The Role of Incident Reporting in Reducing Information Security Risks

Finn Olav Sveen[*, **], Jose Maria Sarriegi[*] & Jose J. Gonzalez[**]

[*]Tecnun (University of Navarra), Manuel de Lardizábal 13, 20018 San Sebastián, Spain

[**]University of Agder, Service Box 509, 4898 Grimstad, Norway and NISlab, Gjøvik University College, 2802 Gjøvik, Norway
finnos@uia.no, jmsarriegi@tecnun.es, jose.j.gonzalez@uia.no

Abstract

This paper examines the role of information security incident reporting systems in the wider context of an information security management system. This work is based on four group model building workshops with participants from mnemonic AS, a Norwegian Managed Security Services Provider. We found that incident reporting is a crucial component in creating information security awareness among information system users. Our research indicates that increasing incident reporting rates does not necessarily mean poor security, but rather that the organisation is becoming more security aware, and, arguably, less exposed to information security risks. However, in an organisation with poor awareness, it is possible that incident reporting rates and risk increases simultaneously. Analogous results are known about industrial safety reporting systems and risk of organisational accidents.

Keywords: System Dynamics, Information Security, Incident Reporting, Information Security Management System, Information Security Incidents, CSIRT

Introduction

Modern corporate information systems are extremely complex, technically, as well as socially and organisationally (Schneier 2000). Combined with rapid change in technology, its use and threats, the likelihood that some vulnerabilities remain undetected is substantial, despite a well run information security management system (ISMS). There should therefore be procedures for incident detection and reporting. Indeed, incident reporting systems (IRS) are recommended in many information security standards, including ISO 27001:2005.

Johannes Wiik pioneered the use of System Dynamics for studying information security IRS (Wiik 2007; Wiik, Gonzalez, and Kossakowski 2005; Wiik and Kossakowski 2005). Wiik studied DFN-CERT, a major coordinating CSIRT. Its constituency is the German Research Network, which is the network backbone connecting most of the research institutions in Germany. DFN-CERT coordinates incident response across many different entities. Underreporting and cover up of incidents; skill and knowledge at customer sites; lack of management support; needing more budget and/or resources; lack of trained staff and lack of funding, were identified as problems. Wiik also found that the observed variations in the number of reporting sites were mainly caused by internal DFN-CERT policies.

In this paper we add to the sparse literature on the dynamics of IRS by reporting on MIRSA (Modelling Information Security Reporting Systems and Awareness), a collaborative project between three educational institutions and a private company. These are the University of Agder, Gjøvik University College and mnemonic AS in Norway, and Tecnun (University of Navarra) in Spain. mnemonic AS is one of Norway's largest information security companies. In addition to operating an internal IRS, mnemonic also advices customers on implementation of IRS. mnemonic's CSIRT is not a coordinating team, but a small centralised internal team, whose primary job is to respond directly to incidents.

Unfortunately, mnemonic lacks data in written and numerical form on incident reporting rates. We had to rely on the knowledge of experts who work daily with the incident reporting system. This knowledge is fragmented, each person holding pieces of the puzzle, making Group Model Building (GMB) ideal for the task (Andersen and Richardson 1997; Richardson and Andersen 1995; Vennix 1996). Four GMB workshops were held in May and June 2008, two lasting one day each and another two lasting half a day each. One more half day workshop was conducted in September that year, with the purpose of validating the results.

The modelling team fills different roles (Andersen and Richardson 1997; Richardson and Andersen 1995; Vennix 1996). Four roles, the facilitator, the process consultant, the modeller and the recorder, can be considered a bare minimum. Unfortunately, our modelling team was small, consisting only of two people for the majority of the workshops. Each team member wore multiple hats, which presented a considerable challenge. We managed by taking turns being the facilitator, while the other acted as modeller, process consultant and recorder.

During the workshops, concept models of the type described by Richardson were used to engage the participants in discussion (Richardson 2006). The first full simulation model was developed between workshops three and four, and subsequently improved. In this paper we present the final simulation model and key dynamics in mnemonic's information security IRS. The remainder of the paper consists of the sections Reference Modes, Model Description, Simulation Runs, Model Usefulness, and Conclusions.

Reference Modes

A necessary starting point for modelling is to know the behaviour of key variables, as the goal of the modelling effort is to discover why those variables behave as they do. Unfortunately, statistical and written data were in short supply, and not all of the data could be released, due to confidentiality requirements. We therefore asked the workshop participants to define indicators and draw three graphs for each indicator, the current, worst case and best case behaviour, i.e., to assess what would indicate a worsening or improving situation. The reference modes are shown in Figure 1.

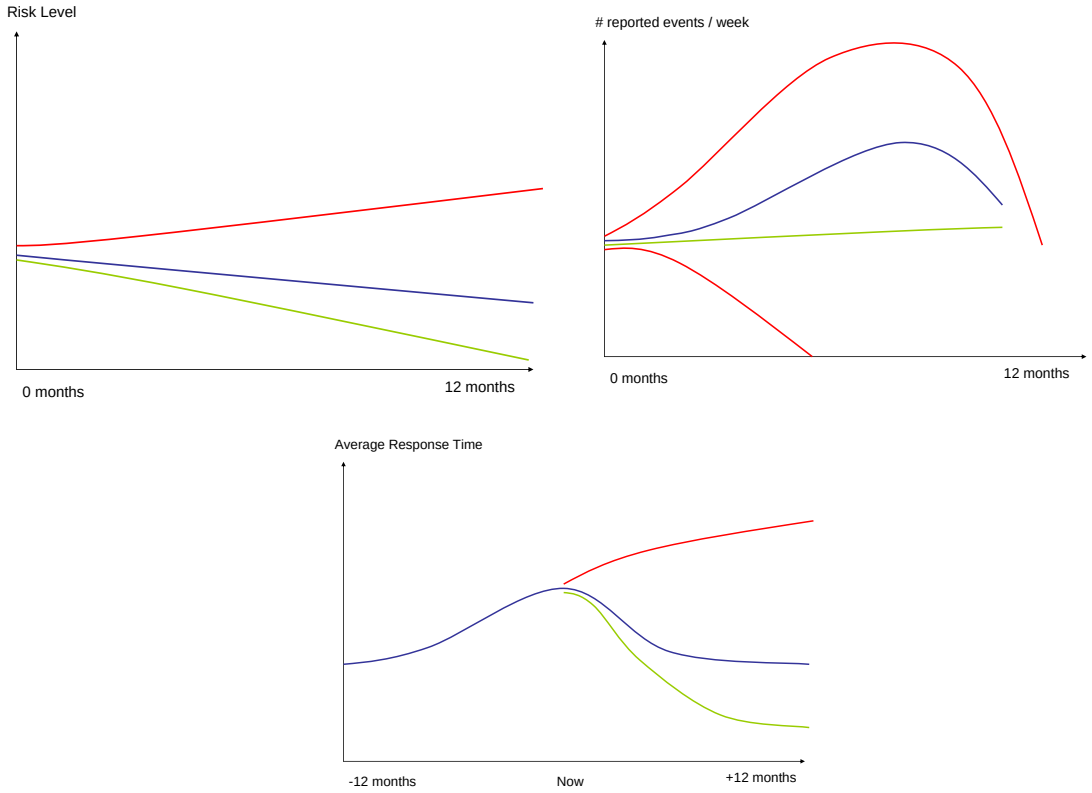

Figure 1: Key reference modes. The blue line indicates current situation, green best case behaviour and red worst case behaviour.

Risk Level evaluated in external risk assessments have decreased. Although, the top left graph in Figure 1 only shows a 12 month period, the current behaviour line follows the same behaviour as that seen over several years.

In information security it is customary to differentiate between incidents, where an actual security breach has occurred, and events, which are unsuccessful breaches or other security related occurrences. # Reported Events measures the aggregate of both events and incidents. It is currently increasing and has been for some time. Increased focus on incident reporting in the near past may have contributed to this increase. The reduction in Risk Level indicates that # Reported Events should start to reduce, as underreporting is minimized.

Average Response Time is the delay before incident reports are responded to. It is currently decreasing, after a temporary increase owing to high workload burden. Resources for incident handling were therefore added to reduce response time.

From the behaviour of these indicators it is possible to define the problem to be solved: How can the rise in # Reported Events, Work Hours for Incident Handling and Response Time be stabilized or reduced, without reversing the reduction in Risk Level. In the next section we describe the structure of the final simulation model.

Model Description

An IRS is part of an ISMS, whose purpose is to control risks to the business' information assets, which may be stored in computer systems, on paper or in people's

heads. A comprehensive approach to risk control is needed. Two methods have traditionally been employed: Technical Controls and Security Policies.

