# A System Dynamics Model of an Insider Attack on an Information System

CARLOS MELARA, JOSE MARIA SARRIEGUI
Campus Tecnológico de la Universidad de Navarra (TECNUN)
Pº Manuel de Lardizabal 13, 20018 San Sebastian, Spain
Tel. (34) 943 21 98 77 Fax. (34) 943 31 14 42
Email: cmelara@tecnun.es, jmsarriegui@tecnun.es

JOSE J. GONZALEZ, AGATA SAWICKA
Faculty of Engineering and Science, Agder University College
Groosveien 36, N-4876 Grimstad, Norway
Tel. (47) 37 25 32 40 Fax: (47) 37 25 31 91
Email: jose.j.gonzalez@hia.no, agata.sawicka@hia.no

DAVID L. COOKE
Haskayne School of Business, University of Calgary
2500 University Drive NW, Calgary, Alberta, Canada T2N 1N4 Canada
Tel. (403) 255-3878 Fax: (403) 255-0820
E-mail: dlcooke@ucalgary.ca

## Abstract

There is little doubt that information systems security is a major concern for companies that are dependent on information technology. Among the risks to information system security, insider attacks seem to have the greatest potential for creating a significant system failure. Despite the likelihood of insider attacks and the potential magnitude of their impact, companies are still not doing enough to protect themselves against this kind of threat. By presenting and analyzing a model of an insider attack on an information system, this paper provides insights into the dynamics of the problem and suggests policies to minimize the risk of security failures or at least to reduce the extent of damages should an insider attack occur.

## Introduction

### Insider Attacks, Outsider Attacks and Malicious Insiders

There are a wide range of possible attacks by malicious individuals that can jeopardize the operation of an information system, and therefore the operation of a company that depends on it. Broadly, speaking, these attacks can be categorized into insider attacks and outsider attacks, depending on whether they were initiated from inside or outside the organization. Schultz defines an insider attack as “the intentional

misuse of computer systems by users who are authorized to access those systems and networks" (Schultz 2002). The insider attacker, then, would usually be an employee, a contractor or a temporary worker trusted by the organization, and so he[1] can cause damage from inside any perimeter defenses placed around the system. This fact has considerable importance because most companies tend to secure their networks only against outsider attacks.

Schneier uses the term 'malicious insider' (Schneier 2000), which seems more reasonable, because an insider attacker always has a motive to commit the attack (e.g. disgruntlement, revenge, profit-seeking or espionage). A 'malicious insider' poses great risk to the company because he understands the system, he masters the organization and – what is worse – he has nearly perfect knowledge of their weaknesses and vulnerabilities. As Schneier points out, "a 'malicious insider' might have considerable expertise, especially if he was involved in the design of the system he is now attacking" (Schneier 2000).

Thus, we can define a "malicious insider" as a perpetrator who has the necessary skills and knowledge, enough access to the system, and a motive to commit the attack. From this point onwards, we will refer to a "malicious insider" only as an "insider."

According to many authors, insider attacks occur far more frequently than outsider attacks (Briney 2001; Dhillon 2001; Dhillon and Moores 2001; Schneier 2000). On the other hand, other sources suggest that most attacks come from outside (Power 2002; Schultz 2002). However, Schultz points out that "it is more likely to be true that more successful attacks come from inside (...) there is no debate that insider attacks pose a far greater level of risk than outsider attacks" (Schultz 2002). Mitnick expresses it this way: "Experience and statistics have clearly shown that the greatest threat to the enterprise is from *insiders* [Mitnick's emphasis]. It's insiders who have intimate knowledge of where the valuable information resides, and where to hit the company to cause the most harm" (Mitnick and Simon 2002, p. 161).

Hence, we can expect that attacks from inside are more likely to succeed and be more harmful to the system than outside attacks. However, many companies are not getting the right message. As Scalet points out, "Many companies don't do enough to protect against insider threats" (Scalet 2002). Similarly, the 2001 Information Security Industry Survey showed that the number one priority of security professionals is securing the network perimeter against external attacks (Briney 2001).

[1] Since the vast majority of the malicious insiders have been males there is nothing sexist in using the male pronoun "he" throughout this paper.

## Information Security Concerns

Many authors agree that information security is not only a matter of technical controls or measures (Power 2000; Dhillon 2001; Dhillon and Moores 2001; Gonzalez and Sawicka 2002; Shaw, Ruby, and Post 1998; Schneier 2000). Security work systems involve people, organizational factors, technology, tasks people and the working environment (Carayon and Kraemer 2002; see also Carayon and Smith 2000; Smith and Carayon-Sainfort 1989), and therefore security must cover all of these aspects. In this regard, Dhillon has proposed three kinds of security controls to effectively secure an information system:

1. **Technical Controls**. Technical controls of security are mechanisms that protect the system from incidents or attacks: Antivirus software, access controls, backups, recovery and audit software, for example.

2. **Formal Controls**. Formal controls of security are business structures and processes that ensure the correct general conduct of business and reduce the probability of an incident or an attack, or at least minimize its impact. For example, separating the security organization from other IT departments, designing correct segregation of security duties and therefore access rights and privileges, designing and controlling the appropriate employee-supervisor relationship, routine risk evaluations, etc.

3. **Informal Controls**. Informal controls essentially deal with the culture, value and belief system of the organization. An organizational culture in which it is possible to understand management's intentions, and which is conducive to developing a shared vision and other informal objectives, would make members of the organization more committed to their activities and to the success of the organization as a whole. Informal controls might be created, for example, by increasing awareness of security issues through education and training programs.

Thus, an organization needs to correctly implement these three kinds of controls to effectively secure an information system. The absence of even one of these controls can jeopardize the effectiveness of the information system security. Under this model we can view security as being a chain with three links: technical, formal and informal controls. Like any other chain, security will be only as good as its weakest link.

In the next section, we present the Tim Lloyd/Omega case study. Analysts consider this case to be one of the worst information security disasters that ever happened. This case can give us some insights into the factors that lead to a harmful and potentially devastating insider attack.

# Synopsis of the Tim Lloyd/Omega Case

On July 10, 1996, Timothy Allen Lloyd was fired from Omega Engineering Corp., a high-tech measurement and instrumentation manufacturer based in Bridgeport, NJ. Lloyd had worked for Omega for 11 years, working his way up from being a lowly machinist to system administrator. Nevertheless, as the company expanded into a global enterprise, Tim Lloyd's prominent position slipped from being one of authority into being just one member of a team. Feeling 'disrespected' because of this perceived demotion, Lloyd turned on the company and planted a software "time bomb" that destroyed the hub of the network that he himself had created. The prolonged system downtime that resulted from this incident led to damages, lost contracts, and impaired worker productivity that totaled more than $10 million.

On the morning of July 31, 1996, the time bomb activated and made the server crash as Lloyd had planned, deleting more than a thousand programs that "ran" the company. As Gaudin points out, "Omega executives didn't know this yet, though. All they knew was that the file server was down and the manufacturing machines were sitting idle, waiting for the tooling programs that had been stored in the file server" (Gaudin 2000, p. 2).

