Using Dynamic Stories to Communicate Information Security[1]

Stefanie Hillen, Finn Olav Sveen, Jose J. Gonzalez,

Research Cell "Security and Quality in Organizations",
Faculty of Engineering and Science, Agder University College, Serviceboks 509
NO-4898 Grimstad, Norway

Abstract. Safety reporting systems, e.g. Air Safety Reporting Systems, are extremely efficient components of well-functioning safety schemes. An Information Security Reporting System is badly needed, but good information security data is very difficult to gather and many barriers prevent making existing data available for scientific purposes. In the scarcity of real-cases, we argue that 'Dynamic Stories', i.e. the various narratives that can be derived from system dynamics models of the existing system dynamics studies of information security might help establish a Virtual Information Security Reporting System. We do have an interesting opportunity in our running study of information security risks in the transition to eOperations in the offshore oil & gas sector. Given the importance of security for eOperations and the huge stakes involved, it seems that an umbrella organization such as the Norwegian Oil Industry Association is a potential adopter of a Virtual Information Security Reporting System. Our paper formulates issues that need to be solved in order make our vision of such reporting system a tangible prospect.

1 Introduction

"There is a certain irony with people. Collectively they are the largest single risk, but if properly supported, they can also be the strongest layer in an organization's defense." (ERNST & YOUNG 2004, 24)

It is a sad observation that most organizations do not succeed in collecting information security data; in most cases, neither the quality of the data nor its quantity is adequate enough for scientific studies. Skilled attackers act to conceal their attacks, hence complete data capture is rare. Also, organizations gather data on attacks for narrow purposes, such as for forensic purposes or to document damage. As a consequence, collected data is often not appropriate for scientific purposes. To the extent that such data exists, organizations are reluctant to share it with the research community. Sharing of information might be precluded by the rules of evidence in a criminal persecution. Very often, information security data is withheld out of concerns over publicity, reputation, etc. When data is shared, restricted use agreements or even guarantees of confidentiality are imposed. It is then very difficult, if not impossible, to carry out extensive studies in the spirit of scientific communication. Particularly, comparative studies across organizations become more or less utopian (ANDERSEN ET AL. 2004).

[1] Information Security = all aspects related to defining, achieving, and maintaining confidentiality, integrity, availability, non-repudiation, accountability, authenticity, and reliability of information or information processing facilities. We use the term 'Information Security' according to ISO- standards ISO/IEC Guide 73, ISO/IEC 13335-1, and ISO/IEC 17799:2005.

Poor availability of relevant security data means that one of the most effective frameworks for improving security, viz. a well-established Information Security Reporting System (ISRS)[2], has not yet been developed (see also GONZALEZ 2005). There should be little doubt about the need to improve reporting of information security data – intrusion attempts, successful intrusions, incidents of all kinds, Distributed Denial of Service (DDoS), etc –, followed by analysis and sharing of insights. True, the numerous computer emergency response teams (CERTs) and computer security incident response teams (CSIRTs) around the world have established Information Security Reporting Systems of sorts. But this is not enough: One could quote many papers and books lamenting that the scarcity and incompleteness of (most) security incident data are hampering progress. A particular and passionate statement (SCHNEIER 2000, 391ff.) compares the frustrating situation for information security data reporting with the success of 'Air Safety Reporting Systems'.

COOKE (2003) shows one issue that needs to be handled: People might learn from incidents or near incidents. However, some potential barriers may emerge hindering the communication about security failures, thus inhibiting the learning process.

- Reporting failures often blame someone in an organization. Hence a tendency of avoiding to report can be recognized (COOKE 2003, 96).
- The awareness of knowledge about security is often not appropriate to detect failures. (You only perceive what you already know.)
- Transparency about failures may damage the organization's reputation and thus cause loss of consumers.
- Information security incidents are seen as business as usual.

However the potential and historical risks, incidents need to be 'reported' in an appropriate and a well-prepared environment. In general this requires a management culture, or more specific an information security culture.