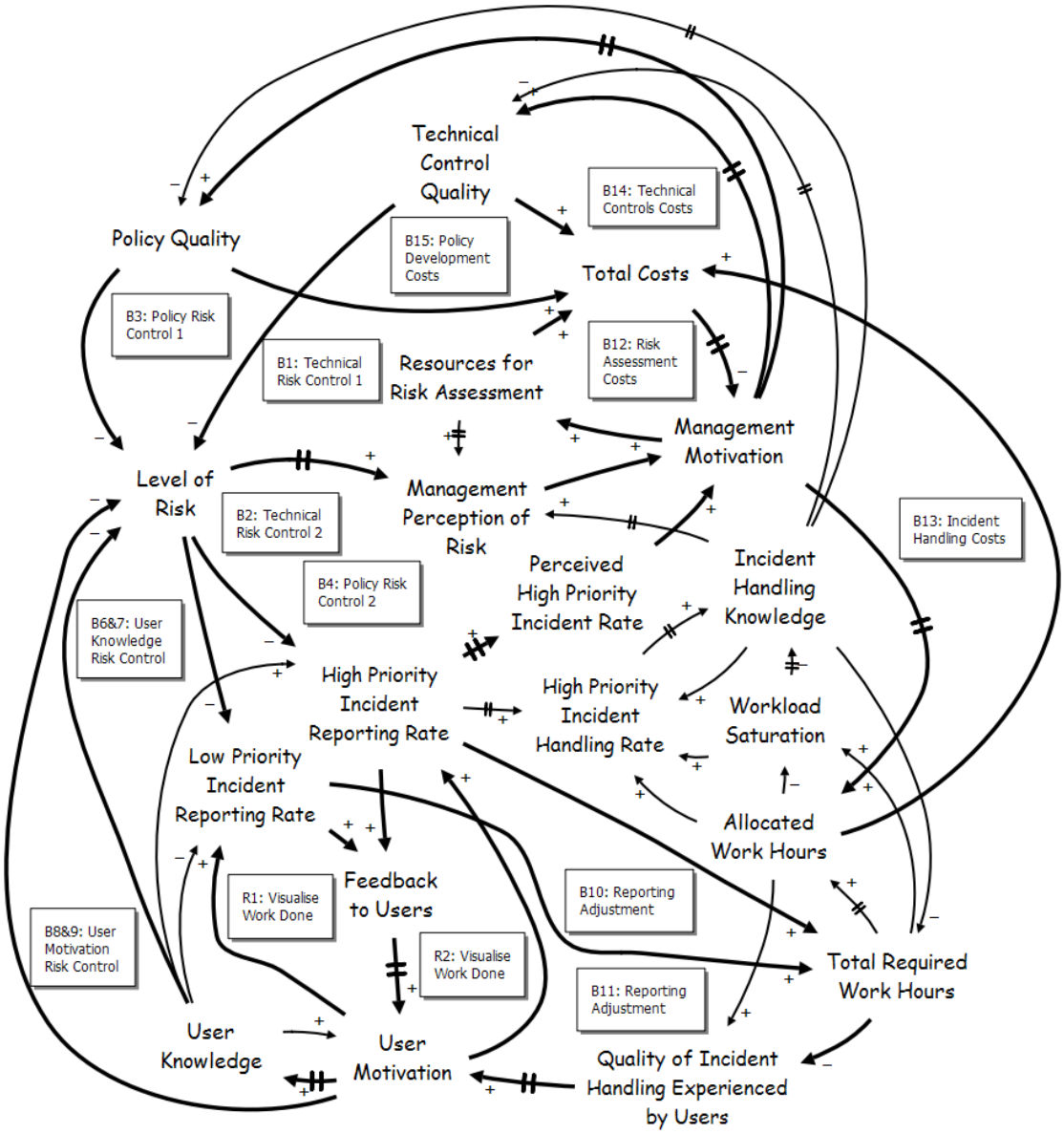

Figure 2: CLD with key variables in mnemonic incident reporting system model. Thick lines indicate that the link form part of one of the marked loops.

Technical Controls

Technical controls are used to protect confidentiality and integrity of information and information systems, as well as ensuring availability. They range from physical door locks, to sophisticated encryption schemes to protect information as it travels over computer networks.

The degree to which technical controls are adapted to the current technology and risk situation, determines their efficiency. This is represented in the model in Figure 2, by the variable *Technical Control Quality*. If its value is unity, the technical controls are highly adapted, if it is zero, they are poorly adapted. An increase in *Technical Control Quality* reduces *Level of Risk*, and vice versa. *Level of Risk* is also defined as a value between unity and zero, unity is equal to high and zero is low. Management perceives

Level of Risk partially through risk assessments, which are performed yearly, meaning that there is a one year perception delay between *Level of Risk* and *Management Perception of Risk*.

Management Perception of Risk influences *Management Motivation*, which represents upper management's commitment to information security, and is modelled as a value between unity and zero, where unity is high motivation, and zero is low. If *Management Perception of Risk* rises, *Management Motivation* increases. In turn, *Management Motivation* determines the desired level of *Technical Control Quality*. There is a delay between *Management Motivation* and *Technical Control Quality*, which represents the implementation time.

Together, the variables *Management Motivation*, *Technical Control Quality*, *Level of Risk* and *Management Perception of Risk* form the balancing loop *B1: Technical Risk Control 1*. The loop balances risk with management's perception of risk. A second loop, *B2: Technical Risk Control 2*, contains almost the same variables as *B1*, substituting *Management Perception of Risk* with *Perceived High Priority Incident Rate*. It is another balancing loop which functions as another method of perceiving risk.

High priority incidents are incidents that are considered critical to mnemonic's security. They are usually not disastrous, but enable the company to learn about its systems. Unlike risk assessments, reports on incident activity reach upper management more frequently. The delay in perceiving *High Priority Incident Reporting Rate* is therefore shorter.

Information Security Policies

Security Policies are the second method traditionally used to control information security risk. Security Policies define rules for proper conduct when handling information and information systems. They define appropriate user behaviour, recovery strategies and how technical systems should be maintained[1].

Policy Quality is defined in the same manner as *Technical Control Quality*, that is, the degree of adaptation to the current technology and risk situation. *B3: Policy Risk Control 1* is an analogous loop to *B1*. It is balancing and includes *Management Motivation*, *Policy Quality*, *Level of Risk* and *Management Perception of Risk*. The loop *B4: Policy Risk Control 2* includes the variables *Management Motivation*, *Policy Quality*, *Level of Risk*, *High Priority Incident Reporting Rate* and *Perceived High Priority Incident Reporting Rate*. The two loops control risk.

The Users

Most threats to information systems usually involve the user, who may have to visit a webpage, click on a link or open an email attachment to give malware a chance to infect the system. The attack vector may also not involve computers, for example impersonation over the phone or face to face. The user has a central role in ensuring the security of information and information assets.

[1] Note that this is different from the SD concept of policy, which is more akin to the term strategy.

Users are also relied upon to report information security incidents. Users are defined broadly, including workers, but also network and system administrators who are not primarily security experts. If any user detects something suspicious, it should be reported. However, security is not their primary job, making motivation an issue.

Users' commitment to information security is represented by *User Motivation*, which is defined in the same manner as *Management Motivation.* An increase in *User Motivation* causes an increase in *High Priority Incident Reporting Rate* and *Low Priority Incident Reporting Rate*, and vice versa.

Low priority incidents are not unimportant, but compared to high priority incidents, they are not critical and the learning potential is limited. An example is leaving a door ajar by accident. Low priority incidents are, to some extent, noise that take up valuable time and resources.

If an incident is reported, but the perceived quality of the response is low, it has negative consequences for *User Motivation.* Increases in *High Priority Incident Reporting Rate* and *Low Priority Incident Reporting Rate*, cause *Total Required Work Hours* to increase. Management may not immediately recognise the need to increase resources, as higher reporting rates may only be temporary, therefore a wait-and-see attitude may be adopted. It is also difficult to find people with the required skill set, making the hiring process time consuming. Personnel may have to be trained internally. There is a long time delay before *Allocated Work Hours* matches *Total Required Work Hours*. This discrepancy reduces the users' experienced quality of the incident handling process. Response time increases, and in some cases, incident reports may not be responded to at all. Stressed incident handlers may have to cut corners, which means that analyses will be less thorough, increasing the chance for relapse.

Hence, an increase in *Total Required Work Hours* decreases *Quality of Incident Handling Experienced by Users*. The latter variable has been modelled as a ratio between *Allocated Work Hours* and *Total Required Work Hours*. Quality has many components, but the simple expression captures discrepancy between allocated and needed resources, which are the origin of the quality problems. One part of quality is Response Time, shown in Figure 1. An increase in Response Time is equal to falling quality. Response Time was not modelled directly since this is a variable with a time frame of hours, at most a few days, whereas the simulation runs over several years.

If *Quality of Incident Handling Experienced by Users* fall, *User Motivation* also decreases, in turn decreasing *High Priority Incident Reporting Rate* and *Low Priority Incident Reporting Rate*. Thus, two loops have formed: *B10* and *B11*: *Reporting Adjustment*. These two loops balance the high and low priority incident reporting rates to available incident handling resources.

Response time has historically increased, but is now decreasing (Figure 1). The increase prompted the development of a mechanism to counteract the effect of falling quality on *User Motivation*. Care is taken to communicate the importance of reporting incidents and what has actually been done in response to incident reports. This is represented by the links from *Low Priority Incident Reporting Rate* and *High Priority Incident Reporting Rate* to *Feedback to Users*. Increases in the two former variables,

cause increase in the latter. When *Feedback to Users* increase, *User Motivation* also increases. These two loops, *R1* and *R2*: Visualize Work Done, creates a reinforcing effect that counteracts *B10* and *B11: Reporting Adjustment.*

Reporting of incidents allows the organisation to learn about vulnerabilities in their information systems and procedures, allowing for the implementation of countermeasures. In this way, the users contribute indirectly. The users also contribute directly to risk reduction. Motivated users are more likely to keep up to date on current corporate information security policies specifically and information security in general, and are more likely to follow the policies.

The first mechanism is represented by the link from *User Motivation* to *User Knowledge*, which represents the users' level of knowledge of information security and organisational policies. An increase in *User Motivation* causes an increase in *User Knowledge*, which in turn decreases *Level of Risk.* Lower *Level of Risk* means that the probability of incidents occurring is reduced; hence *Low Priority Incident Reporting Rate* and *High Priority Incident Reporting Rate* decrease. Consequently, *Feedback to Users* also decreases, in turn decreasing *User Motivation*. The variables form the balancing loops *B6* and *B7: User Knowledge Risk Control*, counteracting the effects of *R1* and *R2*.

