

Adapting Group Model Building Methods to Improve Information Security Data

Ying Qian

Jose J. Gonzalez

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

ying.qian@hia.no

jose.j.gonzalez@hia.no

Abstract

Cyber security data restrictions, e.g. due to fear of bad publicity, hinder systematic investigation of information security issues. We argue that group model building is a promising method to help mitigate such restrictions: 1) Models emerge from even incomplete and inaccurate data; 2) group model building helps develop a trustful relationship between data owners and modelers; 3) the iterative nature of group model building leads to gradually structurally richer and more useful models, thus boosting further client interest and trust. We describe our experiences using a case for the transition to eOperations in the oil and gas industry. We analyze the outcome of two group model building workshops, the follow-up meetings and interview. We show the trajectory for how we gain access to data, how we developed and improve a model, what insights the client learned, and more important, how we built up trust with the client during this process.

Keywords: Cyber data restriction, information security risk, Integrated Operations, system dynamics, group model building, trust

1. Introduction

Good data is important for systematic investigation of a problem. However, cyber data restrictions are the rule in the field of information security: first, good data may not exist; second, existing data may not be accessible; and third, the accessed data may not have a quality good enough to use (Andersen et al. 2004).

Information assets defenders are generally not motivated to collect large-scale data. Most of them are often over-burdened with reactive work (Gonzalez 2005), which drives them away from proactive work, such as data collection and analysis (Killcrece et al. 2003).

To the extent that organizations collect cyber data, we can not assume that they will make it accessible to scientists. Data on incidents may be withheld due to concerns about publicity, reputation, or worries about copycat activities. When detailed data are shared, they often become available only under restricted-use agreements or guarantees of confidentiality: Barriers exist between researchers and domain experts (

Figure 1). Trust is a key issue: Can organizations trust that scientists treat confidential data confidentially? Might the models and the scientific papers disclose embarrassing facts? To generate trust, sensitive data must not only be kept confidential and be used under the restricted-use agreements, but also scientific work must generate useful insights for the organizations.

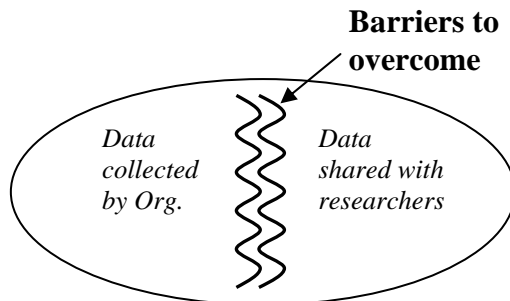


Figure 1 Data restriction between researchers and organizations

To help overcome these barriers, the Security and Quality in Organization (SQO) research cell in Agder University College initiated a research project 'AMBASEC' (A Model-Based Approach to Security Culture). Hydro, a leading Norwegian Oil and Gas Company, kindly provided a case—the offshore platform Brage. We hope that this case study could develop into a template for introducing SD as tool in the information security field in general. In this paper, we focus the discussion on how we use system dynamics model-based interventions to establish trust between data owners and scientists to gain access to more data.

2. Case Description

The Norwegian Oil and Gas Industry are transitioning from traditional operations to Integrated Operations (formerly called eOperations). The transition requires new technology, new work processes, new knowledge and organizational changes. The transition is planned to occur in two stages, starting in 2003 and being completed in 2015. The first stage, planned for 2003 to 2010, comprehends the integration of on-and offshore operations (Generation 1). Stage two, from 2007 to 2015, is planned to include the integration of companies (Generation 2).

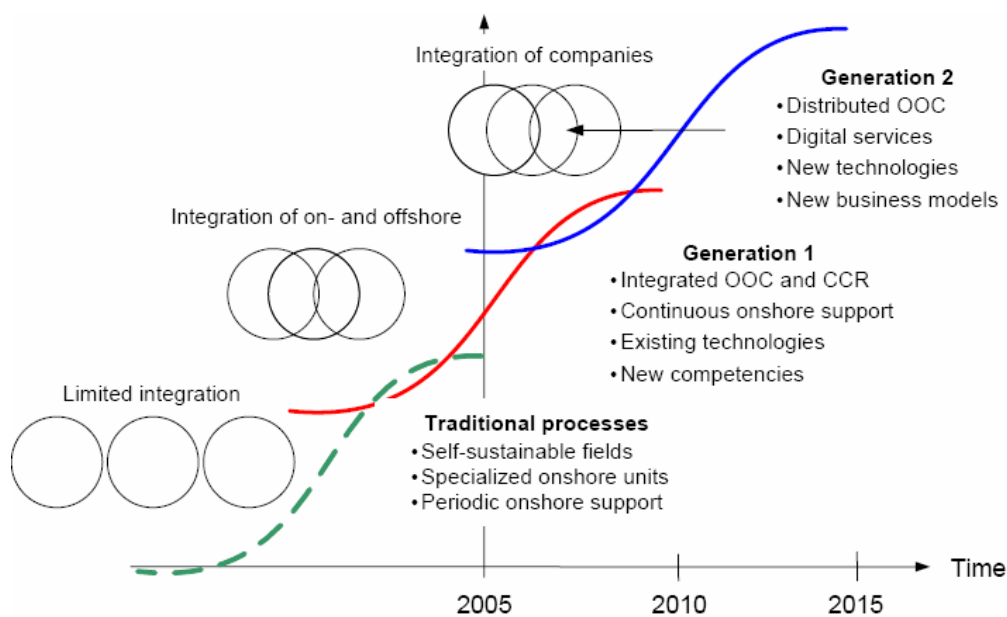
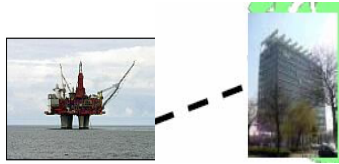
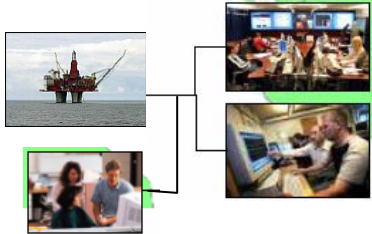