Jim Ferguson, plant manager at Omega, who was called immediately after the server had crashed and failed to reboot, went looking for the backup tape while other workers tried to bring the server back up. The programs could be taken off the backup tape and the machines could run, minimizing the impact of the disruption, even if the server was down. However, the backup tape could not be found. It was discovered later that Lloyd had removed the backup tape as part of his preparations to maximize the impact of the time bomb.

Ferguson then accessed the individual workstations to retrieve any programs that the workers had saved to their desktops. There was nothing for him to find there either. "It was an awful feeling," Ferguson says. "We were just starting to get an idea of all the impact and what it was going to mean and how it was going to affect us" (Gaudin 2000, p. 2).

Ferguson's attention then turned to Omega's former system administrator, Tim Lloyd, who had been fired three weeks before the system crashed. Besides having designed Omega's main computer network, Lloyd had also been the company's network administrator. As O'Brien points out: "He knew the ins and outs of the system and had all the supervisory privileges to make network additions, changes and deletions" (O'Brien 2002, p. 692). In addition, as Gaudin explains: "He was also in charge of doing backups" (Gaudin 2000, p. 3).

Lloyd knew exactly where information was stored and what actions would hurt the most. He had an accurate perception of Omega's security level and its weaknesses, as most insiders do. This let him devise and execute specific actions that would increase the attack's impact. As Gaudin explains, "Lloyd had recently taken programs off the workstations and centralized them on the one file server, telling workers not to store them locally any longer" (Gaudin 2000, p. 3).

When Lloyd was fired, "No one at Omega assigned someone other than Lloyd to do the backups. No one checked the file server before or after he left. No one even hired a new network administrator after Lloyd was terminated, assuming that all it needed was simple maintenance and an outside contractor could take care of that" (Gaudin 2000, p. 5).

Apparently, Lloyd developed his plan over several months, seemingly spending much more effort than the company had done to protect itself from insider attacks. Omega did not perceive the threat posed to its information system, although precursor incidents indicating that security was compromised should have alerted management. Indeed, failure to learn from precursor incidents is an ubiquitous trait in all kind of safety and security problems (see Cooke 2003a and references therein).

## Problem Analysis

Before the preparation and execution of the "big attack", Tim Lloyd caused the occurrence of some incidents that affected proper operation of the information system and caused downtime. Arguably, in the absence of formal controls, management would perceive downtime as an indicator of security level. Since downtime seems to have occurred rarely in the past, and had not have been very serious, management was not concerned so much about security. Omega seemed to have an acceptable security level, and from this sense of complacency they became victims of their own success.

In the time before the attack, Omega was expanding from a local company into a global enterprise. The high pressure to grow is likely to have diminished management's commitment to security. Low commitment to security and misperception of the security level meant that management actions to improve or, at least, maintain the security level were grossly inadequate.

The incidents mentioned above and the downtime they generated also caused workplace discontent. Workplace discontent seems to have worried management the most because it affected productivity directly. As described below, management took some actions to stop these incidents and improve workplace climate: Tim Lloyd received verbal and written warnings, and was demoted. However, there is no

evidence to the effect that management perceived Lloyd's actions as threats to security. Rather, there is clear evidence that management interpreted Lloyd's behavior only as a threat to workplace climate while continuing to trust him completely as a computer expert.

Tim Lloyd was in charge of all security tasks and had unrestricted access to the system. As a malicious insider, he had the advantage of being able to reduce the security level through actions derived from his knowledge of the system. Such actions included centralizing the programs and files that "ran" the company in the one file server and removing the backup tapes from Omega's premises.

## Time Horizon

We shall consider as time horizon for the model to be the period from early 1995 until the end of July of 1996. Indeed, in 1995 Tim Lloyd was demoted from a "staff employee," in charge of Omega's information system, to a "rank and file" employee. This perceived demotion led to Lloyd's disgruntlement and to an escalation of his subversive activities that culminated in the "time bomb."

## Model Boundaries

The model boundaries will be drawn around the insider and Omega's management, their perception of security and its influence over the security level. We assume that Omega had a malicious insider and we analyze which factors provoked a successful attack. We are not going to study the insider's profile or his psychological behavior.

## Reference Modes

Following his demotion from a star employee to an average worker, Tim Lloyd exhibited public signs of discontent. He became "an angry man who lashed out, verbally and physically, at his co-workers, bottlenecked projects simply because he wasn't in charge of them, and even knowingly loaded fault programs to make coworkers look bad, according to Omega executives. In that year, he had received verbal warnings, was written up twice and demoted" (Gaudin 2000, p. 4).

A crucial observation is that management perceived Lloyd's problematic behavior as a disruption of workplace climate and not at all as a threat to the security of the company: "I had trusted Tim Lloyd completely," manager Ferguson told the jury (Gaudin 2000, p. 3). Further: "…even while he [Ferguson] was pleading with Lloyd for information about the [missing backup] tape, he still was having a hard time imaging that Lloyd would have damaged the system. Ferguson had held on to that kind of trust even when Lloyd had become a problem employee" (Gaudin 2000, p. 4).

Management's total obliviousness concerning Tim Lloyd as a threat to Omega's security is astonishing because Lloyd *did* cause some problems to the computers and the networks, following his feelings of being disrespected, and "…even knowingly loaded fault programs to make coworkers look bad …" (Gaudin 2000, p. 4).

Accordingly, the reference behavior modes include Tim Lloyd's disruptions of workplace climate as well as some security incidents that went unnoticed as security threats. Further, the reference behavior includes management preoccupation with workplace climate and corresponding obliviousness toward the security threat posed by Lloyd. It is likely that the high pressure to grow, which had characterized Omega since 1985, made workplace climate the key aspect of concern for management.

There was an absence of formal policies, as Dhillon defines them (designing correct segregation of security duties, designing and controlling an appropriate employee-supervisor relationship). Neither are there clues about any security audits: The deliberate "markers" left by Lloyd stayed unnoticed. Therefore, we assume that security audits did not exist.

Tim Lloyd made up his mind to strike some months in advance of the "big attack." His disgruntlement may have triggered his actions to reduce the security level of the system. About a year before he committed the attack, he showed visible signs of discontent, and the failure of management to respond to this behavior from a security perspective may have encouraged Lloyd to plan his attack. Lloyd's behavior and his actions to disrupt the information system can also be interpreted as deliberate markers to test whether such behavior and manipulations would provoke management suspicion of an insider attack. Management's failure to react to these markers was a clear sign that nobody seemed to be concerned about information security at Omega. This lack of concern let Lloyd act with impunity to make the system more vulnerable in the few months before he committed the attack. Interestingly, Mitnick and Simon (2002, see e.g. p. 20-21) document that probing the alertness of defenses through appropriate "markers" is part of the "bag of tricks" of malicious agents.

The security level was extremely low at the end of the considered time horizon, i.e. when the attack actually occurred. The severe consequences of the attack support this conclusion. The security level had decreased significantly during the last few months preceding the attack.

There was a high pressure on the company to grow its business during the entire time horizon under consideration. Figure 1 depicts the reference behavior modes of the problem.