It is not sufficient for the users to have knowledge of policies and information security; they must also be motivated to use that knowledge. Therefore, *User Motivation* influences *Level of Risk*. Two balancing loops, *B8* and *B9* are formed. They follow nearly the same paths as *B6* and *B7*, only omitting *User Knowledge*. These loops also counteract *R1* and *R2*.

The Cost of Security

There is a trade-off between achieving the lowest possible risk, and low costs. It takes time and resources to perform risk assessments; develop policies; develop, implement and maintain technical solutions; and handle incidents. The balancing loops *B12* to *B15*, describe how increases in *Resources for Risk Assessment*, *Technical Control Quality*, *Policy Quality* and *Allocated Work Hours*, in turn increase *Total Costs*, which negatively impacts *Management Motivation*, and vice versa.

The IRS that has been described is complex, with a large number of loops. Only the most important have been described here. To determine the behaviour of the system we next examine three simulation scenarios.

Simulation Runs

A first test of the model's behaviour is its ability to recreate the behaviour of the reference modes. This is the purpose of Base Run, which is described in the next section and compared to the indicators described in Figure 1.

Base Run

At the start of the simulation there are sufficient resources to handle all incoming incidents. The simulation runs over a time period of three years, from 1st of January 2007 to 1st of January 2010, a period of approximately one year before project start to two years beyond, giving sufficient time for observing long term effects.

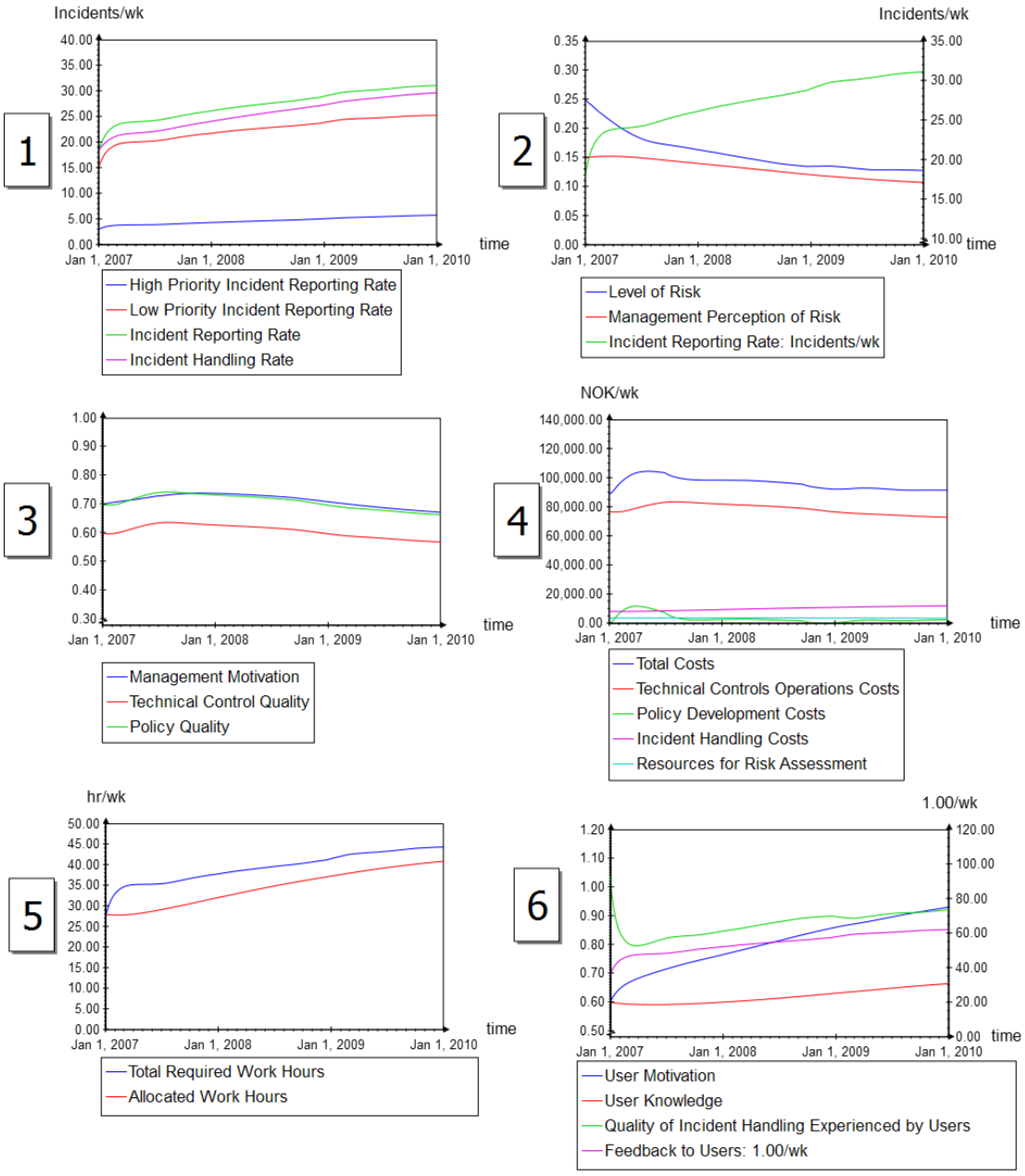

Figure 3: Responses of key variables in Base Run.

Graph no. 1 in Figure 3, shows the development of *High Priority Incident Rate* and *Low Priority Incident Rate*. In the first few months, there is a sharp increase, which is later replaced by steady growth lasting throughout the simulation. This is consistent with # Reported Events (See Figure 1).

Level of Risk is reduced throughout the simulation (Figure 3, graph 2). The rate of decrease is largest during the first six months, after which the decrease is steady until the end of the simulation. The difference between *Management Perception of Risk* and *Level of Risk* is high at the start of the simulation, but it diminishes throughout.

Level of Risk and *Incident Reporting Rate*[2] exhibit diverging behaviour. This is consistent with the two indicators # Reported Events and Risk Level, which also have diverging behaviour (See Figure 1).

The growth in *High Priority Incident Rate* raises management's concern about security issues. Consequently, the loops *B2* and *B4* become stronger, and *Management Motivation* is further strengthened (See Figure 3, graph 3). Policy development is increased and new technical controls put in place. This aids in reducing *Level of Risk*, but also increases costs (Figure 3, graph 4). The reduced risk (*B1* and *B3*) and increased costs (*B12* to *B15*) combine to reduce *Management Motivation* to below the initial level. Less money is spent on policy development, technical controls, incident handling and risk assessment. This slows the reduction in *Level of Risk.*

The increase in *Incident Reporting Rate* causes an increase in *Total Required Work Hours* (Figure 3, graph 5). The significant time delays in hiring new or transferring existing staff to incident handling makes *Allocated Work Hours* increase slower.

The gap between *Total Required Work Hours* and *Allocated Work Hours* makes the loops *B10* and *B11* more powerful. The falling *Quality of Incident Handling Experienced by Users* has the potential to reduce *User Motivation* (Figure 3, graph 6). However, the communication strategy, expressed through *R1* and *R2,* is sufficiently strong to counteract reduced quality. *Feedback to Users* is high enough to increase *User Motivation*, which causes an increase in *Low Priority Incident Reporting Rate* and *High Priority Incident Reporting Rate*.

After the initial creation of the gap between *Total Required Work Hours* and *Allocated Work Hours*, continuously added resources slowly close it. *Quality of Incident Handling Experienced by Users* starts to increase and keeps increasing slowly throughout most of the simulation, further reinforcing *User Motivation*. In other words *B10* and *B11* become weaker.

No training is given in this scenario; users must acquire knowledge on their own. This is a time consuming task and *User Knowledge* actually decreases slightly in the first year of the simulation (Figure 3, graph 6). However, as *User Motivation* increases, users put in more effort to learn about security and security policies. This creates a reinforcing effect as deeper knowledge about security also makes users care more about security, increasing *User Motivation*. However, the increase in *User Knowledge* is not sufficient to significantly influence the ratio of high to low priority incident reports.

Initially, *Policy Quality* and *Technical Control Quality* contribute to decrease *Level of Risk.* But, when *Management Motivation* decreases, less is spent on policies and technical controls. Technology changes throughout the simulation, causing *Policy Quality* and *Technical Control Quality* to reduce. This force slows the reduction in *Level of Risk.*

[2] *Incident Reporting Rate* is the aggregate of *High Priority Incident Reporting Rate* and *Low Priority Incident Rate*.

User Motivation is the biggest contributor to the reduction in *Level of Risk.* A shift of the security burden from policy and technical controls towards the users occurs after the first six months. Management is satisfied with the security level, and expenses are rising, which reduces *Management Motivation* and consequently *Policy Quality* and *Technical Control Quality* also reduces. However, the loops *R1* and *R2* are strong enough to maintain the lower *Level of Risk*.

Although, resources needed for incident handling increase, this scenario does yield a good result with regards to reductions in risk. The main contributor to the increasing *Incident Reporting Rate* is the strategy of encouraging users to report. *Feedback to Users* increases, causing *User Motivation* to increase. As a consequence, users report more incidents, increasing the workload of the incident handling team, which reduces quality. But, the users also become more aware of security issues, reducing *Level of Risk.*

No Feedback to Users

In Base Run, the communication and recognition that users receive when they report, expressed through the loops *R1* and *R2* and *Feedback to Users*, have been driving the rise in *Incident Reporting Rate*. In this scenario, that feedback mechanism will be turned off, allowing us to examine a system without focus on incident reporting.

