Managing emerging information security risks during transitions to Integrated Operations

Ying Qian
University of Agder
Norway
ying.qian@uia.no

Yulin Fang
City University of Hong Kong
Hong Kong
ylfang@cityu.edu.hk

Martin Gilje Jaatun
SINTEF ICT
Norway
Martin.G.Jaatun@sintef.no

Stig Ole Johnsen
SINTEF Technology and Society
Norwegian University of Science and Technology
Norway
Stig.O.Johnsen@sintef.no

Jose J. Gonzalez
University of Agder
Gjøvik University College
Norway
Jose.j.gonzalez@uia.no

Abstract

The Norwegian Oil and Gas Industry is adopting new information communication technology to connect its offshore platforms, onshore control centers and the suppliers. The management of the oil companies is generally aware of the increasing risks associated with the transition, but so far, investment in incident response (IR) capability has not been highly prioritized because of uncertainty related to risks and the present reactive mental model for security risk management. In this paper, we extend previous system dynamics models on operation transition and change of vulnerability, investigating the role of IR capability in controlling the severity of incidents. The model simulation shows that a reactive approach to security risk management might trap the organization in low IR capability and lead to severe incidents. With a long-term view, proactive investment in IR capability is of financial benefit.

1. Introduction

Connecting to a complex environment is not a choice for today's organizations, but a necessity to survive and thrive. Even the businesses where the consequences of incidents could be major, such as oil and gas production, are moving towards this direction. Intense competition requires organizations to be more effective, often by the means of information and communication technologies (ICT). The cost to organizations is that the technology is often more complex, takes specialized support and resources, and creates a rich environment for breeding vulnerabilities and risks [2][4][11].

According to the 2008 CSI/FBI (Computer Security Institute / Federal Bureau of Investigation) Computer Crime and Security Survey, 47% of the 512 responding firms experienced computer security incidents, such as virus, insider attack, laptop theft, denial of service attacks, unauthorized access of data or networks, and bots. The survey also shows that incidents occur frequently, with 47% of those who experienced incidents, reported to have 1-5 incidents over the 12 month, 14% reported 6-10 incidents over the 12 months, and 13% reported over 10 incidents over the 12 months. The average financial loss per respondent was $288,618 [1].

Most organizations view security control as an overhead and adopt a reactive security management approach, i.e., they address security concerns only when security incidents are discovered. (Not all incidents are discovered. Some stay latent in the system.) Indeed, "actions taken to secure an organization's assets and processes are typically viewed as disaster-preventing rather than payoff-producing, which makes it difficult to determine how best to justify investing in security, and to what level" [5]. For those responsible for security, it is often difficult to persuade senior executives and board members of the need to implement information security in a systemic way [5].

The difficulty to "sell" the proactive investment is because a paradox exists in information security management: If investment is made proactively, the frequency of incidents and severity of incidents will be reduced, leading to low perception of risk and making it difficult to justify the investment in information security management. Caralli and Wilson [6] point out that the reason why security is viewed as overhead is the lack of financial justification. They argue that "organizations do not routinely require return on investment calculations on security

IEEE computer society

978-0-7695-3869-3/10 $26.00

investments, nor do they attempt to measure or gather metrics on the performance of security investments".

In this paper, we argue that the reactive approach to security risk management could trap enterprises into blindness to minor incidents, which could finally result in severe incidents. We do so by building a system dynamics model that capture the dynamics of risk management. We investigate a specific case: an offshore oil platform that started transiting its traditional operation to Integrated Operations (IO), by adopting advanced ICT (information and communication technology) to connect to the onshore control centers and suppliers. The operation transition will last several years with profound ICT-enabled changes to many work processes [3]. These changes, however, inevitably come with security risks. System dynamics is used to model the operation transition as well as the managerial responses to the information security risk.