1.1 The argument of the paper in brief

System dynamics models are demonstrably efficient in capturing fragmented knowledge. They are robust in that they deliver sensible results from expert knowledge even when data is scarce, provided that the essential elements of the problem in question have been identified. System dynamics models do not aim at predictions – an impossible task for extremely complex dynamic problems – but at "memory of the future" in the sense of INGVAR's famous paper (1985). System dynamics models deliver fundamental insights, and

[2] The use of this term includes the ideas of incident, event and information technology. This term, on the one hand helps to distinguish better between safety and security, on the other hand it is more comprising than e. g. Incident Reporting System.

they improve mental models upon which decisions are based. System dynamics models illuminate the causal structure behind the events (e.g. attacks, failures, etc.) and trends (’reference behavior modes’).

An interesting feature of system dynamics models with rich feedback structure is their potential for generating many ’Dynamics Stories’. While case studies are typically used as departing points for modeling and analysis, a system dynamics model can be used to reverse the approach, i.e. to generate narratives based on a particular sequence of events following from feedback loops that are important for such dynamics. In the absence of a Information Security Reporting System, a family of system dynamics models in a particular domain, say security in the eOperations regime of oil and gas companies, could be a starting point to establish a *Virtual* Information Security Reporting System (VISRS).

1.2 AMBASEC and Group Model Building

The AMBASEC (A Model Based Approach to Security Culture) research project aims to advance the quality of reporting and use of ICT security data by extending and evaluating qualitative and quantitative data analysis methods in a dual setting of learning environments and audit instruments.[3] The project targets generating new knowledge of basic and applied nature about information security in the transition to eOperations in the Norwegian oil & gas fields. AMBASEC collaborates with IRMA, another RCN-funded program,[4] and with the Norwegian Oil Industry Association. The aim of eOperations is to increase production by 10%, reduce costs by 30% and extend the lifetime of mature fields in the Norwegian offshore sector through better utilization of drilling and production data, and closer collaboration between offshore and land-based personnel. Information security is critical for performance and for health & safety aspects. The crucial significance of eOperations for the energy sector[5] implies that there is an opportunity to introduce a *Virtual* Information Security Reporting System as a forerunner and sub system of an Information Security Reporting System proper.

The AMBASEC project uses Group Model Building (GMB) methodology to gather and analyze qualitative and quantitative data. Various GMB approaches exist and they differ in several respects. Some GMB-Workshops target an application of the model as a forecast simulation tool; others are using the model to derive policies, and some just *to* get insights

[3] AMBASEC grant number 164384/V30. IKTSoS is an abbreviation for the IKT Sikkerhet og Sårbarhet (ICT Security and Vulnerability) research program of the Research Council of Norway (RCN).
[4] IRMA, Incident Response and Management, grant number 164372/V30.
[5] To illustrate the potential of eOperations: A pilot case, the Brage platform, that would otherwise have been shut down in 2005 is now profitable and will be continue operating through 2010 – implying about several hundred millions US dollars in additional revenues. The total NPV of the added valued through eOperations has recently been estimated to more than 40,000 billions of US dollars (see http://www.olf.no/english/news/?32101.pdf, quoted 24 May 2006).

into messy problems (VENNIX, 1999) within ill-structured subject matters. Nevertheless there are some general issues:

- Different individuals are involved and brought together, including the target group (clients) and modelers.
- The methodology of system dynamics modeling is applied.
- An iterative process involving modelers and clients is used to sharpen the problem definition.

All in all GMB methods have been proved to support insights and changes in a positive way (ROUWETTE ET AL. 2002, 15).

1.3 The 'ping-pong' procedure

As mentioned above, the iterative 'ping-pong' process between modelers and clients is a fundamental part. We stress that this is an enabler in GMB that allows one to catch people's ideas, perceptions, experiences and mindsets about information security. People have to reflect on their own fuzzy, flawed and incomplete mental models. Forcing people to think behavior over time and tell 'Dynamic Stories' enables or enhances communication, in our case, communication about security awareness. The story-like expression of a mental model and reflection upon them by the modelers and the whole group may lead to a very first elicitation and elaboration of the problems. Furthermore, this reflection process, supported by modeling activities, leads to an evaluation of the participant's mental models via the formalized and simulated system dynamics-model.

2 'Dynamic Stories' in System Dynamics

2.1 Review

The GMB approach applied by ANDERSEN & RICHARDSON (1997) describes workshop routines as 'scripts', i.e. specific tasks or assignments for the participants. Scripts intend to keep the model building process going. One central mission of scripts is to describe problems verbally: "... that generates products such as a stakeholder analysis, a precise description of a problem to be solved … ". (ANDERSEN & RICHARDSON 1997, 108).