Incident Reporting Rate increases more slowly than in Base Run (Figure 4, graph 1), and the incident handling team is able to handle all incoming incidents, as there is virtually no gap between *Total Required Work Hours* and *Allocated Work Hours* (Figure 4, graph 5).

However, *Level of Risk* develops disastrously (Figure 4, graph 2). It increases steadily throughout the simulation run. *Management Perception of Risk* increases, which increases *Management Motivation* (Figure 4, graph 3). The loops *B1* and *B3* become stronger. *Policy Quality* and *Technical Control Quality* increase, but this is not enough to counteract the influence of falling *User Motivation* on *Level of Risk.*

Feedback to Users has no influence in this scenario. Consequently, *Quality Experienced by Users* becomes more central in determining *User Motivation*. This is expressed through the loops *B10* and *B11,* which become dominant (Figure 4, graph 6). *Quality Experienced by Users* is higher than in Base Run, but it is lower than unity in the whole simulation period, which reduces *User Motivation*.

User Knowledge also falls because the users are no longer as interested in keeping up to date on information security. When *User Knowledge* is reduced, *User Motivation* is negatively impacted. This effect is triggered by the fall in *Quality of Incident Handling Experienced by Users*, and then reinforces itself.

This scenario shows the importance of taking the users seriously and explicitly communicating why they should report incidents and how their reports are handled. Increasing *User Motivation* is crucial in reducing *Level of Risk.*

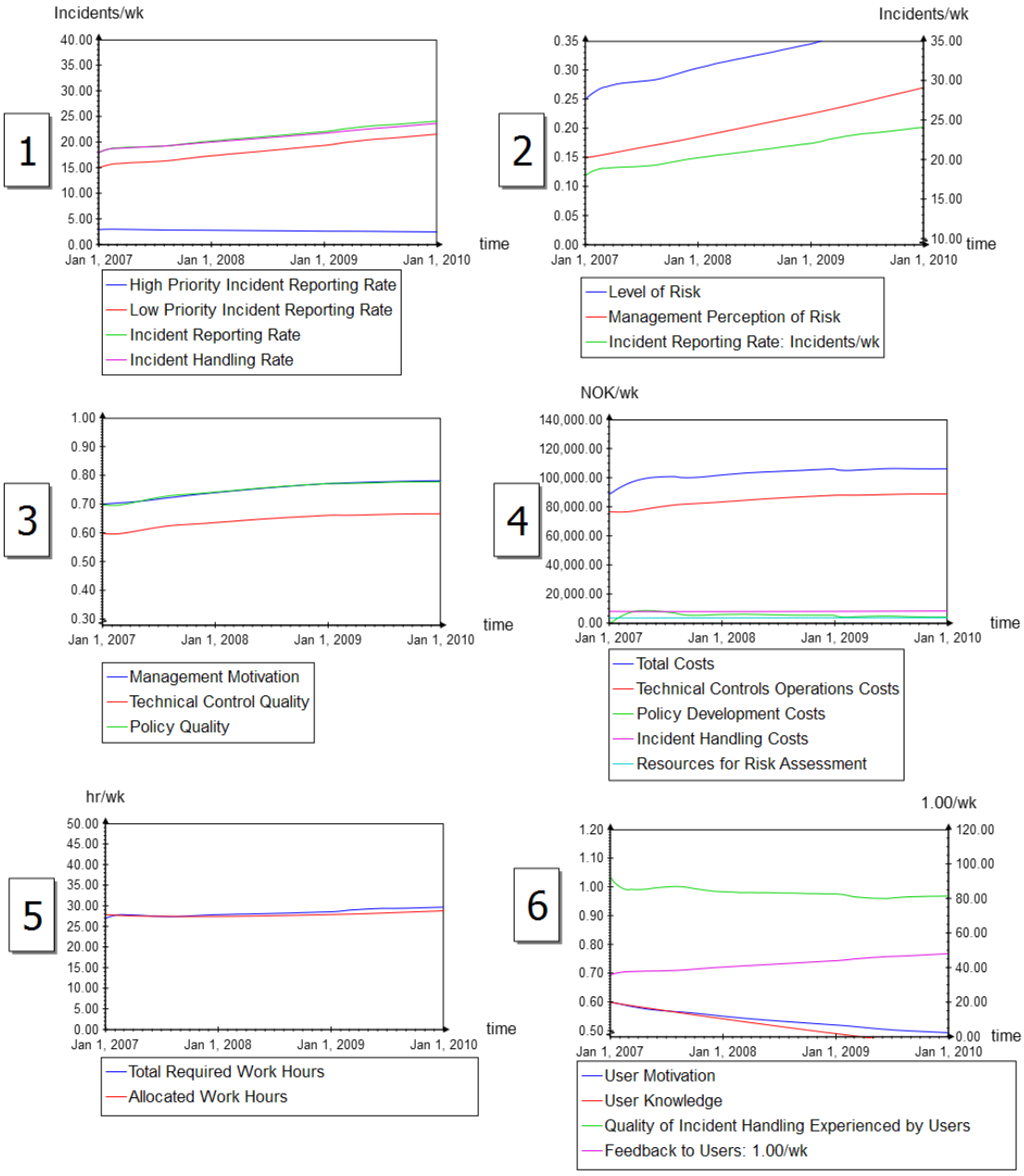

Figure 4: Responses of key variables in No Feedback to Users.

Commitment to Zero Risk

With respect to *Level of Risk*, Base Run is a successful scenario, especially when compared to No Feedback to Users. However, one problem in Base Run is that management's commitment waivers when *Level of Risk* is reduced. This is the same as when a student achieves a good grade on a test, relaxes because the target has been reached, and then experiences lower grades on the next test. In Base Run, *Level of Risk* did not increase after decreasing, but levelled off because the security burden was shifted towards the users who were motivated owing to good communication regarding reporting of incidents. This scenario tests what happens when management's commitment does not waiver. Specifically, this means that *Management Motivation* is unaffected by reductions in *Level of Risk*.

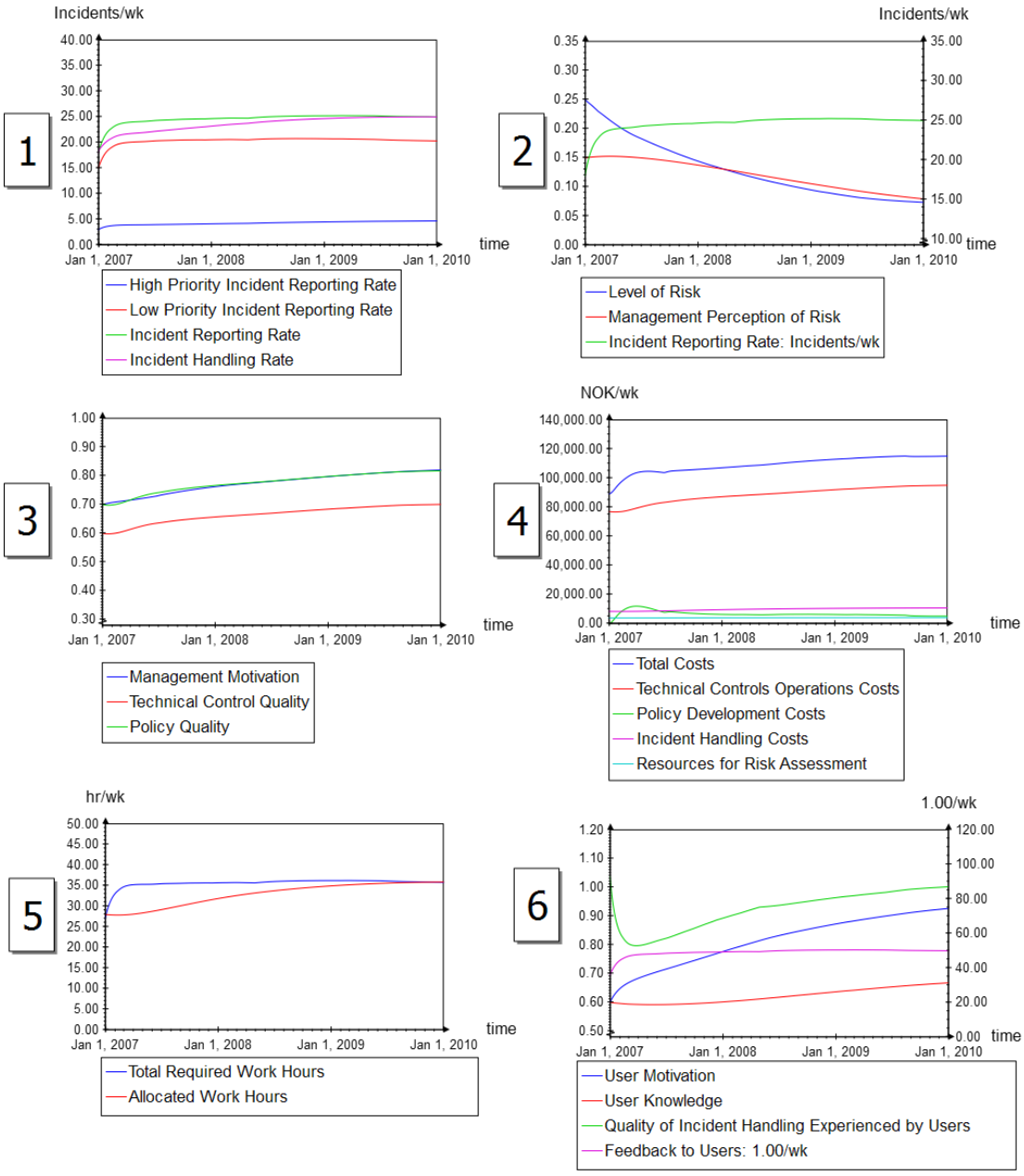

Figure 5: Responses of key variables in Commitment to Zero Risk.