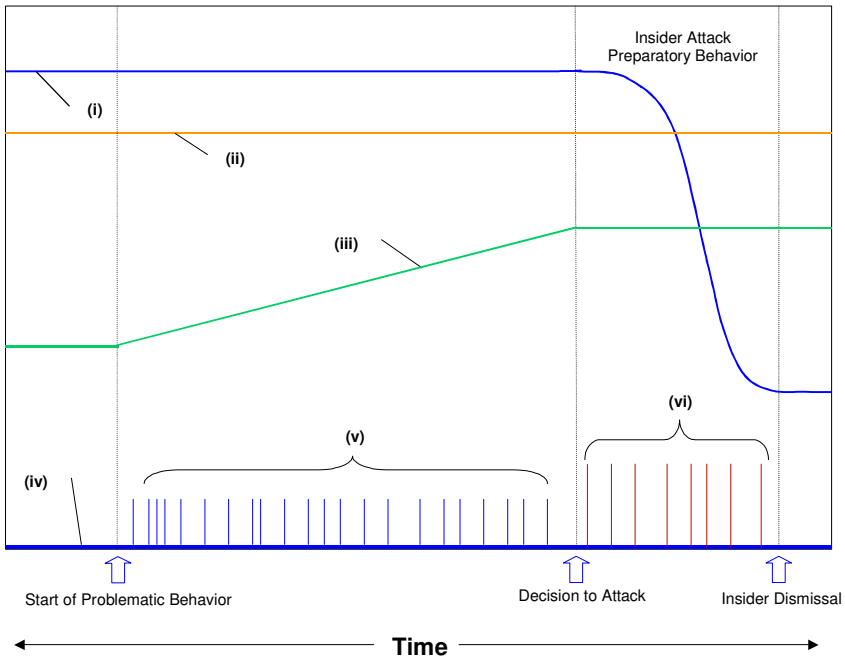


**Fig. 1:** Reference Modes: (i) Security Level; (ii) Pressure to Grow; (iii) Workplace Discontent; (iv) Formal Controls; (v) Disruptions of Workplace Climate and Precursor Incidents; (vi) Actions to Reduce Security Level.

## Dynamic Hypothesis

The dynamic hypothesis is that insider attacks tend to occur when potential malicious insiders perceive the system as being extremely vulnerable. In the case of Omega, risk misperception and management priority on growth over security provoked an erosion of standards that led Omega to a low level of security (see erosion of standards due to the compounded effect of instrumental conditioning and risk misperception in Gonzalez and Sawicka 2002, 2003).

Apparently, the malicious insider perceives this security exposure in an accurate manner and this reinforces the probability of attack. The insider tests the alertness of the system with "markers", i.e. creating small disruptions. In fact, it is likely that the intent to launch a big attack originates gradually when small disruptions motivated by the insider's discontent fail to be detected by management, thus indicating to the insider that the system is vulnerable.

Further, the accurate perception of the system's vulnerability, including the observation that nobody seems to care, induces insider actions to maximize the impact of the attack without being detected. For example, as in Lloyd's case, to conduct a test attack before the 'big attack' or to take the programs off the workstations and centralize them in just one file server. These actions to probe the system's defenses

can be interpreted as part of the insider's preparatory behavior before launching a full-scale assault.

## Stock and Flow Model

The interaction of the key variables of the Tim Lloyd/Omega case can be conveniently shown in the stock and flow model in figure 2.

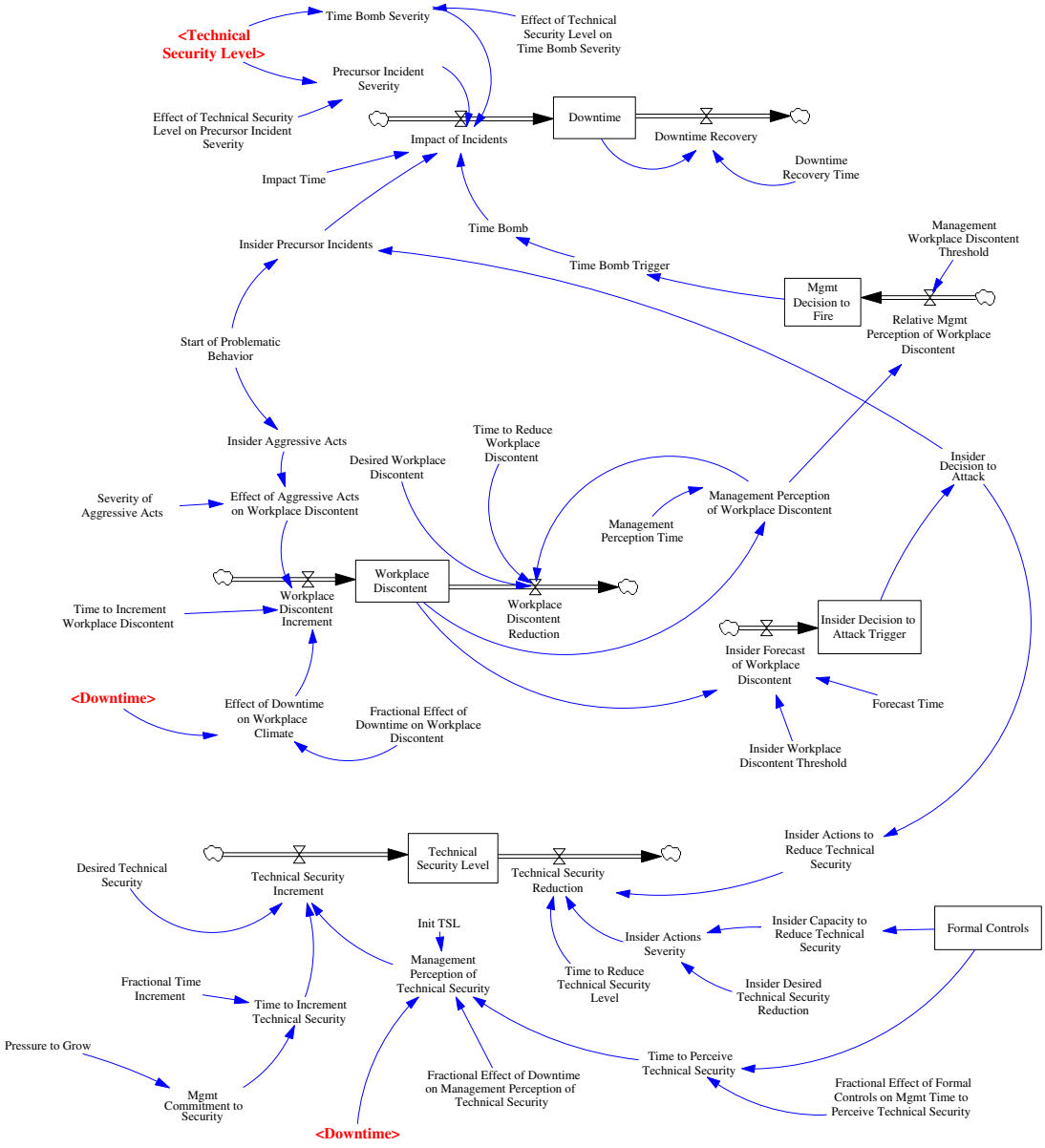


**Fig. 2:** Stock and Flow Model.

In this model, Tim Lloyd's initial problematic behavior arises as two streams of events: the insider precursor incidents and the insider aggressive acts. Both streams of events are spontaneous manifestations of Tim Lloyd's disgruntlement, rather than parts of a planned attack.