Figure 2 Transition to Integrated Operations¹

In traditional operations, each offshore platform is a self-contained field, where daily operational decisions are made with limited onshore support. The offshore field is essentially a closed system. In Integrated Operations, personnel onshore monitor offshore operations in real-time and make production decisions collaboratively with the offshore team. In generation 2 of Integrated Operations vendors and external experts will be able to deliver their services digitally over the net. (Table 2)

Table 1 Traditional operations vs. Integrated Operations

Traditional operations	Integrated Operations
<ul style="list-style-type: none"> • Daily operational decisions are made offshore with limited onshore support. • Plans are made and changed fragmentally and at fixed times. • IT solutions are specialized and silo-focused. 	<ul style="list-style-type: none"> • Decisions are made collaboratively by operators on/offshore and vendors' expert centers. • Several work processes and decisions are automated. • Vendors deliver services digitally, i.e., over "the net".
	

With better utilization of drilling and production data, and closer collaboration between offshore and onshore personnel and experts, Integrated Operations is expected to lead to

¹ The Figure 2 is taken from a presentation about integrated work processes, presented at the meeting on Integrated Operations in the Oil and Gas Industry in Stavanger, June 2nd, 2005. The presentation can be viewed at <http://www.olf.no/io/?26566>

10% production increase and 30% cost reduction.² Nevertheless, the newly-adopted technology, work processes, etc, introduce new vulnerabilities to the system. Information security issues emerge not only from technology issues but also from human and organizational factors. First, unfamiliarity with new work processes, knowledge and technologies may lead to an increasing amount of unintended human errors. Second, employees' perception of "safe and secure" remains anchored in traditional operations. They are not aware of higher information security risks in Integrated Operations. The perception of "safe and secure" will change only after long delays and after a significant number of incidents have occurred. Third, the competence to use new technology takes long time to build up. It lags behind the introduction of new technology. Therefore, as the operation transition takes place, the know-how gap might be widened, generating higher information security risks as well.

The Brage platform serves as a pilot project in the transition to Integrated Operations. Brage started production in 1993. With 13 years of production, Brage is a so-called mature platform and it has reached its tail-stage. The platform was originally planned to shut down in year 2005. Moving to Integrated Operations helps it to achieve higher revenue, reduce costs and remain profitable. If Integrated Operations is successful, it is estimated that Brage will be operated through 2010, implying additional revenues of several hundred millions of US dollars.

3. Methods

In this project, System Dynamics group model building methods and other SD model-based communications are used to tackle the cyber data restriction problem, because SD matches our requirement to generate insights even from incomplete and imprecise data and SD models may serve as interactive communication platform, i.e. to elicit supplementary information from clients. The System Dynamics model plays multiple roles in the research: 1) The formal model addresses the client's problem, helping to discover high leverage policies; 2) The model-based interventions help to convey model insights to client; and 3) The model-based intervention stimulate discussions to elicit information (data) from client. With more and better data, we can further improve the model. Thus, knowledge is transferred bilaterally, 1) from modelers to clients (i.e. model-based insights in security) and 2) from clients to modelers (improved data and causal structures). Such process enhances learning, fosters consensus and creates commitment. Hopefully, trust can be built up between the researchers and client during this process, trust being a requisite for sustainable improvement of security data reporting.

The AMBASEC project spans over a three-year time period from March 2005 to March 2008. So far, two group model building workshops, several teleconferences and one interview have been arranged with the client. (For references on group model building, see Andersen and Richardson 1997; Andersen, Richardson, and Vennix 1997; Vennix 1996; Vennix 1999; Luna-Reyes and Andersen 2003; Richardson and Andersen 1995; Richardson, Andersen, and Luna-Reyes 2005). Our paper describes the evolution of data and models during the first year of the AMBASEC project.

