005). Simulation of these models supports the business case for the adoption of these controls and generally improves understanding, communication, and training of the benefits of the controls.

Providing IT and security managers with models and simulations of the benefits of robust change management controls will enable them to garner organizational support for adoption of the controls, leading to much higher IT and security operational success. In addition these controls have core elements that help prevent, detect, and correct variance in change and patch management procedures, which are critical to facilitating independent audit of IT and security operations.

Much of the difficulty of developing a compelling and credible business case for adopting change management controls is due to the dynamic complexity of IT and security operational problems and barriers to the effective implementation of change management controls. Many problems suffered by low performers worsen gradually over time with typical fixes helping in the short term but exacerbating the problem in the longer term. The worse-before-better behavior of the many effective solutions can be very difficult for managers to understand and accept. In addition, cultural barriers, such as those that view change management as overly bureaucratic, can be particularly difficult to overcome. SD modeling and simulation help to provide insights into these aspects of the problem and demonstrate the benefit of solutions that work in the long term.

References

Andersen, D. F., D. Cappelli, et al. (2004). Preliminary System Dynamics Maps of the Insider Cyber-threat Problem. 22nd International Conference of the System Dynamics Society, Oxford, UK.

Atkinson, R. C. and R. M. Shiffrin (1968). Human memory: A proposed system and its control processes. The Psychology of Learning and Motivation. K. W. Spence and J. T. Spence, Academic Press. **2**.

Behr, K., G. Kim, et al. (2004). The Visible OPs handbook: Starting ITIL in 4 Practical Steps, IT Process Institute (ITPI).

CSO Magazine (2004). 2004 E-Crime Watch Survey, available at http://www.cert.org/archive/pdf/2004eCrimeWatchSummary.pdf.

Davies, G. (1996). A History of Money from Ancient Times to the Present Day,, University of Wales Press.

Gonzalez, J. J. (2005). Towards a Cyber Security Reporting System -- A Quality Improvement Process. Twenty Fourth International Conference on Computer Safety, Reliability and Security, Fredrikstad, Norway.

Gonzalez, J. J. and A. Sawicka (2003a). Modeling instrumental conditioning -- The behavioral regulation approach. 36th Hawaii International Conference on System Sciences (HICSS 36), Big Island, Hawaii.

Gonzalez, J. J. and A. Sawicka (2003b). The Role of Learning and Risk Perception in Compliance. Proceedings of the 21st International Conference of the System Dynamics Society, New York.

Hammond, K. R. (1996). Human Judgment and Social Policy: Irreducible Uncertainty, Inevitable Error, Unavoidable Injustice. New York, Oxford University Press.

Hammond, K. R., G. H. McClelland, et al. (1980). Human judgment and decision making : theories, methods, and procedures. New York, Praeger.

Lipson, H. F. (2002). Tracking and tracing cyber-attacks: Technical challenges and global policy issues. Pittsburgh, PA, CERT Coordination Center**:** 71.

Martinez-Moyano, I. J. (2004). Rule Dynamics: Towards a Theory of Rule Change in Organizations. Albany, NY, University at Albany**:** 790.

Melara, C., J. M. Sarriegui, et al. (2003). A system dynamics model of an insider attack on an information system. From modeling to managing security: A system dynamics approach. J. J. Gonzalez. Kristiansand, Norway, Høyskoleforlaget AS - Norwegian Academic Press**:** 9-36.

Norwich, J. J. (1993). Byzantium - The Apogee. Sydney, Austrailia, Penguin.

Oliva, R. (2001). "Tradeoffs in Responses to Work Pressure in the Service Industry." California Management Review **43**(4): 26-43.

Oliva, R. and J. D. Sterman (2001). "Cutting Corners and Working Overtime: Quality Erosion in the Service Industry." Management Science **47**(7): 894-914.

Randazzo, M. R., M. M. Keeney, et al. (2004). Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector, U.S. Secret Service and CERT Coordination Center / Software Engineering Institute**:** 25.

Sawicka, A. (2004). Dynamics of Security Compliance: Case of IT-based Work Environments. Kristiansand, Norway, Agder University College.

Spitzner, L. (2003). Honeypots: Tracking Hackers. Boston, Addison-Wesley.

Stewart, T. (1988). Judgment Analysis: Procedures. Human Judgment: The SJT View. B. Brehmer and C. R. B. Joyce. Amsterdam, North-Holland.

Sturgeon, W. (2005). "Passwords: How difficult can it be to get this right?" Retrieved March 9, from http://software.silicon.com/security/0,39024655,39128518,00.htm.

Swets, J. (1992). "The Science of Choosing the Right Decision Threshold in High-Stakes Diagnostics." American Psychologist **47**(4): 522-532.

Taylor, J. R., J. H. Allen, et al. (2005). Change and Patch Management Controls: Critical for Organizational Success, Institute of Internal Auditors, Global Technology Audit Guides.

The Honeynet Project (2004). Know Your Enemy: Learning About Security Threats. Boston, Addison-Wesley Publishing Company.

U. S. Congress (2002). Sarbanes-Oxley Act of 2002. Pub. L. 107-204, 116 Stat. 745.

Weaver, E. A. and G. P. Richardson (2002). The Cycling of a Decision Threshold: A System Dynamics Model of the Taylor Russell Diagram. 19th International Conference of the System Dynamics Society, Palermo, Sicily.

Wiik, J., J. J. Gonzalez, et al. (2004). Dynamics of Vulnerability - Modeling the Life Cycle of Software Vulnerability. 22nd International Conference of the System Dynamics Society, Oxford, U.K.

Wilmer, S. (2002). "Preventive Security." Retrieved March 13, 2005, from http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=436.