Research based on this case using system dynamics has been reported earlier in previous HICSS conferences and other conferences [13][14][15][16][19], where research effort was devoted to forming conceptual models [13][14][15], and building a formal model that focused on understanding how to reduce the vulnerability of the operation processes during the operation transition [16][19]. The current study takes one step further by adding a sub-model to understand the decision-making process of investing in IR capability. Specifically, we compare the proactive security risk management approach (i.e., investing before the operation transition) with the reactive approach (invest in IR capability as and when incidents are discovered).

The remainder of the paper is organized as follows: Background information about the case will be provided in section 2. Section 3 presents the literature review relevant for this case study. We will describe the model in section 4, and the analysis of the model behavior is presented in section 5. Finally, we discuss our findings in section 6.

2. Norwegian Oil and Gas Industry's Transition to Integrated Operations

2.1. Transition to Integrated Operations

The Norwegian Oil and Gas Industry is moving into integrated operations (IO), which lead operating companies to adopt new ICT solutions. These solutions include collaborative videoconferencing, remote control of hardware and real-time decision support, linking the different actors (onshore, offshore, suppliers) together through high-capacity computer networks.

Profound changes will take place for the operation transition. In traditional operation, an offshore field is essentially a closed system: all the skilled resources need to be on-platform, at significant cost and some risk to personal safety (see Figure 1).

- 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

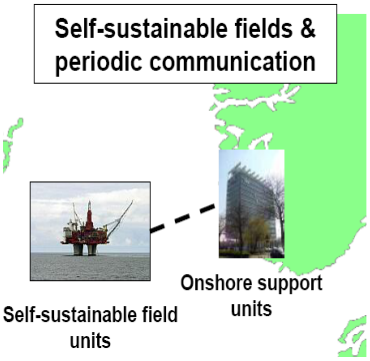

Figure 1 Traditional operation

In the IO paradigm, onshore centres normally closely collaborate with offshore personnel through ICT technology solutions that share real-time data and provide real-time collaboration facilities.

- Decisions are made together by operators on/offshore and consultants at vendors' onshore expert centers
- Several work processes and decisions are automated
- The vendors deliver their services digitally, i.e., over "the net"

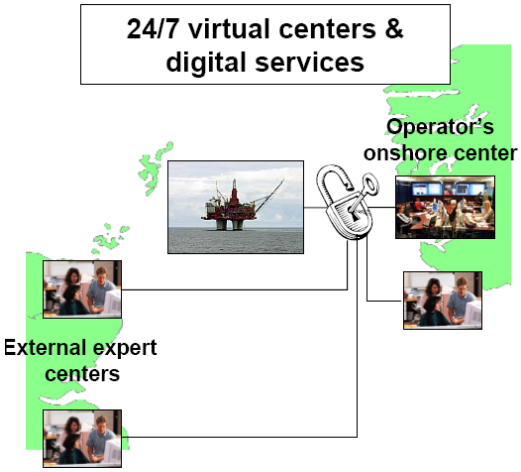

Figure 2 Integrated Operations

This operation transition is expected to increase production by 5%-10% and reduce cost of operating by 20%-30%. It is estimated that the net present value of Integrated Operations on the Norwegian Continental Shelf (NCS) is in the order of NOK 150 bill [3]. (Also see www.olf.no)

Despite the huge financial benefit of IO, the operation transition is full of challenges, with the increasing information security risks as a major one.

From the technological aspect, the prevalence of standard PC hardware and commercial off-the-shelf (COTS) software, and the availability of remote control create a new opening for malware to infect (and ultimately control) the systems. The increased interconnections between process control networks and office networks create more points where the combined network may fail or be exploited by outsiders and other external attacks.

From the human factors aspect, change is a difficult and painful process. When advanced technology is in place and new work processes are implemented, people need to take time and effort to familiarize themselves with the new system. Unfamiliarity is one reason which causes human error [18]. The new operation is based on the effective communication and collaboration via video conferencing, which is completely different from the traditional operation. It is a challenge for people to learn to communicate effectively in a new way, and for those who are moved from offshore to onshore, new skills will be needed to perform the new tasks.

From the organizational aspect, new work assignments and new work locations could disrupt the company's social structures and their associated "know-who" networks. Rebuilding such structures takes time. Above all, the company is moving into an uncharted territory where no former experience exists. What to do, how to do, when to do are questions that must be considered with care.