² The NPV of the increased value facilitated by eOperations has been estimated to more than 40,000 billions of US dollars. See <http://www.olf.no/english/news/?32101.pdf>, quoted 24 May 2006.

4. Analysis: Data, Model and Others

In section §4.1 we present a table summarizing the evolution of data, model, insights, and client attitude during the four initial stages. Then, in sections §4.2-4.5 we provide detailed information about these items and discuss their implications.

4.1 Overview of the stages of the research project

Table 2 summarizes the four initial stages of our project.

Table 2 Overview of the change of data, insights and client attitude

(GMB: Group model building; WS: Workshop)

Stage	GMB WS 1	Between GMB WS 1 and WS 2	GMB WS 2	Post WS 2 Meetings & interviews
	<i>(See 4.2 p 6)</i>	<i>(See 4.3 p 8)</i>	<i>(See 4.4 p 9)</i>	<i>(See 4.5 p 12)</i>
Purpose	Problem identification & SD concept model	Problem articulation	Develop a prototype simulation model	Advance the model structure & calibrate the model
Data	<ul style="list-style-type: none"> - Stakeholder map - Policy lever map - Key indicators and their behavior over time - Dynamic stories (with stakeholders, policies and key indicators) 	Qualitative and quantitative information about transition to Integrated Operations	<ul style="list-style-type: none"> - Overview of the transition to Integrated Operations - Information about one concrete work process flow - Risk Matrix - Work process development timeframe 	<ul style="list-style-type: none"> - Qualitative and quantitative data - Information about incidents response activities
Model	<ul style="list-style-type: none"> - Open loop model - Some feedback loops 	- System Archetypes	- Prototype model (four submodels)	Extended model (seven submodels)
Insights	<ul style="list-style-type: none"> - Basic problem: transition to Integrated Operations generates security risks. - Inadequate knowledge in relation to work processes causes system vulnerability. 	Understand motivation, steps and effect of transition to Integrated Operations	<ul style="list-style-type: none"> - New technologies enable new work processes but also introduce new vulnerabilities - Maturing technologies, work processes and knowledge reduce vulnerabilities - Incident response and knowledge management speed maturation 	<ul style="list-style-type: none"> - During the operation transition, different types of risk behave differently because they have their own accelerators and mitigators. - Maturation of knowledge, technology, work processes, learning from incidents, and improving security culture can help reduce the information security risk, while slowing down the transition can also reduce the risk.
Client attitude	From skeptical to supportive		Positive remarks about the GMB WS Committed to act as model reference group	This is a good approach. It is practical and related to the problem in reality.

4.2 Group Model Building Workshop 1

Time: May 25-26 2005

Participants: AMBASEC (6 persons: three served as “client,” the other three served as modeler and process observers)
IRMA³ (3 persons: all of them were client)
Hydro (1 person: The CEO of the Integrated Operations project)
Albany (3 persons: facilitation team)

The client group included information security specialists from the AMBASEC team and the IRMA team, and domain experts from Hydro.

Only one person from Hydro (the CEO of the Integrated Operations project) attended the first group model building workshop. At that stage there was a misperception at Hydro about the purpose of the group model building workshop and Hydro was still reluctant to participate in full.

Purpose: To identify problem and form some SD concept maps.

Many companies, especially those in hazardous industry, are concerned about the information security risks they will face in the future. There are many potential issues: Is the technology sufficiently mature? What about human factors and know-how? Is the security culture adequate? Hydro one such concerned company. And with the transition to Integrated Operations, the concern about information security risks is on a rise. However, it is difficult to clearly spell out what the problem is.

Data obtained:

✓ ***Stakeholder map***

We identified more than 40 stakeholders and clustered them according to their influence and interest in the problem. Forming this map, we created a shared view of stakeholders and their concerns and perspectives to the problem. The high influence/high interest stakeholders are candidates for model reference team. Some of them were present, such as ‘Crisis management team’ (represented by IRMA), while some others were not present, such as ‘Platform chief’, ‘Control room manager’, and ‘Chief information security officer’.

✓ ***Policy lever map***

The client group came up with more than 30 policy statements. For each policy lever, there is an implied problem. For example, one policy lever is ‘continuous training’, implying that there might be a problem with know-how. The policy ‘create formal CSIRTs (computer security incident response teams)’ shows concern

³ IRMA (Incidents Response Management) is another research project sponsored by Research Council of Norway. The research team is from SINTEF, one of the largest research institutes in Norway. IRMA has close collaboration with Hydro on its incidents response management. Therefore, they served as client in the GMB workshop.

about incident handling capacity. There are policies around incident reporting and information sharing, which imply inadequate learning from incidents.

✓ ***Key variables and their behavior over time***

The client group identified more than 30 key variables and their behavior over time. These variables could be grouped into several categories: some describe the transition to Integrated Operations; some are about external threats; some describe the knowledge gap; etc.