The terms 'verbal story', 'dynamic story', or 'feedback story' are used in several scripts of ANDERSEN & RICHARDSON (1997). One script is called 'eliciting feedback structure'; the authors described it as follows: "The last and most difficult task in conceptualizing model structure is getting the client team to think in detail about causal linkages that form the key feedback loops controlling the system. We have experimented with a number of tasks to assign to subgroups and plenary groups to accomplish this task, such as having a group tell *verbal stories* about what controls key levels or rates, while the facilitator tries to translate these verbal protocols into causal loops of some sort." (ANDERSEN & RICHARDSON 1997, 120).

Dynamic Stories are also used in a script called 'capacity utilization' (ANDERSEN & RICHARDSON 1997, 121). "The group focuses on two key levels and is asked to describe what will happen when these two key levels get far out of alignment. This simple question naturally elicits feed back stories from the client group."

Another script of ANDERSEN & RICHARDSON is called 'reference mode elicitation'. "First, the task is designed to elicit as many dynamic behaviors and stories about those behaviors as possible." (ANDERSEN & RICHARDSON, Unpublished paper, 24).

In STERMAN'S book 'Business Dynamics' (2000) the author explains some of the Causal Loop Diagrams with narratives. For instance, he explicates the fundamental modes of dynamic behavior, such as the effect of exponential growth due to compound interest (STERMAN 2000, 108). On the one hand, his explanations do have the generic form of stories (STERMAN 2000, 108), on the other hand, most of these stories concern real phenomena, e.g. the exponential growth of the world's population (STERMAN 2000, 110).

A similar approach is used by SENGE (1990). A prominent Dynamic Story is the 'beer game' (ibid, 25ff.) A Causal Loop Diagram which reveals the core of the dilemma accompanies the story (SENGE 1990, 50). To explain archetypes, for instance 'shifting the burden', SENGE (1990, 104ff.) describes taking drinks to mitigate stress (SENGE 1990, 109).

In his 2004 paper named "Using generic systems archetypes to support thinking and modelling" WOLSTENHOLME uses Causal Loop Diagrams to present a core set of four system archetypes. For example, he associates the 'out of control' problem archetype with early hospital discharges (2004, 349) – he explains it by using a concrete health care issue – by using a 'Dynamic Story'.

In addition to ANDERSEN & RICHARDSON, STERMAN, SENGE and WOLSTENHOLME, many other authors have also used Dynamic Stories implicitly.

2.2 The tacit use of Dynamic Stories

The theory or the concept of a Dynamic Story is not precisely defined in the references mentioned above. An internet search shows that there are countless definitions of and ideas about Dynamic Stories. The findings span from lectures about International Trade Theory and Policy,[6] computer simulations,[7] writing techniques, to internet games, etc. We choose to focus on system dynamics approaches and take the specific and well-known references in this research field into account. One conclusion we can draw is that Dynamic Stories are not well defined or described as a separate key factor but they are more or less informally used to support insight and comprehension.

[6] http://internationalecon.com/v1.0/ch90/90c010.html
[7] http://www.forio.com/article_story.htm

The frequently used method of verbally describing archetypes or system dynamics models leads us to the following insight: Dynamic Stories are utilized more or less tacitly, but in a way that highlights structure and insight. We propose that the impact of using Dynamic Stories to transfer information security knowledge is potentially powerful.

2.3 AMBASEC's definition of Dynamic Stories

Dynamic Stories are narratives. They describe how a feedback structure gives rise to a particular behavior over time. A Dynamic Story is often connected to a single case, but it does not have to. A Dynamic Story can also describe a generic process; this allows the author to describe a real as well as a fictive or assumed situation in the future. Generically, Dynamic Stories use the language of the participants, encompassing behavior over time aspects and referring strongly to the problems of concern.

'Case studies' and 'Dynamic Stories' are closely related. The key difference is that the latter are 'memories of the future' (INGVAR 1985). That means that the GMB participants do 'cognitive simulations' during the Workshop. They exchange and evaluate ideas about potential future events. Additionally, some aspects of these stories are elicited and highlighted through discussion during the GMB-Workshop. Nevertheless, these assumptions are based on individual and collaborative working experience and expertise of the present and the past. At least their reliability, in particular their behavior over time is evaluated by the formalized simulation of the system dynamics-model.