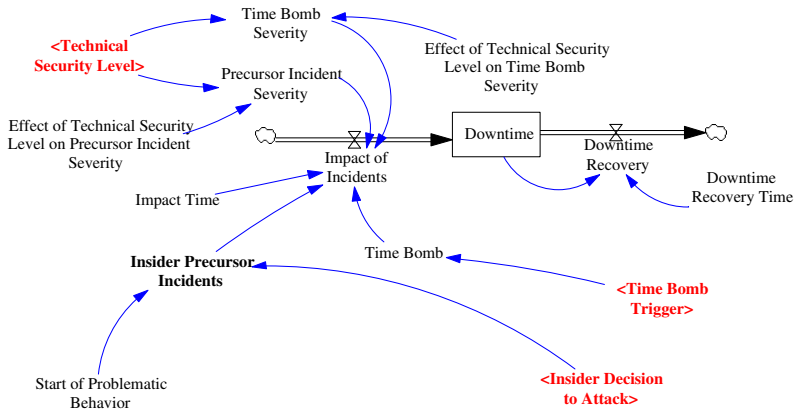


**Fig. 3:** Effect of Insider Incidents on system Downtime.

The *Insider Precursor Incidents* are Tim Lloyd's actions that directly affect the information system causing downtime hours. This effect is represented in figure 3 and, as it can be seen, the impact of those incidents on the system downtime depends on their frequency and on their severity. Since these incidents act directly on the information system, the *Technical Security Level* of the system determined their severity.

We are assuming that the totality of the technical security mechanisms completely protects the system from attacks or, at least, that if an attack occurs then its impact on downtime is negligible. Therefore, the technical security level determines the severity of the time bomb and the precursor incidents.

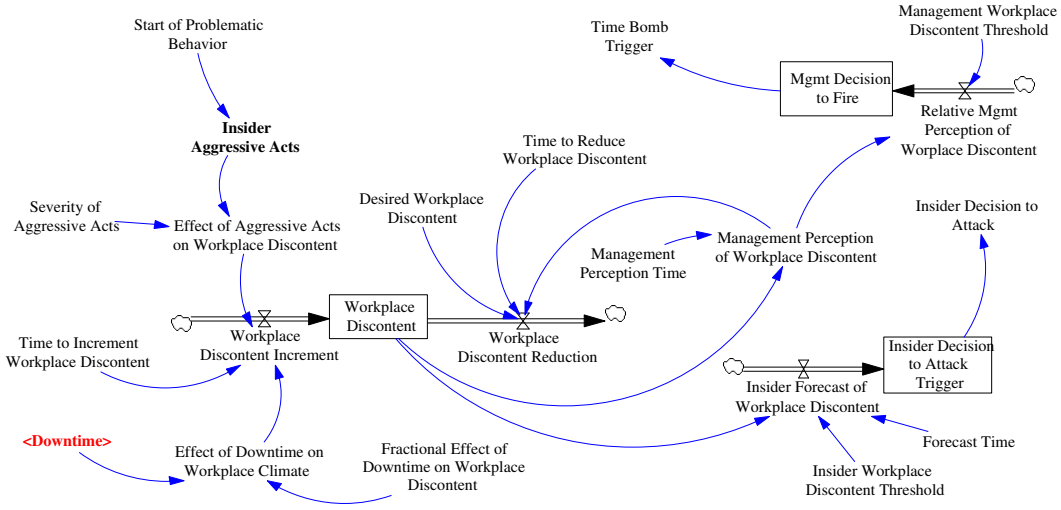


**Fig. 4:** Effect of Insider Actions on Workplace Discontent.

Note that the effect of the time bomb is also represented in this part of the model, although it is part of a planned attack. This happens because this subsystem captures the effect of Tim Lloyd's actions on the system downtime. Prior to the time bomb, these actions were not perceived as security problems but rather as disruptions of workplace climate (see the next subsystem).

The second stream of events, *Insider Aggressive Acts*, includes verbal and physical actions by Tim Lloyd against other employees at Omega, which were emotional signs of his disgruntlement. As shown in figure 4, these aggressive acts and the downtime due to incidents caused a climate of *Workplace Discontent*. Management perceived this discontent and warned Tim Lloyd. When workplace discontent reached a certain threshold, management took the decision to fire him. This triggered the time bomb countdown.

An important aspect is that Tim Lloyd anticipated that he would be fired. In the lower right corner of figure 4, the variable *Insider Forecast of Workplace Discontent* represents this fact. It is assumed that Lloyd anticipated that his actions would increase workplace discontent and that he would be fired as a consequence. Based on his forecast of the future chain of events, he decided to attack and made all the necessary preparations for the time bomb in advance. During this preparation time, he stopped creating the precursor incidents that caused downtime in the system so as not to be caught. When the management decided to fire Lloyd, the bomb was already tested and ready to deploy.

These two 'decision' variables, *Management Decision to Fire* and *Insider Decision to Attack*, act as binary variables (true or false). Their value has a significant impact on the global behavior of the system.

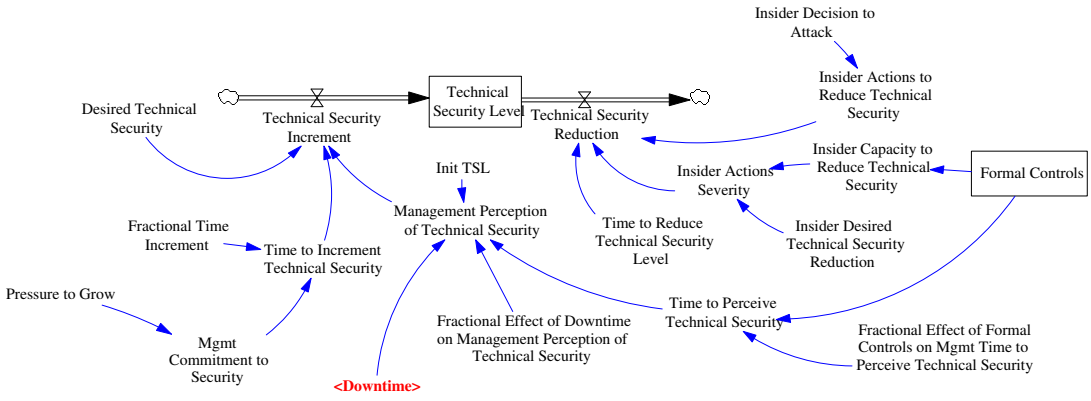


**Fig. 5:** Security Level Reduction.

Figure 5 represents the security level reduction subsystem. Upon his decision to attack, Tim Lloyd reduced the technical security level of the system through well-targeted actions. As a result, the severity of the time bomb would be maximized. In the absence of formal controls Tim Lloyd could act unnoticed to reduce the technical security level.

The lack of formal controls is also manifested in the way management perceived the security level of the system in terms of downtime instead of in terms of security audits

or another established formal controls. This perception on the part of management and the *Management Commitment to Security* determined the technical security increment. Note that management commitment to security depends on the pressure to grow as has been argued before, which is analogous to management commitment to safety depending on the pressure for production as modeled by Cooke (2003b).