In some cases, different participants came up with the same variable but with different behavior over time. It implies that 1) this variable could be an important variable in the model, and 2) different mental models about this variable exist. Identifying the disagreements, presenting different views from different stakeholders and reaching consensus through discussion is a learning process embedded in a group model building process.

✓ ***Dynamic stories***

In this exercise, the participants were divided in two groups and each of them was invited to choose some stakeholders, some policies, and some key variables and link them into a dynamic story. One result was a dynamic story about 'Virus exposure in a virtual organization' and the other one was 'Suppliers as Trojan Horses'. Though the two stories have different focus, both of them addressed a common key problem, i.e. the operation transition generates a knowledge gap and the knowledge gap drives vulnerability up. A common understanding of the problem emerged.

Insights:

The group discussion leads to several dynamic hypotheses. Two examples follow:

- The transition from traditional to Integrated Operations creates vulnerabilities. The timing and frequency of these vulnerabilities may depend on how well the organization is able to change its operating processes, train its staff and contractors, and gain acceptance for the transition among the staff.
- Development of a capacity to detect and learn from security problems may facilitate the transitions process. Conversely, a limited capacity to detect security problems will obstruct change and delay corrections, increase risk, and put the project at greater peril.

Maps and models:

An open loop model was developed describing the operation transition as capacity in traditional operation moves into capacity in Integrated Operations. Work processes and knowledge change accordingly. But it takes time for work processes and even longer time for knowledge to mature. Therefore, the operation transition creates work processes and knowledge gaps, which generate vulnerabilities.

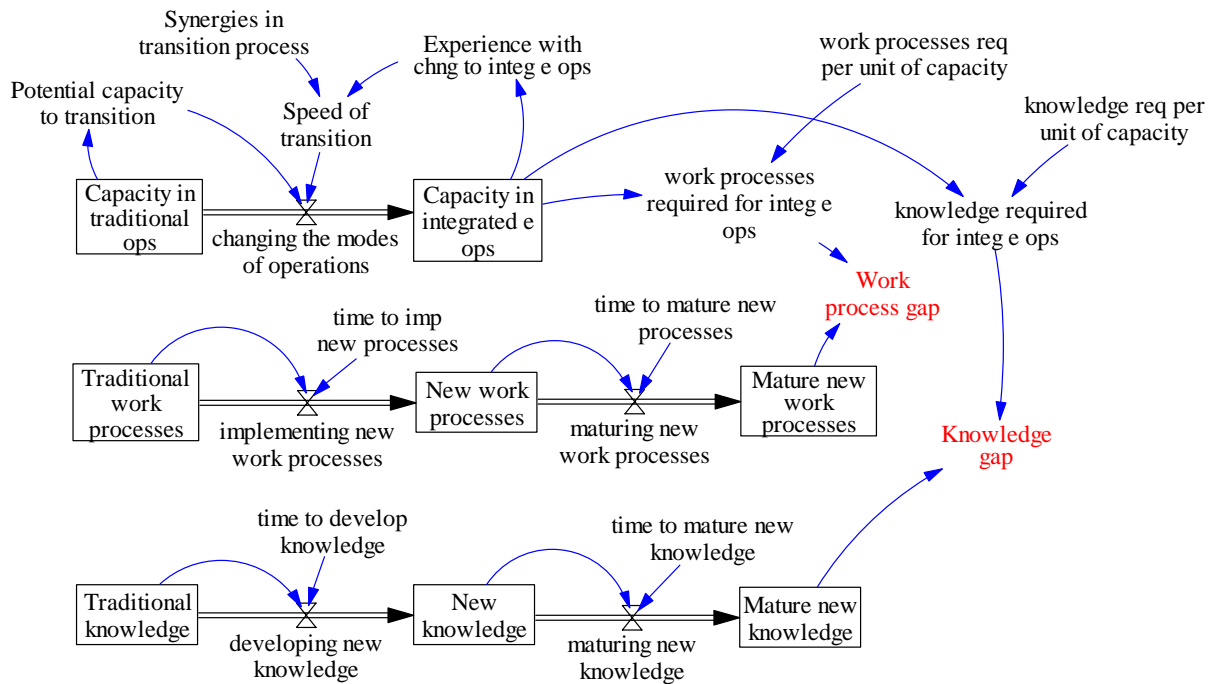


Figure 3 Open loop model derived from the GMB Workshop 1

Client attitude:

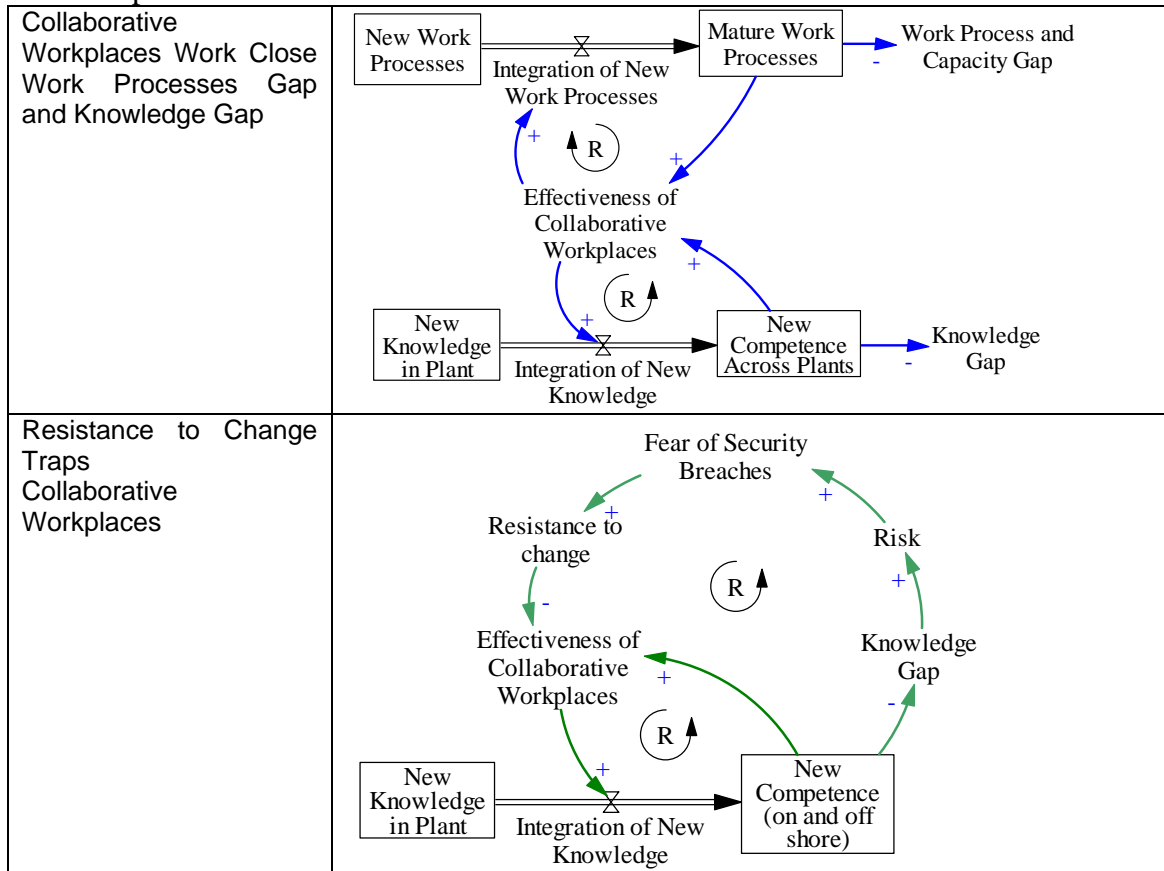
As mentioned in sector 4.2 participants (P. 6), the client was originally skeptical about the SD group model building method and only the CEO of the project joined the first workshop. After the workshop, he expressed an impression that SD group model building was a useful tool to address the information security problem in the transition to Integrated Operations. He promised to assign more people to join the second GMB workshop. (For detailed information on this workshop, please refer to Rich, Andersen, and Richardson 2005)

4.3 After the Group Model Building Workshop 1

In the interval between the first and second group model building workshop, we analyzed the data we collected in workshop 1. We articulated the problem and some sub-problems using system archetypes (Gonzalez et al. 2005; Qian, Gonzalez, and Sveen 2005). Additionally, we gathered some qualitative data and quantitative data about the transition to integrated operations and the platform Brage. Most of quantitative information provided in the introduction sector was collected during this time period.

The Albany modeling team produced an integrated SD map. This map is composed of 11 basic structures and theories that emerged during the first GMB workshop. In Table 3, two examples are presented. (For details, please refer to Rich and Gonzalez 2006)

Table 3 Two examples of the basic structures and theories emerged during May GMB workshop



4.4 Group Model Building Workshop 2

Time: Sep 7-8 2005

Participants: AMBASEC (7 persons: three senior researchers in information security served as client, the other four were modeler and process observers)
 IRMA (3 persons: all of them served as client)
 Hydro (5 persons: including CEO of the Integrated Operations project, platform chief, chief information security officer and other two persons working in ICT field)
 NTNU⁴ (1 person: expert in information security served as client)
 Albany (3 persons: facilitation team)

More people participated in the second workshop, indicating greater client engagement. Trust started to build between the client and SD modelers. Interestingly, the participants are mostly those with high interest / high influence listed on the stakeholder map. This could have different reasons. We like to believe that the stakeholder map captured indeed the most relevant actors and that they perceived the GMB workshop as relevant.