3 Dynamic Stories to disseminate information security aspects

3.1 Needs

People directly involved in the GMB activities do learn a lot (ROUWETTE ET AL. 2002) about information security. Collectively they have an opportunity to construct and exchange ideas about potential risks and failures, future settings and the like, through the provided GMB communication 'platform'. A fruitful learning effect occurs during the process. One result is the construction of a system dynamics-model.

To serve the needs of most people involved in such complex security problems one must also reach the 'external' audience, i.e. those not participating in the GMB process but who still need the insights. However, system dynamics models are often large and complex. One method that has been used by several authors is the utilization of system archetypes. This 'reduction' leads to a model size which is manageable for the human mind.

Nevertheless two problems still remain:

- People are unfamiliar with or are not able to read causal loop diagrams or archetypes
- The process of thoughts can not be represented well in a model

Embodying the essential insights of a GMB-workshop into 'Dynamic Stories' enables a transfer of information security issues to a broader audience. The development of an information security culture can be seen as a part of organizational learning.
Dynamic Stories have the potential to create 'memories of the future' and, thus, to unveil not yet detected problematic issues. This helps overcome the 'repairing issues' in information security (i.e. from a reactive to a proactive approach).

3.3 Requirements

From a technical point of view the system dynamics model serves as a generator for Dynamics Stories. Multiple scenarios are computable by parameter variation of a system dynamics model, or by just using sub-models, etc. Each of these scenarios can be employed to constitute a Dynamic Story. Dynamic Stories must on the one hand be very concrete and strongly related to the security approach. People must have the chance to take part in these stories. On the other hand, the stories have to be as generic as possible, so to be transferable to potential similar events in the future. Issues for the design of such stories can be derived from the discipline of complex problem solving in particular the principles for complex learning environments (SAVERY & DUFFY 1995; HILLEN 2004).

3.4 A double challenge with the concept of 'Dynamic Story'

The term 'Dynamic Story' is still informal. A good approach must be developed to conceptualize this issue. 'Dynamic Stories' would have to be generated from system dynamics models. On the one hand a template for their design has to be developed. To disseminate the encapsulated expert knowledge within the SD model the integration of Dynamic Stories in a useful learning environment is needed. On the other hand the Dynamic Stories will serve as backbone for a virtual reporting system – a "Virtual Information Security Reporting System." It must be secured that 'Dynamic Stories' are continuously elaborated and that new ones are following. One underlying research aim for both functionalities of Dynamic Stories is to accomplish the improvement of information security.

3.4.1 Dynamic Stories and Reporting Systems

3.4.1.1 Structures and procedures within Reporting Systems

DE KEYSER ET AL. (2004) propose a series of steps that must be fulfilled in order to establish any reporting system: The development of the reporting interface, data collection, data analysis, recommendations, implementation and its evaluation. The organization of these steps is shown in the following figure 1.

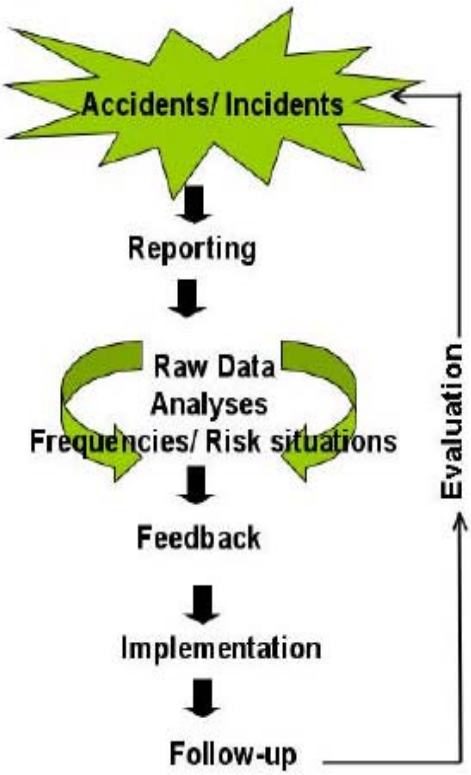

Figure 1: Developing a reporting system (DE KEYSER ET AL. 2004,13)