Note that we have calibrated the model parameters so that the behavior obtained from the model is coherent with the chronology of the real case. This is arguably a good choice given there is no precise information about the *quantity* and *magnitude* of the precursor incidents nor about the actions to debilitate the technical security of the system.

Some modifications of the temporal parameters can make the system behave significantly differently. For example, when *Time to Reduce Workplace Discontent* is decreased, the simulated Tim Lloyd does not decide to attack the system. Another interesting behavior appears when *Management Perception Time* is increased. In such case, the simulated Tim Lloyd is committed to attack but Omega does not fire him. In order to obtain a more realistic behavior, the model should include a mechanism that allows Tim Lloyd to revoke his decision to attack upon realizing that he is not going to be fired anyway.

## Behavior over Time

The simulation results show that the causal structure described above was able to faithfully reproduce the reference behavior modes.

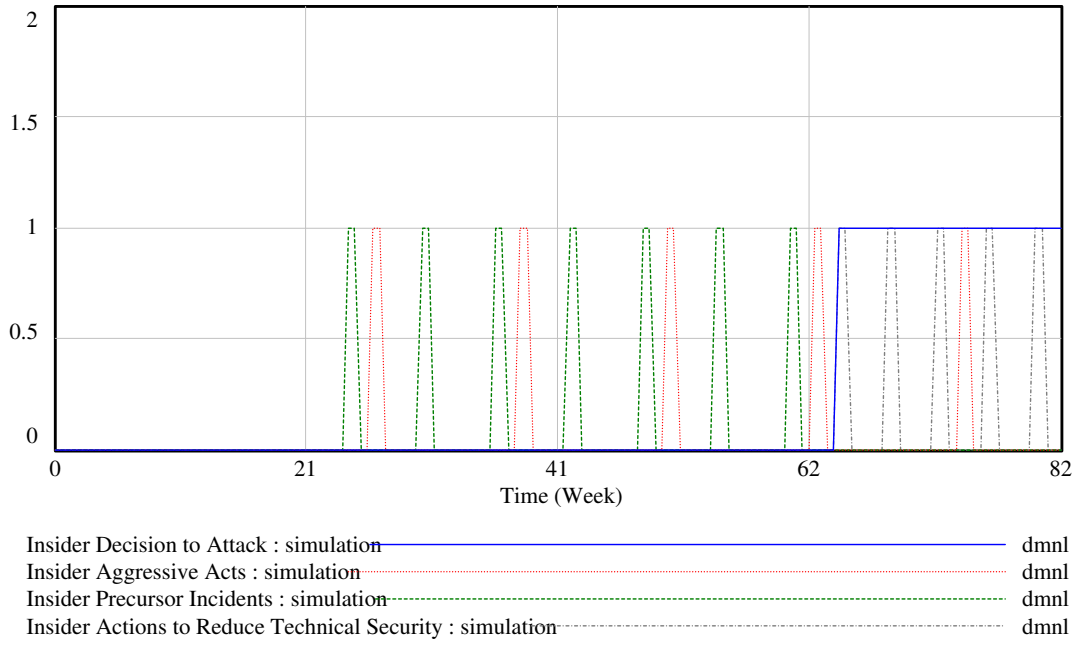


**Fig. 6:** Behavior of Insider Actions over Time.

Figure 6 shows how the model represents the *Insider Precursor Incidents* and the *Insider Aggressive Acts* as a train of pulses of value 1. When Tim Lloyd decides to attack, this train of pulses stops and the *Insider Actions to Reduce Technical Security* level starts.

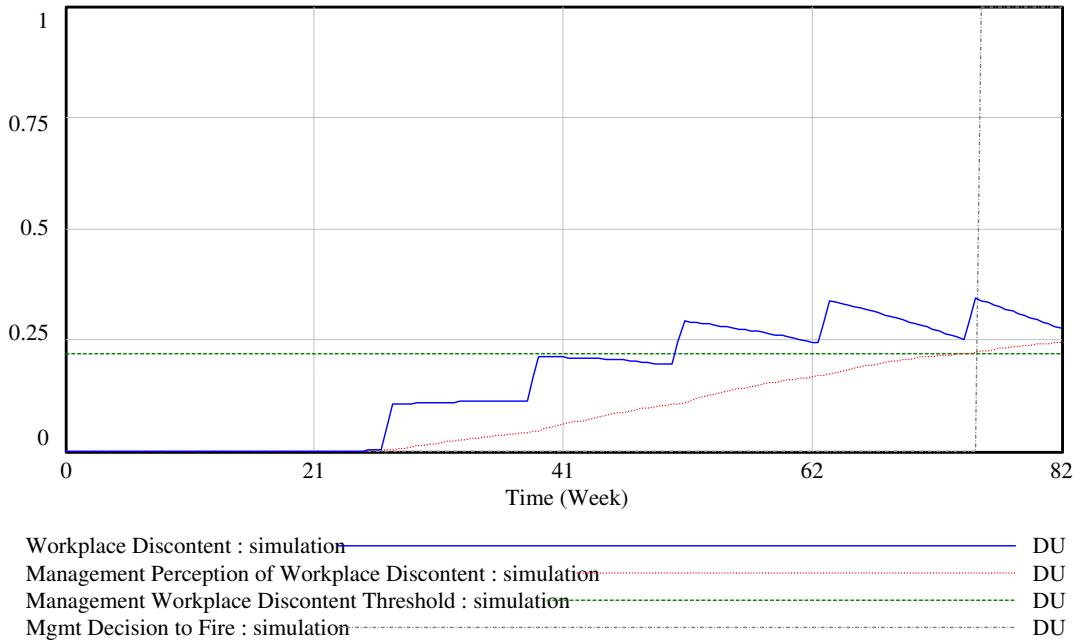


**Fig. 7:** Behavior of Workplace Discontent over Time.

Figure 7 shows the effect of the insider aggressive acts and downtime due to precursor incidents on workplace discontent climate. Management perceives this discontent and compares it to a workplace discontent threshold. When discontent reaches the threshold in week 74, management decides to fire Tim Lloyd.