In this scenario, *Policy Quality* and *Technical Control Quality* increase as a result of increasing *Management Motivation* (Figure 2, *B1* and *B3*, and Figure 5, graph 3). *Level of Risk* is therefore reduced, making the loops B6 to B9 stronger. This limits the increase in *Incident Reporting Rate*, which increases less than in Base Run (Figure 5, graph 1).

Since *Level of Risk* is lowered, fewer incidents occur. Consequently, there are fewer incidents to report. The loops B6 to B9 act to further limit the increase in *Incident Reporting Rate*, by making *R1* and *R2* less powerful. This causes *Allocated Work Hours* to actually reach *Total Required Work Hours* near the end of the simulation period (Figure 5, graph 5). The incident handling team does not have to utilise the safety valve of not handling low priority incidents. As a result, *Quality of*

Investigation Experienced by Users recovers more rapidly. Even if *R1* and *R2* are weaker in this scenario, *User Motivation* still increases at a good pace.

The only drawback in this scenario is the increasing costs. However, as *Level of Risk* has been substantially reduced, the chance of disastrous security breaches occurring should be much lower. Information security is a bit like insurance. It is not possible to win against the insurance company (except by engaging in fraud). For the house owner, insurance will never be profitable, but it is crucial if the house burns down.

Model Usefulness

We cannot take much comfort in statistical processes leading to validation support of complex systems (Forrester and Senge 1980). Information delays and feedback create non-linear behaviours outside the range of statistical inference. This makes statistical tools hard to use. Furthermore, statistical data was largely unavailable. The pragmatic approach towards validation of complex models is to attempt to break them, and reflect on the findings. Each time a model passes a concerted attempt to challenge its contents confidence is built in its conclusions (Barlas 1989, 1996; Forrester and Senge 1980). We have considered three broad categories of tests for this work.

Model Boundary and Formulation

Our model is built to represent the effects of security incident management within an organization. It contains a set of plausible forces that would affect the general tendencies of individuals in the firm. The relationships between psychological variables are considered from the basis of aggregate or average behaviours anticipated in the GMB workshops. These assumptions are made clear and we have tested them by examining if the model outcomes change as assumptions are varied.

Structural Validity

The model was scrutinised for structural inconsistencies in the last workshop with participants from mnemonic. We also considered whether it is built in accordance with extant theory. The information security literature highlights the role of the user in achieving high security, which is consistent with our results (Albrechtsen 2007; Hitchings 1995; Kruger and Kearney 2006). We have also performed unit testing to detect mathematical inconsistencies in equation formulation.

Behavioural Validity

Written and numerical data was limited; the workshop participants instead helped us develop reference modes, which the model is capable of reproducing. The model was further examined under extreme conditions.

Conclusions

The contrast between Base Run and No Feedback to Users is telling. In the first, *Level of Risk* is reduced while *Incident Reporting Rate* increases. In the second, *Level of Risk* goes up and *Incident Reporting Rate* increases, because sufficient information security awareness is not created among the users.

In Base Run, the explicit communication strategy towards users creates this awareness, which has positive consequences for the performance of the ISMS. High incident reporting rates do not necessarily mean poor security. But rather that there is more

awareness of security issues, and therefore more is done to reduce risk. Still, as was shown in *Commitment to Zero Risk*, it is important that management stays committed and does not relax once good results have been achieved.

Similar dynamics have been observed in industrial safety IRS (Jones, Kirchsteiger, and Bjerke 1999; Sveen, Rich, and Jager 2007; Sveen, Sarriegi, and Gonzalez 2007), indicating that there might be a generic structure that has wider validity. It is likely that the dynamics found in this paper can be extended to security in general, not just information security. However, more needs to be done to establish whether this is the case.

Acknowledgements

We thank mnemonic for participating in the project and Dynaplan for providing the excellent Smia SD modelling software for free. It made implementation and analysis much easier!

References

Albrechtsen, Eirik. 2007. A qualitative study of users' view on information security. *Computers & Security* 26:276-289.

Andersen, David F., and George P. Richardson. 1997. Scripts for Group Model Building. *System Dynamics Review* 13 (2):107-129.

Barlas, Y. 1989. Multiple tests for validation of system dynamics type of simulation models. *European Journal of Operations Research* 42:59-87.

———. 1996. Formal aspects of model validity and validation in system dynamics. *System Dynamics Review* 12 (3):183-210.

Forrester, Jay Wright, and Peter M. Senge. 1980. Tests for Building Confidence in System Dynamics Models. In *System Dynamics*, edited by A. A. Legasto, Jr. and e. al. New York: North-Holland.

Hitchings, Jean. 1995. Deficiencies of the Traditional Approach to Information Security and the Requirements for a New Methodology. *Computers & Security* 14:377-383.

Jones, Simon, Christian Kirchsteiger, and Willy Bjerke. 1999. The Importance of Near Miss Reporting to Further Improve Safety Performance. *Journal of Loss Prevention in the Process Industries* 12 (1):59-67.

Kruger, H.A., and W.D. Kearney. 2006. A prototype for assessing information security awareness. *Computers & Security* 25:289-296.

Richardson, George. 2006. Concept Models. Paper read at The 24th International Conference of the System Dynamics Society, July 23-27, at Nijmegen, The Netherlands.

Richardson, George P., and David F. Andersen. 1995. Teamwork in Group Model Building. *System Dynamics Review* 11 (2):113-137.

Schneier, Bruce. 2000. *Secrets and Lies*: Wiley Computer Publishing.

Sveen, Finn Olav, Eliot Rich, and Matthew Jager. 2007. Overcoming Organizational Challenges to Secure Knowledge Management. *Information Systems Frontiers* 9 (5):481-492.

Sveen, Finn Olav, Jose M. Sarriegi, and Jose J. Gonzalez. 2007. Incident learning systems: From safety to security. Paper read at Twenty Fifth International Conference of the System Dynamics Society, at Boston, MA, USA.

Vennix, Jac A. M. 1996. *Group Model Building: Facilitating team learning using System Dynamics*. Chichester, England: John Wiley and Sons.
Wiik, Johannes. 2007. Dynamics of incident response effectiveness – A System Dynamics Approach (Unpublished phd thesis), University of Bergen.
Wiik, Johannes, Jose J. Gonzalez, and Klaus-Peter Kossakowski. 2005. Limits to effectiveness of Computer Security Incident Response Teams (CSIRTs). Paper read at Twenty Third International Conference of the System Dynamics Society, 17-21 July 2005, at Boston, MA.
Wiik, Johannes, and Klaus-Peter Kossakowski. 2005. Dynamics of CSIRT Management. Paper read at Seventeenth Annual FIRST Conference on Computer Security Incident Handling, June 26-July 01, 2005, at Singapore.