Purpose: To develop a prototype simulation model

⁴ NTNU stands for Norges Teknisk-Naturvitenskapelige Universitet (Norwegian University of Science and Technology)

The first GMB workshop had identified the problem and formed eleven basic structures and theories. These eleven basic structures were presented in the initial stage of the second workshop to help refresh consensus. Looking ahead for the scope of the second GMB workshop, we intended to develop a prototype simulation model with the group.

Data obtained:

✓ ***Introduction of Integrated Operations***

The presentation showed the vision of Integrated Operation, the executive plan and the current stage and some issues during the operation transition.

✓ ***Introduction of one new work process implemented in Integrated Operations***

One of the most important new work processes implemented at Brage is the daily production optimization process. This new process could retrieve a higher percentage of oil from the reservoirs, implying higher revenue. The workflow for this new work process was presented.

✓ ***Presentation of the Brage’s Information System architecture***

The Brage’s Information System architecture was presented. The Brage team explained how information (data) flows from the platform to the control center and vice versa.

✓ ***Risk matrix***

IRMA presented the risk matrix they had developed for the Brage case. The matrix includes two dimensions, the frequency of incidents and the consequence of incidents. (Figure 4). Various incidents are represented by different points in the matrix.

Frequency	F5	F4	F3	F2	F1
Consequence					
C5			R1		
C4		R4		R2	
C3		R5		R3	
C2			R6		
C1				R7	

Figure 4 Risk Matrix⁵

The color-coding represents relative severity of incidents. The red zone incidents should not happen. Policies to reduce the frequency or the consequences of these incidents should be implemented immediately. The yellow zone is less severe. Policies for these incidents require a cost-benefit analysis. Finally, the green zone incidents have low impact and they can be ignored for now. This matrix is the experts’ estimation based on past experience.

✓ ***Work process development timeframe***

The group was asked to develop ideas about the maturation of work processes and to formulate some reference modes. We got three different ideas from three different sub groups among the workshop participants.

⁵ We have hidden all the real data on the risk matrix to keep company’s information confidential.

The timing of the process introduction and maturation appears to range between three and seven years to approach the goal. This information helps us to set the time horizon for the model to be around 100-120 months.

Insights:

Some more dynamic hypotheses emerged during the second GMB workshop. A few examples follow:

- The introduction of new technologies enables new work processes that bring along with them knowledge gaps, creating vulnerabilities.
- Maturing technologies, work processes and knowledge close the gaps and reduce vulnerabilities.
- Attention to incident response and knowledge management speeds up the maturation processes thereby reduces vulnerabilities, incidents, and damage.

Maps and models:

We spent much time in identifying and drawing feedback loops with the client, which resulted in a more complete cognitive map. The stocks and flows characterize the operation transition. The three circles, i.e. organizational change, incidents and learning from incident, illustrate the key issues the model should capture. Future work will address the issues implied in these circles.

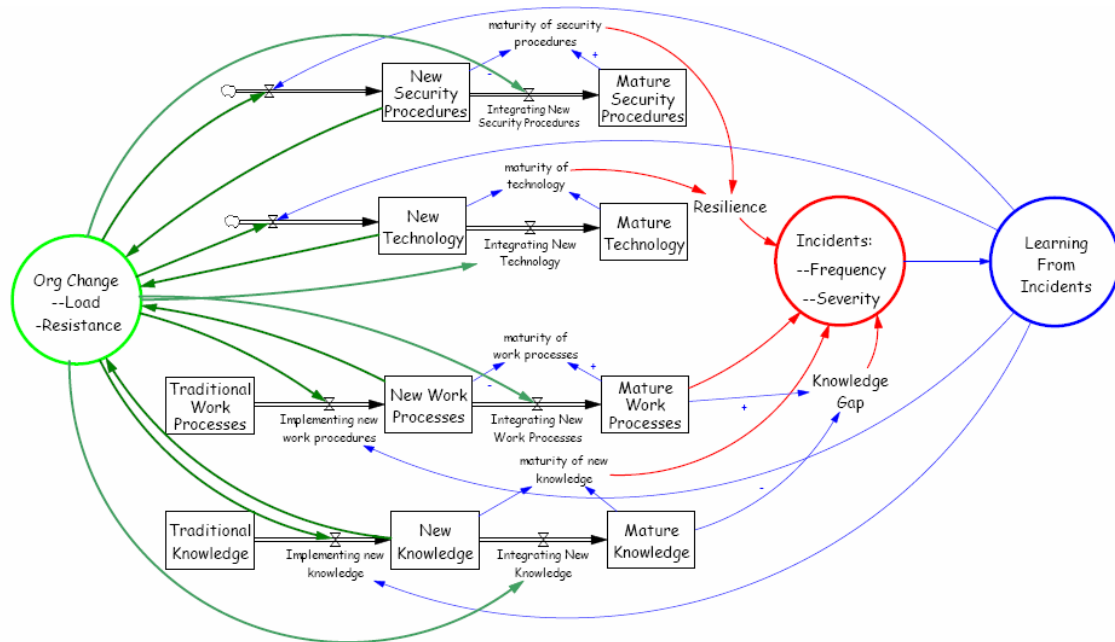


Figure 5 Cognitive map derived from the GMB Workshop 2

Client attitude:

Most of the participants found the group model building workshop an effective way to address the problem. We got very positive comments, especially from the platform chief

and the chief information security officer. The client signaled further commitment as reference group for model development.