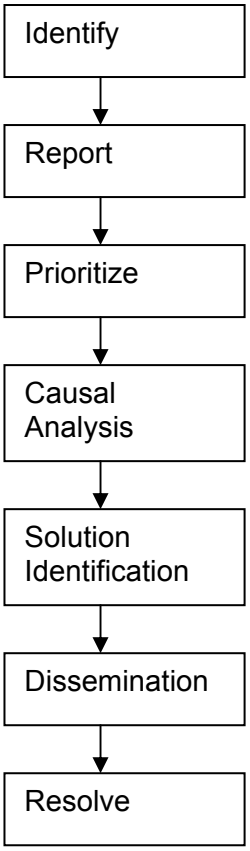

Figure 2: Incident processing stages (PHIMISTER ET AL. 2003, 448)

PHIMISTER ET AL. (2003, 448) describe a procedural structure within Reporting Systems (see figure 2). This stages are derived empirically by a research study based on representative data of enterprises[8] using reporting systems[9].

According to PHIMISTER ET AL. (2003) and NYSSEN ET AL. (2004) this staged approach can be described as follows:

- **Identification**: an incident is recognized to have occured.
- **Reporting:** someone reports the incident.
- **Priorization:** the incident is appraised and the information pertaining to the incident is transferred to those who will assess the follow-up actions.
- **Causal analysis**: Based on the incident, the causal factors that could have enabled the incident has to be identified.

[8] Fortune 500 companies.
[9] All of these companies have been using 'near miss-management reporting systems. Instead of reporting accidents, near-incidents have been taken into account.

- **Solution identification**: a solution to mitigate or avoid the consequences of the incident are identified and corrective actions are determined
- **Dissemination:** the proposed and determined actions are disseminated to the involved or affected people. Additionaly for learning purposes[10] and maintenance or the enhancement of situational awareness it is brodcasted to a wider audience.
- **Resolution**: Corrective actions are sustainably implemented and evaluated. More over necessary follow-up activities are accomplished.

We suggest to take PHIMISTER ET AL. (OP. CIT.) as a generic approach for structuring a reporting system. In our case to develop an Information Security Reporting System.

3.4.1.2 Proposal for the structure of a *Virtual* Information Security Reporting System

As already pointed out above, there are several stages within an ISRS. The very first activity is to recognize and identify an incident. But this early step represents a huge obstacle. The scarcity of good information security data has been discussed before. This leads to our proposal of using 'virtual incidents or virtual data'. This virtual data can be obtained through group model building activities or from a system dynamic model itself. By analyzing the system dynamics model Dynamic Stories can be derived and used as virtual data. In our approach of *Virtual* Information Security Reporting Systems, Dynamic Stories represent placeholders for real incidents. Hence some stages and procedures within an ISRS can be replaced and executed. For instance the simulation of a given system dynamics model, its analysis, e.g. through a sensitivity analysis or by detecting archetypes, replaces the procedure 'causal analysis'.

3.4.2 Telling Dynamic Stories for needs of organizational learning

The application of a 'tool' is needed to disseminate expert knowledge about information security that is enclosed in SD-models. The 'tool' we use is 'Dynamic Stories'.
As mentioned before the content of a Dynamic Story is encapsulated within the SD-model.
The dynamic story told here as an example (see figure 3) is already 'compressed' by using a problem archetype:

Investment in detection capacity improves detection of potential insider activities. As more such signals are detected, risk perception increases, leading to more investment in detection capacity. On the other hand, more detected signals will lead to less managerial trust of the employees, which in turn leads to even more investment in detection capacity. The combined effect of the two reinforcing feedback loops could be overinvestment in detection

[10] Learning from incidents (see COOKE 2003).

capacity and internal trust problems. However, the more serious problem would be if the reinforcing loops operate in the opposite sense – the trust trap: low investment in detection, low detection of intrusions and high, reckless managerial trust of the employees. Again, delays and system boundaries make it difficult to see that the low level of detected incidents might be caused by low capacity to detect them.