Technical Appendix – Model Listing

```
vendor dynaplan
product smia
version 4
language enUS
def {
    submodel 'IT Department' {
        submodel 'Technical Controls' {
            var 'Desired Technical Control Quality' = 'Initial Technical Control
                Quality'*'Effect of Management Motivation on Desired Technical
                Control Quality'
            var 'Effect of Incident Handling Knowledge on Time to Perceive
                Technical Control Quality' = ('Incident Handling Knowledge'/'Incident
                Handling'.Knowledge.'Initial Incident Handling Knowledge')^log(1-
                'Incident Handling Knowledge Learning Coefficient',2 )
            var 'Effect of Management Motivation on Desired Technical Control
                Quality Lookup Table' = {[0.0, 0.5, 1.0, 1.5, 2.0]|0.25, 0.5, 1.0,1.5,
                1.75}
            var 'Effect of Management Motivation on Desired Technical Control
                Quality' = 'lookup linear'('Management Motivation'/'Initial
                Management Motivation', 'Effect of Management Motivation on
                Desired Technical Control Quality Lookup Table')
            var 'Incident Handling Knowledge Learning Coefficient' = 0.15
            var 'Increase in Tecnical Controls to Implement' = 'Perceived Technical
                Controls Quality Gap'/wk
            var 'Initial Perceived Technical Control Quality' = 0.6
            var 'Initial Technical Control Quality' = 0.6
            var 'Initial Time to Perceive Technical Control Quality' = 12 wk
            var 'Perceived Technical Control Quality' = smooth('Technical Control
                Quality', 'Time to Perceive Technical Control Quality', 1, 'Initial
                Perceived Technical Control Quality')
            var 'Perceived Technical Controls Quality Gap' = 'Desired Technical
                Control Quality'-('Perceived Technical Control Quality'+'Technical
                Controls in Pipeline')
            var 'Technical Control Deprecation' = 'Technical Control Quality'*'Rate of
                Change in Technology and Risk'
            var 'Technical Control Quality' = stock 'Initial Technical Control Quality'
                inflow 'Technical Controls Increase' outflow 'Technical Control
                Deprecation'
            var 'Technical Controls Increase' = min('Technical Controls in
                Pipeline'/'Time to Change Technical Controls', (1-'Technical Control
                Quality')/'Time to Change Technical Controls')
            var 'Technical Controls in Pipeline' = stock 0.0 inflow 'Increase in Tecnical
                Controls to Implement' outflow 'Technical Controls Increase'
            var 'Time to Change Technical Controls' = 2 wk
            var 'Time to Perceive Technical Control Quality' = 'Initial Time to
                Perceive Technical Control Quality'*'Effect of Incident Handling
                Knowledge on Time to Perceive Technical Control Quality'
        }
```

```
    submodel Policy {
        var 'Desired Policy Quality' = 'Initial Policy Quality'*'Effect of
            Management Motivation on Desired Policy Quality'
        var 'Effect of Incident Handling Knowledge on Time to Perceive Policy
            Quality' = ('Incident Handling Knowledge'/'Incident
            Handling'.Knowledge.'Initial Incident Handling Knowledge')^log(1-
            'Incident Handling Knowledge Learning Coefficient',2 )
        var 'Effect of Management Motivation on Desired Policy Quality Lookup
            Table' = {[0.0, 0.5, 1.0, 1.5, 2.0]|0.25, 0.5, 1.0,1.5, 1.75}
        var 'Effect of Management Motivation on Desired Policy Quality' =
            'lookup linear'('Management Motivation'/'Initial Management
            Motivation', 'Effect of Management Motivation on Desired Policy
            Quality Lookup Table')
        var 'Incident Handling Knowledge Learning Coefficient' = 0.15
        var 'Increase in Policy to Implement' = 'Perceived Policy Quality Gap'/wk
        var 'Initial Perceived Policy Quality' = 0.7
        var 'Initial Policy Quality' = 0.7
        var 'Initial Time to Perceive Policy Quality' = 12 wk
        var 'Perceived Policy Quality Gap' = max('Desired Policy Quality'-
            ('Perceived Policy Quality'+'Policy Quality in Pipeline'), 0.0)
        var 'Perceived Policy Quality' = smooth('Policy Quality', 'Time to Perceive
            Policy Quality', 1, 'Initial Perceived Policy Quality')
        var 'Policy Deprecation' = 'Policy Quality'*'Rate of Change in Technology
            and Risk'
        var 'Policy Quality Increase' = min('Policy Quality in Pipeline'/'Time to
            Change Policy', (1-'Policy Quality')/'Time to Change Policy')
        var 'Policy Quality in Pipeline' = stock 0.0 inflow 'Increase in Policy to
            Implement'outflow 'Policy Quality Increase'
        var 'Policy Quality' = stock 'Initial Policy Quality' inflow 'Policy Quality
            Increase' outflow 'Policy Deprecation'
        var 'Time to Change Policy' = 2 wk
        var 'Time to Perceive Policy Quality' = 'Initial Time to Perceive Policy
            Quality'*'Effect of Incident Handling Knowledge on Time to Perceive
            Policy Quality'
    }
}
submodel 'Incident Handling' {
    submodel 'Handling Capacity' {
        submodel 'Allocated Resources' {
            var 'Allocated Work Hours' = stock 'Initial Allocated Work Hours' inflow
                Allocation
            var 'Approved Work Hours' = 'Perceived Total Required Work
                Hours'*'Effect of Management Motivation on Approved Work
                Hours'
            var 'Effect of Management Motivation on Approved Work Hours' =
                'lookup linear'('Management Motivation'/'Initial Management
                Motivation', 'Management Motivation Table')
            var 'Goal for Work Hour Gap Satisfaction' = 1.0
            var 'Initial Allocated Work Hours' = 28 hrs/wk
```

```
        var 'Management Motivation Table' = {[0.0, 0.25, 0.5, 0.75, 1.0, 1.25,
            1.5, 1.75, 2.0]|0.199,0.303,0.594,0.851, 1.0,1.00,1.00,1.00,1.00}
        var 'Perceived Total Required Work Hours' = smooth('Total Required
            Work Hours', 'Time to Perceive Required Capacity')
        var 'Time Remaining after High Priority Incident Handling' =
            'Allocated Work Hours'-'Time Used for High Priority Incident
            Handling'
        var 'Time Used for High Priority Incident Handling' = min('Required
            Time to Handle High Priority Incidents'*'Time Reduction Factor
            High Priority Incidents', 'Allocated Work Hours')
        var 'Time Used for Low Priority Incident Handling' = min('Time
            Remaining after High Priority Incident Handling', 'Required Time to
            Handle Low Priority Incidents')
        var 'Time to Change Capacity' = 26 wk
        var 'Time to Perceive Required Capacity' = 26 wk
        var 'Work Hour Gap' = ('Approved Work Hours'-'Allocated Work
            Hours')*'Goal for Work Hour Gap Satisfaction'
        var Allocation = 'Work Hour Gap'/'Time to Change Capacity'
    }
    submodel 'Required Resources' {
        var 'Desired Response Time' = 1.0 wk
        var 'Initial Required Time to Handle Low Priority Incidents' = 'Incident
            Handling'.'Handling Effectiveness'.'Initial Time to Handle Low
            Priority Incidents'*'Initial Low Priority Incident Reporting Rate'
        var 'Initial Time Required to Handle High Priority Incidents' = 'Incident
            Handling'.'Handling Effectiveness'.'Initial Time to Handle High
            Priority Incidents'*'Initial High Priority Incident Reporting Rate'
        var 'Initial Total Required Work Hours' = 'Initial Required Time to
            Handle Low Priority Incidents'+'Initial Time Required to Handle
            High Priority Incidents'
        var 'Required Time to Handle High Priority Incidents' = 'Knowledge
            adjusted Time to Handle High Priority Incidents'*'High Priority
            Incident Reporting Rate'
        var 'Required Time to Handle Low Priority Incidents' = 'Knowledge
            adjusted Time to Handle Low Priority Incidents'*'Low Priority
            Incident Reporting Rate'
        var 'Total Required Work Hours' = 'Required Time to Handle Low
            Priority Incidents'+'Required Time to Handle High Priority
            Incidents'
    }
}
submodel 'Handling Effectiveness' {
    var 'Effect of Incident Handling Knowledge on Time to Handle Incidents'
        = ('Incident Handling Knowledge'/'Incident
        Handling'.Knowledge.'Initial Incident Handling Knowledge')^log(1-
        'Incident Handling Knowledge Learning Coefficient', 2)
    var 'Incident Handling Knowledge Learning Coefficient' = 0.15
    var 'Initial Time to Handle High Priority Incidents' = 4 hrs/Incidents
    var 'Initial Time to Handle Low Priority Incidents' = 1 hr/Incidents
```

```
    var 'Knowledge adjusted Time to Handle High Priority Incidents' = 'Initial
        Time to Handle High Priority Incidents'*'Effect of Incident Handling
        Knowledge on Time to Handle Incidents'*'Paperwork Time Reduction
        Factor'
    var 'Knowledge adjusted Time to Handle Low Priority Incidents' = 'Initial
        Time to Handle Low Priority Incidents'*'Effect of Incident Handling
        Knowledge on Time to Handle Incidents'*'Paperwork Time Reduction
        Factor'
    var 'Paperwork Time Reduction Factor' = 1.0
    var 'Productivity adjusted Time to Handle High Priority Incidents' =
        'Knowledge adjusted Time to Handle High Priority Incidents'*'Time
        Reduction Factor High Priority Incidents'
    var 'Productivity adjusted Time to Handle Low Priority Incidents' =
        'Knowledge adjusted Time to Handle Low Priority Incidents'*'Time