New policies implication:

The second group model building workshop helped to establish a new policy. During the workshop discussions, the client mentioned the issue of staff shifts on the platform. In Norway, the working schedule for on-platform employees is two-week working and four-week vacation. Three groups of people rotate in turn. Currently, there is no formal handover process except for the managers. Helicopters carry off-platform staff onto the platform and bring the on-platform staff back. The idea to invest in mobile communication devices so that staff off-platform will be able to connect with staff on platform emerged during discussion. The improved communication will facilitate information sharing and knowledge building, therefore, reducing vulnerability and speeding up further operation transition. The client decided to further investigate this new policy after the workshop. (For detailed information about this workshop, please refer to Rich, Andersen, and Richardson 2005)

4.5 After Group Model Building Workshop 2

The Albany group developed a prototype model Hydro 1. It includes 4 submodels—Work processes, Knowledge, Vulnerability and Incidents. The simulation model shows how inadequate mature knowledge in relation to new work processes causes higher vulnerability. It also shows that shifting resources to knowledge development significantly reduce vulnerability.

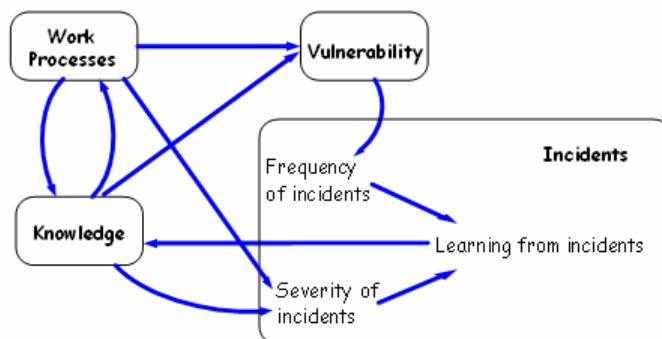


Figure 6 Basic structure of the Hydro 1 model

After the second workshop we had several teleconferences with Hydro and IRMA, presenting the model structure, showing simulation behaviors, discussing the terminology of variables, definition of variables, and parameter values, etc. The client provided more data to calibrate the model. The client also raised questions, some of which requiring explanations, while others providing hints to further model development. For instance, one issue was the definition of knowledge. The modeling team decided to disaggregate knowledge into knowledge about work processes and knowledge about technology. The client felt more comfortable with the model. But then they asked about organizational knowledge. Currently, we are looking for ways to include knowledge about organization into the model. Another model development focus is to link the IRMA risk matrix with the dynamic model. When achieved, the

model will be able to show how different risks change during the operation transition. This is work in progress, requiring further discussion with the client.

Going through these model-based communication processes, the model was extended into seven submodels. The newly added submodels are Technology, Security Culture and Learning from Incidents.

The CEO of the Integrated Operations project expressed that he liked the approach, which he deemed relevant for the practice.

Discussion

The two group model building workshops help to shape our idea. Looking back upon our starting point in March 2005, we assumed that the client's problem was with its CSIRTs (Computer Security Incidents Response Team): how they should be proactive rather than reactive, collect data and share data with scientists. Then in May workshop we found out that there were no formal CSIRTs for platform. Incidents are handled by ad hoc teams. The client's problem was knowledge gap and technology gap generated by the transition to Integrated Operations. This problem definition was gradually dug out from underneath through various exercises. When it was finally articulated by the modeler's reflection, I perceived that all the participants felt enlightened. There was an "Ahaa" experience. After the first workshop, we were able to ask relevant questions, identify related literature and important information because we understood the problem well. We were not walking in the dark any more. The direction to proceed was clear. On the second workshop, we dived into more details, such as specific work process and IT architectures. Through the discussion, more data were collected.

Besides defining the problem and getting data, more importantly, we established trust with our client through the workshops. At the beginning of the first workshop, the project CEO said he was not sure whether Brage was a proper case for the research. After 3-hour morning session, he expressed his interest in the approach. He told us what he didn't like was the "black-box" modeling, showing simulation results without properly showing and explaining the logic behind the model to the client. But it turned out that our approach was not like that. He liked the discussion and felt the ownership of the model. At the end of the day, he was quite convinced that the approach could address Brage's problem. He promised to assign more people to participate in the second workshop. In the second workshop, several high influence/high interest stakeholders participated. We had intensive discussion about the operation transition, technology, incidents etc. The information they provided was of great importance.