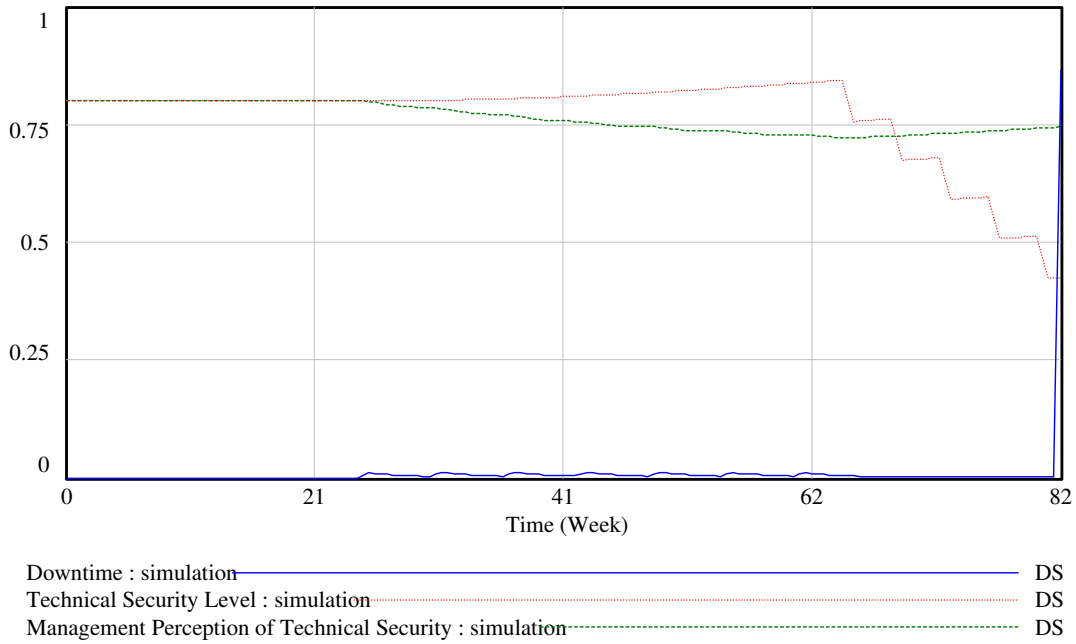


**Fig. 8:** Behavior of System's Security Level over Time.

As argued previously, upon his decision to attack Tim Lloyd acted to reduce the technical security level, and the effects can be seen in figure 8.

Close to week 60, when Lloyd decided to attack, the technical security level starts to decrease. Nevertheless, management did not perceive any threat to security, but rather, as seen before, management interpreted precursor incidents and aggressive acts as threats only to workplace climate. Moreover, in the absence of any other control to measure the security level, Lloyd continued to reduce the technical security of the system. When the "big attack" occurred, the time bomb had disastrous consequences and downtime shot up.

## Discussion of Results

Once the model had been validated against the reference behavior modes, its behavior was tested by making four different assumptions about the formal security controls: absence of formal controls (no formal controls), poor, normal and high level of implementation of formal controls. As argued in this paper, formal controls play an important roll in securing an information system. The results from testing model behavior under these four assumptions appear to support this argument.

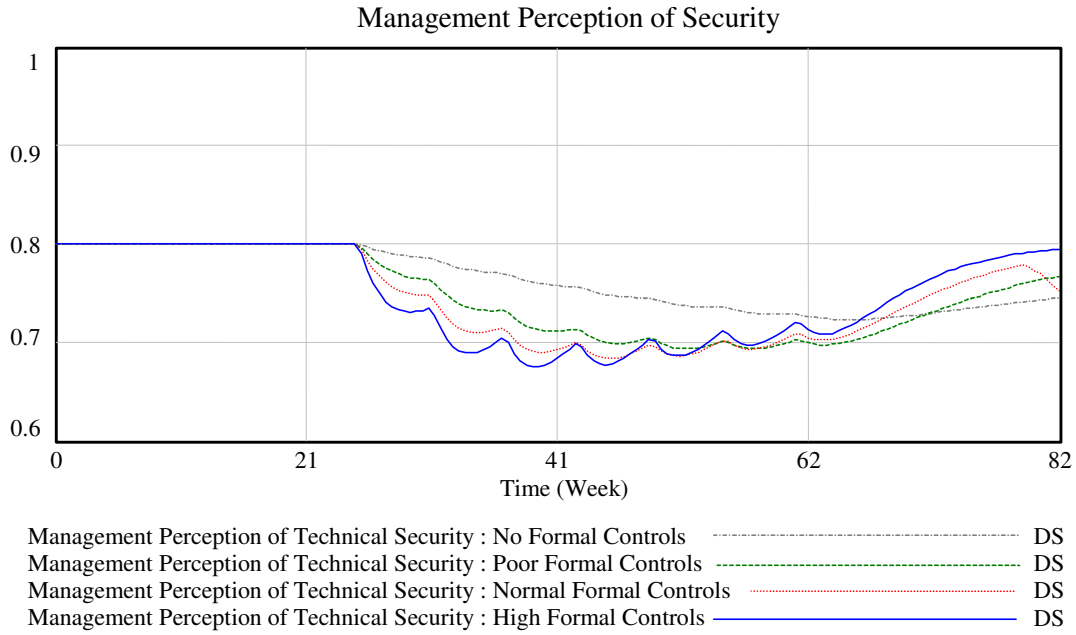


**Fig. 9:** Change in Management Perception of Security when Formal Controls increase.

First, in figure 9 we can see that the quality of management perception of security improves significantly when the level of implementation of formal controls increases. When the insider starts creating incidents in the system, which causes some minor downtime, management quickly perceives the incidents as an important risk exposure

and a reduction in security level. This improved perception lets management increase the technical security level before something worse happens (see figure 11).

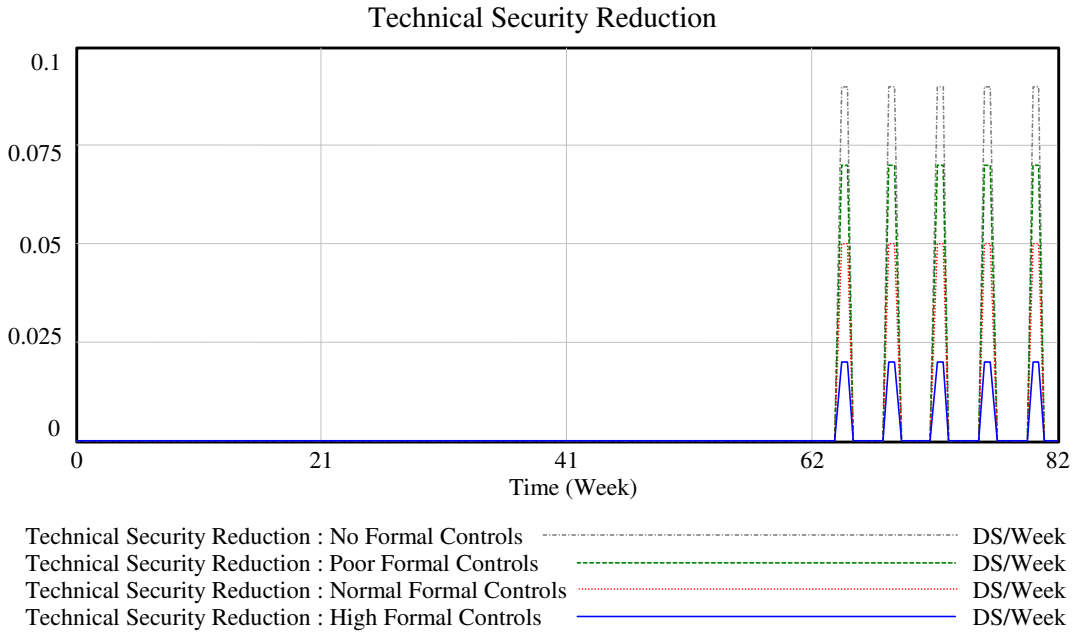


**Fig. 10:** Change in Technical Security Reduction when Formal Controls increase.

The effectiveness of increasing the formal controls can also be seen in figure 10, where the reduction of the technical security level by the insider is diminished. This happens because when formal controls are implemented (e.g. security duties are segregated or access controls are correctly designed), the insider's capacity to damage the system is reduced. Note that there is a fourfold reduction in the insider's capacity to damage the system compared to the initial simulation.