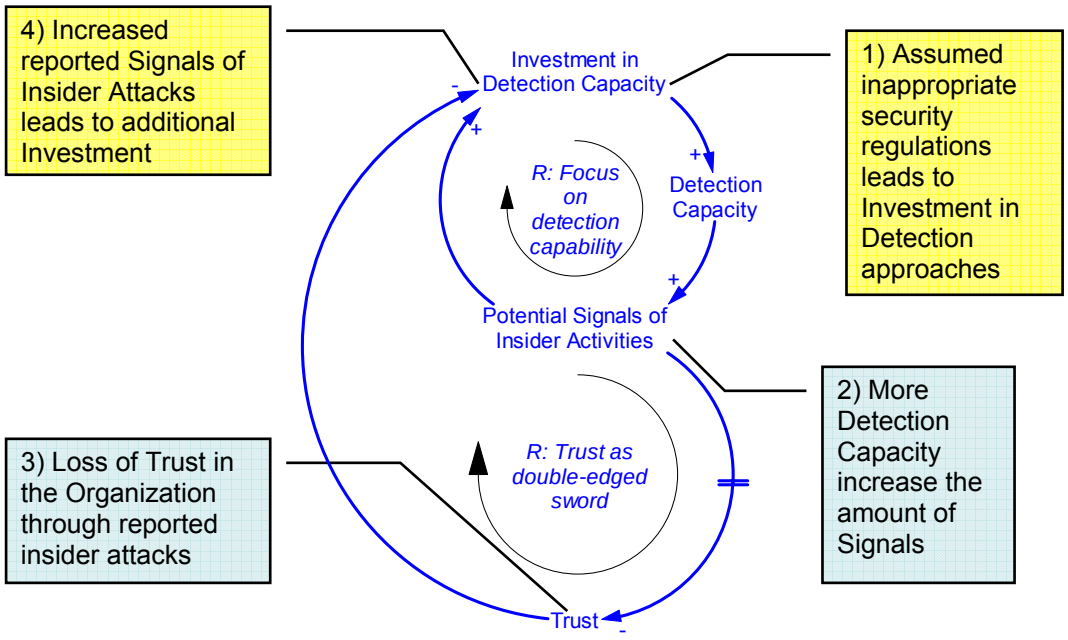

Figure 3: First steps to deduce a Dynamic Story

The 'solution archetype,' which is not shown here, would add routine security audits to assess the real situation and determine the desired detection capacity. Investment decisions should be made according to the gap of desired detection capacity and the actual detection capacity. Typically, security audits correct the picture provided by intrusion detection systems (elimination of false positives and of low-priority attacks from further consideration); alternatively, security audits would tell if intrusion detection capacity is insufficient. In both cases, the resulting action would be a correction of investment in detection capacity.

Even the 'pure' content of the Dynamic Story can be deduced from the model (see above) an instructional design structure is still missing. It has to be developed to evoke meaningful learning. Using Dynamic Stories for learning one rudimentary suggestion is to distinguish between three different types.

Dynamic Story Type 1 (Situation):

This type of Dynamic Story only describes the 'situation'. Facts, behavior and specific data are revealed. Hereby the learner is 'situated' (situated cognition theory[11]; RESNIK 1991) within the story as a responsible (decision maker), but without any specific task.

[11] Situated cognition as a theoretical construct emphasizes that learning should take place in realistic settings and under the guidance of experts.

Dynamic Story Type 2 (one proposed problem):

Unlike Type 1 of a Dynamic Story, Type 2 describes the problem in detail. This has an affinity to 'problem archetypes' in the sense of WOLSTENHOLME (2004). For instance figure 3 depicts a problem archetype (see above).

Dynamic Story Type 3 (one proposed solution):

Dynamic Story Type 3 explains one proposed solution for this problem. This has also an affiliation to WOLSTENHOLME'S classification of a solution archetype (2004).

This arrangement is done for several reasons. In the field of information security 'situational awareness' plays an important role. If people do not perceive that things are going wrong, they aren't able to react in time and appropriately. Perhaps they ultimately do realize the problem, but the system may already have crashed. Enhancing situational awareness is one step in the right direction for the improvement of information security. The ability to perceive potential problems provides time and space for appropriate incident management actions.
To describe this phenomenon in a nutshell: you do not see what you do not know. This is well known in cognitive psychology as selective attention or perception processes.
To detect the problem (DS Type 2) means to discover additional side effects or not intended effects beside the perceived system boundary (WOLSTENHOLM 2004; STERMAN 2000; DOERNER 1996).
There is seldom just one 'solution' for a complex problem (GOMEZ & PROBST 1987). So we do offer one possible solution (DS Type 3) to the described problem (DS Type 2). This does not exclude that the targeted learner may find better or alternative solutions.