Figure 7 Group discussion

The CEO, CISO (chief information security office) and platform chief even continued discussion after we ended the first day workshop. The second morning, they came and told us their new idea about technology as a double-edge sword, which brings improvement as well as vulnerabilities to the system. They all agreed that new technology should be tested before application and employees should be well trained ahead of implementation. At the end of the workshop, the client expressed that they learned a lot during the workshop.

Our research project has made significant progress with the two group model building workshops. However, the meetings and interviews after the workshops are not correspondingly effective. Several problems have shown themselves and continue to persist.

First, we are not located in the same city as the client. Therefore, the meetings we had with client were all via Internet. Thanks to internet software, such as Net Meeting, we were able to share application with the clients. However, the communication is not as good as face-to-face. We were able to follow each others idea most of the time. Yet we had much less discussion than sitting in a room together, drawing on cling sheets on the wall. It is especially difficult to talk about models. We tried to show the model at high level with simple structures, but the clients still have difficulty grasping the model ideas. We are planning to have some roundtable meetings in the future. But still, most of the communication will be through teleconferences. How to improve effectiveness of distant communication through Internet and teleconferencing is an issue.

Second, the members of the model reference team are all high level management personnel. They have a tight working schedule. Though they are interested in the research, they did not have enough time to participate in the model building. The ideal way for them is that we do the research and they learn from the results. But we need the clients' inputs to advance the model. And they are the people to validate the model. Without these, it is difficult to reach meaningful insights. Another point is that in order to build trust in the model, the clients need to be part of the modeling effort. If they do not trust the model, they will not learn from its results either.

We are learning from former experience (Vennix) and from our own experience to look for effective ways of communication. Both the clients and we learn from this process.

Acknowledgment

This paper is an outcome of the AMBASEC project, grant number 164384. We kindly thank the Research Council of Norway for funding.

References

- Andersen, D. F., and G. P. Richardson. 1997. Scripts for group model building. *System Dynamics Review* 13 (2):107-129.
- Andersen, D. F., G. P. Richardson, and J. A. M. Vennix. 1997. Group model building: Adding more science to the craft. *System Dynamics Review* 13 (2):187-201.
- Andersen, David F., Dawn M. Cappelli, José J. Gonzalez, Mohammad T. Mojtahedzadeh, José-María Sarriequi, Elise A. Weaver, Andrew P. Moore, Aldo Zagonel, Eliot Rich, and Jeffrey M. Stanton. 2004. Preliminary System Dynamics Maps of the Insider Cyber-Threat Problem. Proceedings of 22nd International Conference of the System Dynamics Society, July 25-29, at Oxford, England.
- Gonzalez, Jose J. 2005. Towards a Cyber Security Reporting System -- A Quality Improvement Process, in Computer Safety, Reliability, and Security. *Lecture Notes in Computer Science* 3688:368-380.
- Gonzalez, Jose J., Ying Qian, Finn Olav Sveen, and Eliot Rich. 2005. Helping Prevent Information Security Risks in the Transition to Integrated Operations. *Teletronikk*:29-37.
- Killcrece, G., K. Klaus-Peter, R. Robin, and Z. Mark. 2003. *State of the Practice of Computer Security Incident Response Teams (CSIRT)*.
- Luna-Reyes, L. F., and D. L. Andersen. 2003. Collecting and analyzing qualitative data for system dynamics: methods and models. *System Dynamics Review* 19 (4):271-296.
- Qian, Ying, J.J. Gonzalez, and Finn Olav Sveen. 2005. Defining Complex Problems Using Group Model Building and System Archetypes. Proceedings of the 2005 Conference of System Dynamics and Management Science: Sustainable Development of Asia Pacific, at Shanghai, China.
- Rich, Eliot, D. F. Andersen, and G. P. Richardson. 2005. OLF-IRMA-AMBASEC Group Model Building Technical Report I: 25-26 May 2005: University at Albany, State University of New York.
- . 2005. OLF-IRMA-AMBASEC Group Model Building Technical Report II: 7-8 September 2005: University at Albany, State University of New York.
- Rich, Eliot, and J.J. Gonzalez. 2006. Maintaining Security and Safety in High-threat E-operations Transitions. Proceedings of the thirty-ninth annual Hawai'i International Conference on System Sciences, at Hawaii.
- Richardson, G. P., and D. F. Andersen. 1995. Teamwork in Group Model-Building. *System Dynamics Review* 11 (2):113-137.
- Richardson, G. P., D. F. Andersen, and Luis F. Luna-Reyes. 2005. Join Minds: Group modeling to link people, process, analysis, and policy design.
- Vennix, J. A. M. 1999. Group model-building: tackling messy problems. *System Dynamics Review* 15 (4):379-401.
- Vennix, Jac A. M. 1996. *Group model building : facilitating team learning using system dynamics*. Chichester ; New York: J. Wiley.