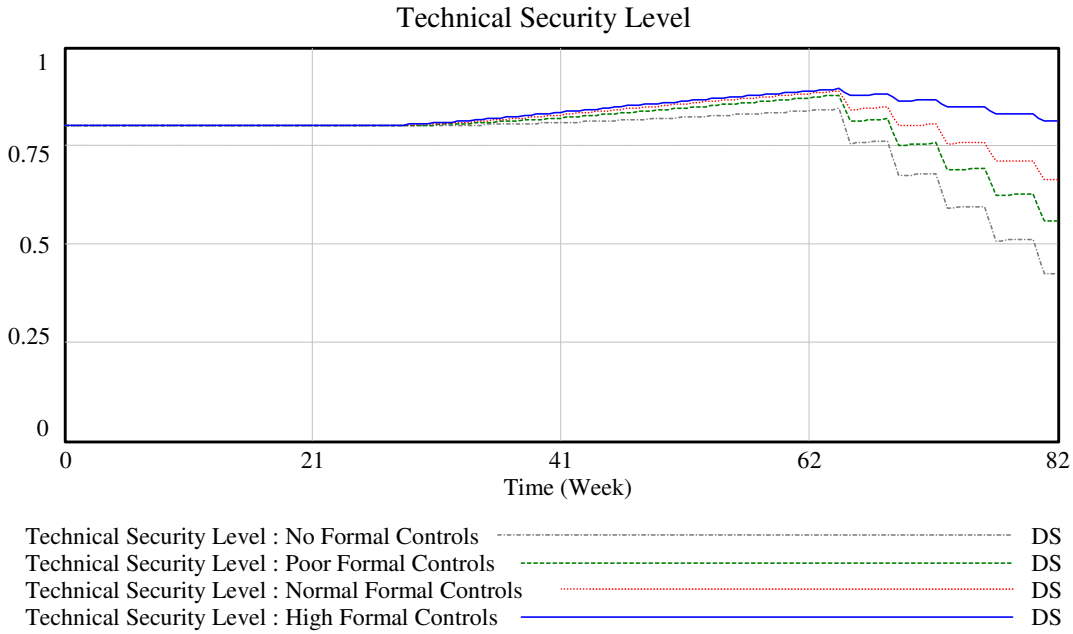


**Fig. 11:** Change in Technical Security Level when Formal Controls increase.

Another important result from increasing the level of implementation of formal controls is that the technical security level at the end of the simulation period does not fall to levels low enough to present a significant risk. As can be seen in figure 11, when no formal controls are implemented, technical security level falls to 40% of its normal level because of the insider's actions. This was a crucial factor in the Tim Lloyd/Omega case in that the impact of the time bomb was extremely high because of the diminished technical security level. As implementation of formal controls increases, the insider's actions to reduce the technical security level are less effective, and therefore the technical security level stays in an acceptable range of values.

## Learning from Incidents

A "Learning from Incidents" policy could also have been implemented at Omega. A thorough discussion of this idea is found in a parallel paper by Cooke (2003a). The kind of "incident learning system" represented by the proposed policy would include a structured analysis of incidents to better understand their causes and consequences. Such a policy may have enabled management to recognize the first incidents generated by Tim Lloyd as a threat to information system security and to take action based on this knowledge. The existence of a policy for more rigorous analysis of the precursor incidents would facilitate detection of the threat posed by Tim Lloyd to the information system.

A practical consequence of this policy could have been Lloyd's early dismissal as soon as he committed the first incidents or, at least, immediate action could have been taken to reduce Lloyd's level of access to the system. The introduction of the policy in the model can be seen in figure 12.

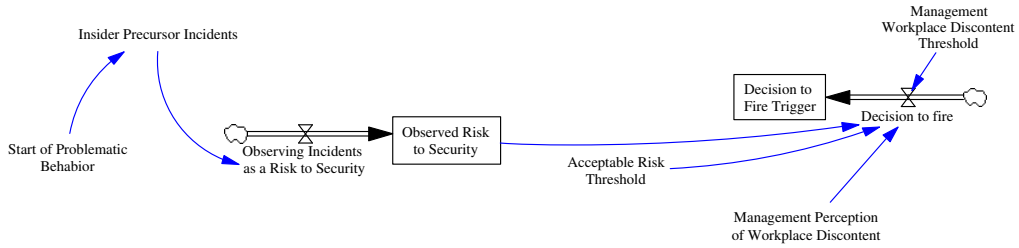


**Fig. 12:** Incident Learning System structure.

It is difficult to anticipate Tim Lloyd's response to early dismissal. In the worst case, he would have tried to attack the system anyway. However, without his preparatory actions to diminish the security level, the impact of such attack would have been significantly reduced. This can be seen in figure 13, where the impact of the attack is represented.

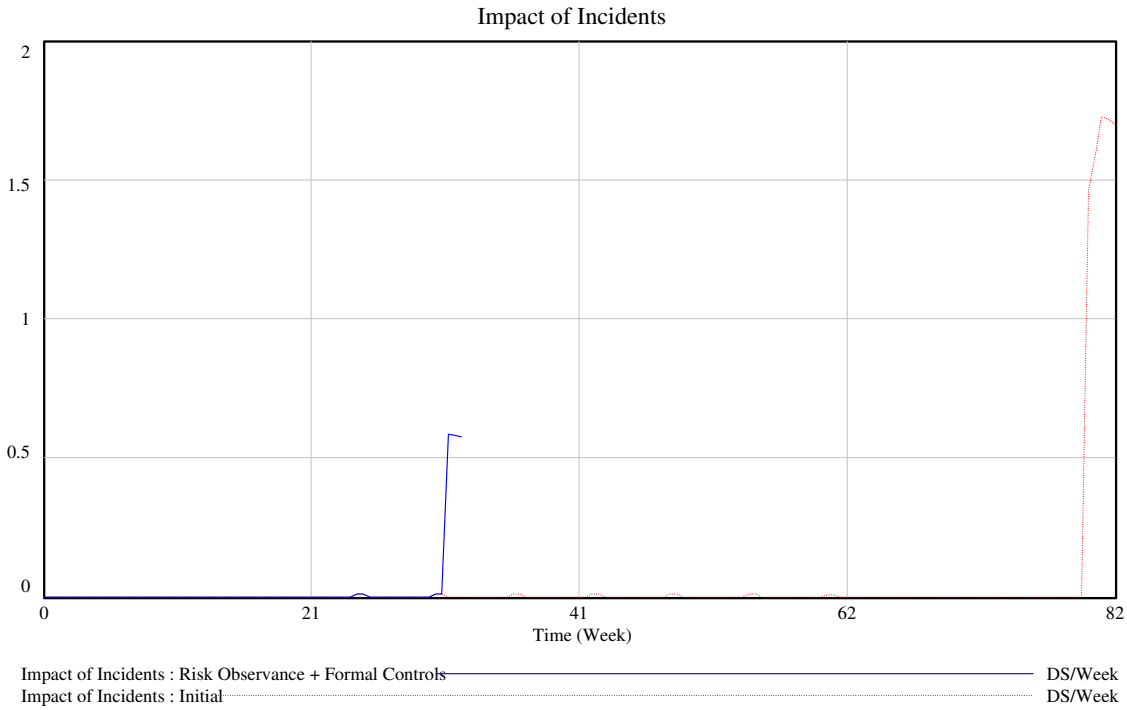


**Fig. 13:** Impact of incidents.

From a more optimistic perspective, the early dismissal of Tim Lloyd could even have prevented the attack. Together with preventative measures, Tim Lloyd may not have had the opportunity to prepare and activate an attack, no matter how desperate he was to do so. Surely, once a decision had been made to fire him, his access to the system would have been cut off completely and security personnel would have escorted him out of the building.