        Reduction Factor Low Priority Incidents'
}
submodel 'Reported Incidents' {
    var 'Effect of Level of Risk on Incident Reporting Rate Lookup Table' =
        {[0.0, 0.25, 0.5, 1.0, 1.5, 1.75, 2.0]|0.39,0.47,0.6, 1.0,1.41,1.54,1.6}
    var 'Effect of Level of Risk on Incident Reporting Rate' = 'lookup linear'
        ('Level of Risk'/'Initital Level of Risk', 'Effect of Level of Risk on
        Incident Reporting Rate Lookup Table')
    var 'Effect of User Knowledge on High Priority Incident Reporting Rate' =
        'lookup linear'('User Knowledge'/'Initial User Knowledge', 'Effect of
        User Knowledge on High Priority Incidents Lookup Table')
    var 'Effect of User Knowledge on High Priority Incidents Lookup Table' =
        {[0.0, 1.0,1.5, 2.0, 4.0]|0.0, 1.0, 1.4, 1.8, 2.3}
    var 'Effect of User Knowledge on Low Priority Incident Reporting Rate' =
        'lookup linear'('User Knowledge'/'Initial User Knowledge', 'User
        Knowledge Low Priority Incidents Lookup Table')
    var 'Effect of User Motivation on Incident Reporting Rate' = 'lookup
        linear'('User Motivation'/Users.Motivation.'Initial User Motivation',
        'User Motivation Lookup Table')
    var 'High Priority Incident Reporting Rate' = 'Initial High Priority Incident
        Reporting Rate'*'Effect of Level of Risk on Incident Reporting
        Rate'*'Effect of User Motivation on Incident Reporting Rate'*'Effect of
        User Knowledge on High Priority Incident Reporting Rate'
    var 'Incident Reporting Rate' = 'High Priority Incident Reporting
        Rate'+'Low Priority Incident Reporting Rate'
    var 'Initial High Priority Incident Reporting Rate' = 3.0 Incidents/wk
    var 'Initial Low Priority Incident Reporting Rate' = 15.0 Incidents/wk
    var 'Low Priority Incident Reporting Rate' = 'Initial Low Priority Incident
        Reporting Rate'*'Effect of Level of Risk on Incident Reporting
        Rate'*'Effect of User Motivation on Incident Reporting Rate'*'Effect of
        User Knowledge on Low Priority Incident Reporting Rate'
    var 'Open High Priority Incidents' = stock 'Initial Open High Priority
        Incidents' inflow'High Priority Incident Reporting Rate' outflow 'High
        Priority Incident Handling Rate' outflow 'Unhandled High Priority
        Incidents Rate'
```

```
    var 'Open Low Priority Incidents' = stock 'Initial Open Low Priority
        Incidents' inflow'Low Priority Incident Reporting Rate' outflow 'Low
        Priority Incident Handling Rate' outflow 'Unhandled Low Priority
        Incidents Rate'
    var 'Total Open Incidents' = 'Open High Priority Incidents'+'Open Out of
        Date Incidents'+'Open Low Priority Incidents'
    var 'User Knowledge Low Priority Incidents Lookup Table' = {[0.0, 0.5,
        1.0, 2.0, 4.0]|2.0, 1.5, 1.0, 0.5, 0.25}
    var 'User Motivation Lookup Table' = {[0.0, 0.5, 1.0, 1.5, 2, 2.5]|0.0,0.37,
        1.0,2.82,3.85,4.5}
    unit Person&Persons = unit
}
submodel Investigation {
    var 'Cleanup Threshold' = 30 Incidents
    var 'Fraction of High Priority Incidents Out of Date' = 1-(min('High
        Priority Incident Out of Date Limit'/'High Priority Incident Residing
        Time', 1.0))
    var 'Fraction of Low Priority Incidents Out of Date' = 1-(min('Low Priority
        Incident Out of Date Limit'/'Low Priority Incident Residing Time',
        1.0))
    var 'High Priority Incident Handling Rate' = min('Time Used for High
        Priority Incident Handling'/'Productivity adjusted Time to Handle High
        Priority Incidents', 'Open High Priority Incidents'/wk)
    var 'High Priority Incident Out of Date Limit' = 9999 wk
    var 'High Priority Incident Residing Time' = 'Open High Priority
        Incidents'/('High Priority Incident Handling Rate'+0.00001
        Incidents/wk)
    var 'Incident Handling Rate' = 'Low Priority Incident Handling
        Rate'+'High Priority Incident Handling Rate'
    var 'Initial Open High Priority Incidents' = 5 Incidents
    var 'Initial Open Low Priority Incidents' = 30 Incidents
    var 'Low Priority Incident Handling Rate' = min('Time Used for Low
        Priority Incident Handling'/'Productivity adjusted Time to Handle Low
        Priority Incidents', 'Open Low Priority Incidents'/wk)
    var 'Low Priority Incident Out of Date Limit' = 4 wk
    var 'Low Priority Incident Residing Time' = 'Open Low Priority
        Incidents'/('Low Priority Incident Handling Rate'+0.00001
        Incidents/wk)
    var 'Open Out of Date Incidents' = stock 15 Incidents inflow 'Unhandled
        Low Priority Incidents Rate' inflow 'Unhandled High Priority Incidents
        Rate' outflow 'Unhandled Incidents Closure Rate'
    var 'Perceived Open Out of Date Incidents' = smooth('Open Out of Date
        Incidents', 'Time to Perceive Out of Date Incidents', 1, 10 Incidents)
    var 'Time to Perceive Out of Date Incidents' = 2 wk
    var 'Unhandled High Priority Incidents Rate' = 'Open High Priority
        Incidents'*'Fraction of High Priority Incidents Out of Date'/wk
    var 'Unhandled Incidents Closure Rate' = if ('Perceived Open Out of Date
        Incidents'≥'Cleanup Threshold', 'Open Out of Date Incidents'/'time
        step', 0 Incidents/wk)
```

```
        var 'Unhandled Low Priority Incidents Rate' = ('Open Low Priority
            Incidents'*'Fraction of Low Priority Incidents Out of Date')/wk
    }
    submodel Knowledge {
        var 'Incident Handling Knowledge' = stock 'Initial Incident Handling
            Knowledge' inflow 'Knowledge Increase' outflow 'Knowledge
            Deprecation'
        var 'Initial Incident Handling Knowledge' = 250 Incidents
        var 'Knowledge Deprecation' = 'Incident Handling Knowledge'*'Rate of
            Change in Technology and Risk'
        var 'Knowledge Increase' = 'High Priority Incident Handling Rate'*'Time
            Reduction Factor High Priority Incidents'
    }
    submodel Quality {
        submodel 'Quality Experienced by Users' {
            var 'Initial Quality of Incident Handling Experienced by Users' =
                'Incident Handling'.'Handling Capacity'.'Allocated Resources'.'Initial
                Allocated Work Hours'/'Initial Total Required Work Hours'
            var 'Quality of Incident Handling Experienced by Users' = 'Allocated
                Work Hours'/'Total Required Work Hours'
        }
        submodel 'Quality of Investigation' {
            var 'Quality of High Priority Incident Handling Lookup Table' = {[0.0,
                0.5, 1.0, 1.5, 3.0]|1.0, 1.0, 1.0, 0.6,0.503}
            var 'Quality of Low Priority Incident Handling Lookup Table' = {[0.0,
                0.5, 1.0, 1.5, 3.0]|1.0, 1.0, 1.0,0.8, 0.7}
            var 'Time Reduction Factor High Priority Incidents' = 'lookup
                linear'('Workload Saturation', 'Quality of High Priority Incident
                Handling Lookup Table')
            var 'Time Reduction Factor Low Priority Incidents' = 'lookup
                linear'('Workload Saturation', 'Quality of Low Priority Incident
                Handling Lookup Table')
            var 'Workload Saturation' = 'Total Required Work Hours'/'Allocated
                Work Hours'
        }
    }
}
submodel Management {
    submodel 'Perceived Risk' {
        var 'Effect of Incident Handling Knowledge on Fraction of Risk
            Uncovered' = ('Incident Handling Knowledge'/'Incident
            Handling'.Knowledge.'Initial Incident Handling Knowledge')^-log(1-
            'Incident Handling Knowledge Learning Coefficient',2)
        var 'Effect of Management Motivation on Resources for Risk Assessment'
            = 'lookup linear'('Management Motivation'/'Initial Management
            Motivation', 'Management Motivation Lookup Table')
        var 'Effect of Resources for Risk Assessment on Fraction of Risk
            Uncovered' = 'lookup linear'('Resources for Risk Assessment'/'Initial
            Resources Spent on Risk Assessment', 'Risk Assessment Lookup
            Table')
```

```
    var 'Effect of Risk Assessment Knowledge on Fraction of Risk Uncovered'
        = ('Risk Assessment Knowledge'/'Initial Incident Risk Assessment
        Knowledge')^-log(1-'Risk Assessment Knowledge Learning
        Coefficient', 2)
    var 'Fraction of Risk Uncovered' = min('Initial Fraction of Risk
        Uncovered'*'Effect of Resources for Risk Assessment on Fraction of
        Risk Uncovered'*'Effect of Incident Handling Knowledge on Fraction
        of Risk Uncovered'*'Effect of Risk Assessment Knowledge on Fraction
        of Risk Uncovered', 1.0)
    var 'Incident Handling Knowledge Learning Coefficient' = 0.15
    var 'Initial Fraction of Risk Uncovered' = 0.7
    var 'Initial Incident Risk Assessment Knowledge' = 1000000 NOK
    var 'Initial Management Perception of Risk' = 0.15
    var 'Initial Resources Spent on Risk Assessment' = 3846 NOK/wk
    var 'Knowledge Deprecation' = 'Risk Assessment Knowledge'*'Rate of
        Change in Technology and Risk'
    var 'Knowledge Increase' = 'Resources for Risk Assessment'
    var 'Management Motivation Lookup Table' = {[0.0, 0.5, 1.0, 1.5, 2.0]|
        0.25, 0.5, 1.0, 1.25, 1.4}
    var 'Management Perception of Risk' = stock 'Initial Management
        Perception of Risk' inflow Change
    var 'Resources for Risk Assessment' = 'Initial Resources Spent on Risk
        Assessment'*'Effect of Management Motivation on Resources for Risk
        Assessment'
    var 'Risk Assessment Knowledge Learning Coefficient' = 0.15
    var 'Risk Assessment Knowledge' = stock 'Initial Incident Risk Assessment
        Knowledge' inflow 'Knowledge Increase' outflow 'Knowledge
        Deprecation'
    var 'Risk Assessment Lookup Table' = {[0.0, 0.5, 1.0, 1.5, 2.0, 4.0, 8.0]|
        0.0, 0.75, 1.0, 1.25, 1.4, 1.7, 2.0}