3.5 Challenges and further perspectives

The AMBASEC project cooperates with the Norwegian Oil Industry Association and this might provide an opportunity to start building and evaluating a *Virtual* Information Security Reporting System. Still, the idea of such *V*ISRS must find acceptance, interest, and demand in the oil & gas industry. While we do expect a receptive audience, experience has told us that our partners are critical and not easy to convince, unless practical results are readily available.
Looking ahead, if the oil & gas industry makes positive experiences with a *Virtual* Information Security Reporting System − in particular has been taken advantages of such reporting system then a 'real' Information Security Reporting System may become a realistic perspective in not too distant a future.

References

ANDERSEN, D.F. ET AL. (2004). Preliminary System Dynamics Maps of the Insider Cyber-threat Problem. In The 22nd International Conference of the System Dynamics Society July 20-24. Oxford, UK.

ANDERSEN, D. F. & RICHARDSON, G.P. (1997). Scripts for group model building. System Dynamics Review. Vol. 13, No 2, 107-129.

ANDERSEN, D. F. & RICHARDSON, G. P. (UNPUBLISHED PAPER). Group Modeling of IT-Based Innovations in the Public Sector.

COOKE, D. L. (2003). Learning from incidents (75-108) in, Jose J. Gonzalez (Ed.), From modeling to managing security. Vol. 35, Research Series. Kristiansand, Norway. Norwegian Academic Press.

DE KEYSER, V. ; NYSSEN, A.S.; LAMY, M.; FAGNART, J.L.; BAELE, P. (2004). Development of a critical incidents reporting system in medicine. Published by the Belgian Science Policy. D/2004/1191/8.

DÖRNER, D. (1996). The logic of failure: Strategic thinking to complex situations. New York: Henry Holt and Company.

ERNST & YOUNG (2004). The annual global information security survey.

GOMEZ, P. & PROBST, G.J.B. (1987). Vernetztes Denken im Management: Eine Methodik des ganzheitlichen Problemlösens (Die Orientierung 89). Bern: Schweizerische Volksbank.

GONZALEZ, J. J. (2005).Towards a Cyber Security Reporting System -- A Quality Improvement Process, in Computer Safety, Reliability, and Security (Lecture Notes in Computer *Science 3688)*, B.A.G. Rune Winther, Gustav Dahll, Editor. Springer. Heidelberg.

HILLEN, S. (2004). Systemdynamische Modellbildung und Simulation im kaufmännischen Unterricht. Elizitation und Elaboration von Mentalen Modellen in komplexen betriebswirtschaftlichen Gegenstandsbereichen. Dissertation. Konzepte des Lehrens und Lernens. Vol.10. Frankfurt/Main. Peter Lang.

INGVAR, D.H. (1985). Memory of the future: An essay on the temporal organization of conscious awareness. Human Neurobiology. Vol. 4,127-136.

NYSSEN, A. S.; AUNAC, S.; FAYMONVILLE, M. E.; LUTCE, I. (2004). Reporting systems in healthcare from a case-by-case experience to a general framework: an example in anaesthesia, European Journal of Anaesthesiology. No 21, 757-765.

RESNIK 1991, L.B. (1991). Shared cognition: Thinking as social practice. In: L.B. Resnik, J.M. Levione & S.D. Teasley (Eds.), Perspectives on socially shared cognition (pp.1-10).Washington DC: American Psychological Association.

ROUWETTE, J. ET AL. (2002). Group model building effectiveness: A review of assessment studies. System Dynamics Review. Vol. 18, No 1, 5-45.

SAVERY, J.R. & DUFFY, T.M. (1995). Problem based learning: An instructional model and its constructivist framework. Educational Technology, No. 35, 31-38.

SCHNEIER, B. (2000). SECRETS AND LIES: DIGITAL SECURITY IN A NETWORKED WORLD. NEW YORK. John Wiley & Sons, Inc.

SENGE, P.M. (1990). The Fifth Discipline. London. Random House.

STERMAN, J.D. (2000). Business Dynamics. Boston. Mac Graw-Hill.

VENNIX, J.A.M.(1999). Group model building: Tackling messy problems. System Dynamics Review. Vol. 15, No 4, 379-401.

WOLSTENHOLME, E.F. (2004). Using generic systems archetypes to support thinking and modelling. System Dynamics Review. Vol. 20, No 4, 341-356.