Chapter 10 of Mitnick and Simon (2002) states the following under the heading Saying Good-Bye to Employees: “The point has been made earlier in these pages about the need for iron-clad procedures when a departing employee has had access to sensitive information, passwords, dial-in numbers, and the like. Your security procedures need to provide a way to keep track of who has authorization to various systems. It may be tough to keep a determined social engineer from slipping past your security barriers, but don’t make it easy for an ex-employee.” This point is illustrated by the case of “the humiliated boss” (Mitnick and Simon 2002, p. 159ff) in which a disgruntled employee managed to plant pornographic slides in a budget presentation made by his former boss, despite his having been taken by surprise by his instant demotion, because of inadequate procedures to eliminate the employees’ access options following his demotion.

## Conclusions

It is important to understand that information system security is not just a matter of implementing technical security mechanisms. A good system of formal controls that has been well implemented can make a big difference to whether or not the security system is breached when an insider attack occurs. It may be too difficult to predict or to avoid an insider attack, but there is no doubt that the effect of a malicious attack can be minimized through better organizational procedures. In this sense, there must be an appropriate segregation of security tasks and other information system administration tasks in order to effectively secure the system against insider attacks. Access controls and privileges must be properly designed and supervised. No single person should control the system from "front to back" and neither should anyone have unrestricted access to the whole network.

Besides, mere technical or formal controls are still insufficient. To effectively secure the system, management should put in place some informal policies such as increasing awareness in security matters through educational and training programs, which help employees to understand:

- How the system works (or should work),
- The kind of risks that are posed to the information system,
- The three different aspects security must cover,
- The role that each employee plays in securing the system,
- The legislative sanctions to intentional misuse of information systems and enterprise-owned data (it is usually a good deterrent of insider attacks), and
- The security tools or measures employees and managers should put in place at any time, especially when becoming aware of a specific risk.

As a result, a company might devise an organizational subculture of information security, where people are aware of the risks posed to the system and are empowered to act in mitigation of them. It is very important that managers lead these kinds of initiatives, showing a public and genuine commitment to security.

Although Dhillon points out informal policies as the most cost-effective controls that an organization can implement to secure the system (Dhillon 1999), there is no doubt that direct results from these kinds of policies are more difficult to measure and might only appear in the long term.

It is important to note that management should pay special attention to any employee who is showing signs of discontent, particularly if that employee holds an information-critical position. Management must consider this kind of problematic behavior as a threat to the information system, and when detected, should monitor the network for unusual activities that may be attributed to the insider.

Although this model addresses a particularly pathological case (most system administrators don't betray their companies), it gives enough understanding of the dynamic and complex relationships between information technology, organizational structure and people in an enterprise environment, and it demonstrates that is in these complex relationships where the general problem of security (or insecurity) of an information system resides.

Although this work has been widely discussed and reviewed by several system dynamics researchers, it is still preliminary. Our effort is part of a research program involving several authors. As a next step we intend to develop a more generic model to facilitate the understanding of the complexity of information system security, paying special attention to insider attacks.

## Acknowledgement

The contribution by Agata Sawicka has been financed with a fellowship of the City of Kristiansand.

# Appendix: Stock and Flow Model Equations

## References


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

Carayon, Pascale, and Sara Kraemer. 2002. Macroergonomics in WWDU: What about computer and information system security? Paper read at 6th International Scientific Conference on Work With Display Units -- WWDU 2002 -- World Wide Work, at Berlin.

Carayon, Pascale, and M J Smith. 2000. Work organization and ergonomics. *Applied Ergonomics* 31:649-62.

Cooke, David L. 2003a. Learning from Incidents. Paper read at The 21st International Conference of the System Dynamics Society, at New York City, USA.

———. 2003b. A System Dynamics Analysis of the Westray Mine Disaster. *System Dynamics Review* 19 (2).

Dhillon, Gurpreet. 1999. Managing and controlling computer misuse. *Information Management & Computers Security* 7 (4):171-175.

———. 2001. Violation of Safeguards by Trusted Personnel and Understanding Related Information Security Concerns. *Computers & Security* 20 (2):165-172.

Dhillon, Gurpreet, and Steve Moores. 2001. Computer crimes: theorizing about the enemy within. *Computers & Security* 20 (8):715-723.

Gaudin, Sharon. 2002. *Case Study of Insider Sabotage: The Tim Lloyd/Omega Case*. Computer Security Journal 2000 [cited 20 October 2002]. Available from http://www.gocsi.com/pdfs/insider.pdf.

Gonzalez, Jose J, and Agata Sawicka. 2002. A Framework for Human Factors in Information Security. Paper read at WSEAS International Conference on Information Security (ICIS'02), at Rio de Janeiro, Brazil.

———. 2003. The Role of Learning and Risk Perception in Compliance. Paper read at The 21st International Conference of the System Dynamics Society, at New York City, USA.

Mitnick, Kevin D, and William L Simon. 2002. *The art of deception : controlling the human element of security*. Indianapolis, IN, USA.

O'Brien, James A. 2002. *Management information systems : managing information technology in the e-business enterprise*. Boston: Irwin/McGraw-Hill.

Power, Richard. 2000. *Tangled Web: Tales of Digital Crime from the Shadows of Cyberspace*. 1 ed. Indianapolis, IN: QUE.

———. 2002. *CSI/FBI Computer Crime and Security Survey* 2002 [cited October 20 2002]. Available from http://www.gocsi.com/pdfs/fbi/FBI2002.pdf.

Scalet, Sarah D. 2003. *Why biggest security risks are inside organizations*. CIO Magazine 2002 [cited 10/01/2003 2003]. Available from http://www.cio.com/archive/060102/doom_content.html.

Schneier, Bruce. 2000. *Secrets and Lies: Digital Security in a Networked World*. New York: John Wiley & Sons, Inc.

Schultz, E. Eugene. 2002. A framework for understanding and predicting insider attacks. *Computers & Security* 21 (6):526-531.

Shaw, Erik, Keven G Ruby, and Jerrold M Post. 2002. *The insider threat to information systems* 1998 [cited 01 Dic 2002 2002]. Available from http://www.pol-psych.com/sab.pdf.

Smith, M J, and P Carayon-Sainfort. 1989. A balance theory of job design for stress reduction. *International Journal of Industrial Ergonomics* 4:67-79.

Back to the Top