    var 'Time to Perceive Risk' = 52 wk
    var 'Uncovered Risk Gap' = ('Fraction of Risk Uncovered'*'Level of
        Risk')-'Management Perception of Risk'
    var Change = 'Uncovered Risk Gap'/'Time to Perceive Risk'
}
submodel Costs {
    var 'Cost of Developing Policy from scratch' = 3000000 NOK
    var 'Cost per Incident Handling Work Hour' = 300 NOK/hr
    var 'Effect of Technical Controls Quality on Technical Controls Costs' =
        'lookup linear'('Technical Control Quality'/'Initial Technical Control
        Quality', 'Technical Controls Quality Lookup Table')
    var 'Incident Handling Costs' = 'Cost per Incident Handling Work
        Hour'*'Allocated Work Hours'
    var 'Initial Cost of Technical Controls Operations' = 77000 NOK/wk
    var 'Initial Incident Handling Costs' = 'Incident Handling'.'Handling
        Capacity'.'Allocated Resources'.'Initial Allocated Work Hours'*'Cost
        per Incident Handling Work Hour'
    var 'Initial Policy Development Costs' = 0 NOK/wk
```

```
    var 'Initial Total Costs' = 'Initial Cost of Technical Controls
        Operations'+'Initial Incident Handling Costs'+'Initial Resources Spent
        on Risk Assessment'+'Initial Policy Development Costs'
    var 'Policy Development Costs' = 'Policy Quality Increase'*'Cost of
        Developing Policy from scratch'
    var 'Technical Controls Operations Costs' = 'Initial Cost of Technical
        Controls Operations'*'Effect of Technical Controls Quality on
        Technical Controls Costs'
    var 'Technical Controls Quality Lookup Table' = {[0.0, 0.5, 1.0, 1.5,
        2.0]|0.0, 0.5, 1.0, 1.7, 3}
    var 'Total Costs' = 'Technical Controls Operations Costs'+'Resources for
        Risk Assessment'+'Incident Handling Costs'+'Policy Development
        Costs'
    unit NOK = unit
}
submodel Motivation {
    var 'Change in Perceived Costs' = 'Gap Perceived Cost'/'Time to Perceive
        Changes in Costs'
    var 'Effect of Costs on Management Motivation Lookup Table' = {[0.0,
        1.0, 2.0, 4.0]|1.5, 1.0, 0.75, 0.25}
    var 'Effect of Costs on Management Motivation' = 'lookup
        linear'('Perceived Costs'/'Initial Total Costs', 'Effect of Costs on
        Management Motivation Lookup Table')
    var 'Effect of High Priority Incidents on Management Motivation Lookup
        Table' = {[0.0, 0.5, 1.0, 1.5, 2.0, 4.0, 10.0]| 0.25, 0.5, 1.0, 1.25, 1.4, 1.5,
        1.6}
    var 'Effect of High Priority Incidents on Management Motivation' =
        'lookup linear'('Perceived High Priority Incident Rate'/'Initial High
        Priority Incident Reporting Rate', 'Effect of High Priority Incidents on
        Management Motivation Lookup Table')
    var 'Effect of Risk on Management Motivation Lookup Table' = {[0.0, 0.5,
        1.0, 1.5, 2.0]|0.25, 0.5, 1.0, 1.25, 1.4}
    var 'Effect of Risk on Management Motivation' = 'lookup
        linear'('Management Perception of Risk'/Management.'Perceived
        Risk'.'Initial Management Perception of Risk', 'Effect of Risk on
        Management Motivation Lookup Table')
    var 'Gap Perceived Cost' = 'Total Costs'-'Perceived Costs'
    var 'Initial Management Motivation' = 0.7
    var 'Management Motivation' = min('Initial Management
        Motivation'*'Effect of High Priority Incidents on Management
        Motivation'*'Effect of Risk on Management Motivation'*'Effect of
        Costs on Management Motivation', 1.0)
    var 'Perceived Costs' = stock 'Initial Total Costs' inflow 'Change in
        Perceived Costs'
    var 'Perceived High Priority Incident Rate' = smooth('High Priority
        Incident Reporting Rate', 'Time to Perceive Change in High Priority
        Incident Rate', 1, 'Initial High Priority Incident Reporting Rate')
    var 'Time to Perceive Change in High Priority Incident Rate' = 26 wk
    var 'Time to Perceive Changes in Costs' = 4 wk
}
```

```
}
submodel Risk {
    var 'Effect of Policy Quality on Level of Risk' = 'lookup linear'('Policy
        Quality'/'Initial Policy Quality', 'Effect of Policy Quality on Risk Lookup
        Table')
    var 'Effect of Policy Quality on Risk Lookup Table' = {[0.0, 0.5, 1.0, 1.5,
        2.0]| 4, 2, 1, 0.5, 0.25}
    var 'Effect of Technical Control Quality on Level of Risk' = 'lookup
        linear'('Technical Control Quality'/'Initial Technical Control Quality',
        'Effect of Technical Control Quality on Risk Lookup Table')
    var 'Effect of Technical Control Quality on Risk Lookup Table' = {[0.0, 0.5,
        1.0, 1.5, 2.0]| 4, 2, 1, 0.5, 0.25}
    var 'Effect of User Knowledge on Level of Risk' = 'lookup linear'('User
        Knowledge'/'Initial User Knowledge', 'Effect of User Knowledge on Risk
        Lookup Table')
    var 'Effect of User Knowledge on Risk Lookup Table' = {[0.0, 0.5, 1.0, 1.5,
        2.0]| 4, 2, 1, 0.5, 0.25}
    var 'Effect of User Motivation on Level of Risk' = 'lookup linear'('User
        Motivation'/Users.Motivation.'Initial User Motivation', 'Effect of User
        Motivation on Risk Lookup Table')
    var 'Effect of User Motivation on Risk Lookup Table' = {[0.0, 0.5, 1.0, 1.5,
        2.0]| 4, 2, 1, 0.5, 0.25}
    var 'Initital Level of Risk' = 0.25
    var 'Level of Risk' = min('Initital Level of Risk'*'Effect of User Knowledge
        on Level of Risk'*'Effect of Policy Quality on Level of Risk'*'Effect of
        Technical Control Quality on Level of Risk'*'Effect of User Motivation
        on Level of Risk', 1.0)
}
submodel Users {
    submodel Knowledge {
        var 'Amount of Knowledge Increased by Training' = stock 0.0 outflow 'User
            Knowledge from Training'
        var 'Effect of User Motivation on Desired Knowledge Lookup Table' =
            {[0.0, 0.5, 1.0, 1.5, 2.0]|0.0, 0.25, 1.0, 1.25, 1.4}
        var 'Effect of User Motivation on Knowledge Desired by Users' = 'lookup
            linear'('User Motivation'/Users.Motivation.'Initial User Motivation',
            'Effect of User Motivation on Desired Knowledge Lookup Table')
        var 'Initial User Knowledge' = 0.6
        var 'Knowledge Desired by Users' = 'Initial User Knowledge'*'Effect of
            User Motivation on Knowledge Desired by Users'
        var 'Time for User to Acquire Knowledge on Own Account' = 52 wk
        var 'Time to Train User Population' = 26 wk
        var 'User Knowledge Gap' = max('Knowledge Desired by Users'-'User
            Knowledge', 0.0)
        var 'User Knowledge Increase' = min('User Knowledge Gap'/'Time for
            User to Acquire Knowledge on Own Account', (1-'User
            Knowledge')/'Time for User to Acquire Knowledge on Own Account')
        var 'User Knowledge Obsolescence' = 'User Knowledge'*'Rate of Change
            in Technology and Risk'
```

```
        var 'User Knowledge from Training' = min('Amount of Knowledge
            Increased by Training'/'Time to Train User Population', (1-'User
            Knowledge')/'Time to Train User Population')
        var 'User Knowledge' = stock 'Initial User Knowledge' inflow'User
            Knowledge Increase' inflow 'User Knowledge from Training' outflow
            'User Knowledge Obsolescence'
    }
    submodel Motivation {
        var 'Change in Delayed Effect of Feeback and Quality' = 'User Motivation
            Effect Gap'/'Time to Change User Motivation'
        var 'Combined Effect of Feedback and Quality' = 'Effect of Feedback to
            Users on User Motivation'*'Effect of Quality on User Motivation'
        var 'Delayed Effect of Feedback and Quality' = stock 'Initial Delayed
            Effect of Feedback and Quality' inflow 'Change in Delayed Effect of
            Feeback and Quality'
        var 'Effect of Feedback to Users Lookup Table Low Effect' = {[0.0, 0.5,
            1.0, 1.5, 2.0, 4.0, 10.0, 100.0]| 0.0, 0.5, 1.0, 1.3, 1.5, 1.55, 1.58, 1.6}
        var 'Effect of Feedback to Users Lookup Table' = {[0.0, 0.5, 1.0, 1.5, 2.0,
            4.0, 8.0]|0.18, 0.4, 1.0,1.23,1.37,1.73, 2.0}
        var 'Effect of Feedback to Users on User Motivation' = if ('Feedback
            Switch'=1, 'lookup linear'('Feedback to Users'/'Initial Feedback to
            Users','Effect of Feedback to Users Lookup Table'), 1)
        var 'Effect of Quality on User Motivation Lookup Table' = {[0.0, 0.5, 1.0,
            1.5, 2.0, 4.0]|0.0, 0.6, 1.0, 1.25, 1.5, 1.75}
        var 'Effect of Quality on User Motivation' = 'lookup linear'('Quality of
            Incident Handling Experienced by Users'/'Initial Quality of Incident
            Handling Experienced by Users', 'Effect of Quality on User Motivation
            Lookup Table')
        var 'Effect of User Knowledge on User Motivation Lookup Table' = {[0.0,
            0.5, 1.0, 1.5, 2.0, 4.0]| 0.25, 0.75, 1.0, 1.25, 1.5, 1.75}
        var 'Effect of User Knowledge on User Motivation' = 'lookup linear'('User
            Knowledge'/'Initial User Knowledge', 'Effect of User Knowledge on
            User Motivation Lookup Table')
        var 'Feedback Strength' = 2/ Incidents
        var 'Feedback Switch' = 1
        var 'Feedback to Users' = 'Feedback Strength'*'Incident Reporting Rate'
        var 'Initial Delayed Effect of Feedback and Quality' = 1.0
        var 'Initial Feedback Strength' = 1 / Incidents
        var 'Initial Feedback to Users' = ('Initial High Priority Incident Reporting
            Rate'+'Initial Low Priority Incident Reporting Rate')*'Initial Feedback
            Strength'
        var 'Initial User Motivation' = 0.6
        var 'Time to Change User Motivation' = 13 wk
        var 'User Motivation Effect Gap' = 'Combined Effect of Feedback and
            Quality'-'Delayed Effect of Feedback and Quality'
        var 'User Motivation' = min('Initial User Motivation'*'Delayed Effect of
            Feedback and Quality'*'Effect of User Knowledge on User Motivation',
            1.0)
    }
}
```

}