The Norwegian Oil and Gas Industry is generally aware of the high risks underlying the operation transition. They use several oil platforms as pilots for the operation transition. One of them is the focus of our study.

2.2. The Platform under Study

The platform under study has been in production for more than 15 years. It has reached its tail stage with decreasing oil production, with traditional operation yielding revenues barely enough to cover the production cost. Rather than writing off this multi-million investment by abandoning these oil fields and their remaining oil reserves, the company could extend the lifetime of the mature platforms with deployment of IO.

Moving into IO, the platform is getting connected to a high-speed information network. Production decisions are now made together with onshore experts. Some of the work is moved to the onshore control center; not all skills are needed all the time on every platform. The basic manning of this platform has been reduced from 41 to 25 persons. The increased production and the reduced manning has increased profit substantially and extended the life span of this platform.

However, nothing comes without a cost. Production processes involved in IO are complex and tightly coupled. Integrated operations require a variety of systems to be interconnected and large amounts of information to be shared. This makes the platform vulnerable [9]. Moving from traditional offshore operations to IO requires the acquisition of more skills. Offshore operators need to know more about how to operate and respond to the new integrated ICT and supervisory control and data acquisition (SCADA) systems. Onshore engineers will need to interpret the data they are receiving from the various sensors and visualizations, rather than what they directly observe on the platform. During the operation transition period when skills are not fully developed and people are not familiar with the complex and tightly coupled work processes, the platform is at risk.

Building IR capability is one important approach to controlling risks [15]. In the traditional operation, IR capability was less relevant because the platform was a closed and secure system with very few information security incidents. The major concern was about safety accidents in a hazardous environment. There was no formal incident response team on

the platform; ad hoc teams assembled when emergencies happened. However, moving into IO has increased the needs for information security risk management. During implementation of IO, there is a need to integrate ICT and SCADA systems. The knowledge, background and risk perceptions between ICT and SCADA professionals vary greatly. The ICT professionals have based their risk perceptions on ISO 17799, while the SCADA professionals have based their risk perceptions on IEC 61508. In addition the responsibility of ICT and SCADA systems are placed in different organizational silos, with little collaboration and few common risk perceptions [17].

Interviews with experts in security management showed that the platform management teams had not worked to proactively identify risks related to integration of ICT and SCADA systems or improve IR capability when the operation transition started. Almost no risk and vulnerability analysis has been performed of the integration of ICT and SCADA systems, i.e. some of the risks and challenges are not known in addition to few common risk perceptions. One important motivation of IO is to reduce cost, and additional investment in IR capability must be presented to management and supported by both the SCADA and ICT professionals. This has not always been presented in such a manner that IR capability has been increased. Although the management is aware of increasing risk during the operation transition, they still think the probability of incidents happening is pretty low. Their mental model is investing in IR capability when real signs of increasing incidents are observed, i.e., a reactive approach.

In the early 1990's, when the use of internet started to spread in business organizations, Loch, Carr and Warkentin conducted a survey of information systems managers and found a gap between the use of modern technology and the understanding of the security implications inherent in its use. They pointed out that "many of responding information systems managers have migrated their organizations into the highly interconnected environment of modern technology but continue to view threats from a perspective of a pre-connectivity era." They also identified that the respondents were aware of the threats but naively viewed their risk to be moderately low [11]. From our group discussions with our client and interviews with information security management experts, the platform's management has the same mental model as that presented by Loch, Carr and Warkentin 15 years ago.

Perrow has proposed a theory of normal accidents based on interaction (degree of complexity) and couplings. When interactions between systems are complex and the couplings between systems are tight. Perrow proposed that an accident could be the "normal" outcome 错误！未找到引用源。 This perspective is relevant in IO since the implementation of IO can lead to increased complexity and increased coupling. The two dimensions of interest, Interaction and Coupling are discussed further in the following.

Interactions are described as going from linear (expected and familiar sequence) to complex (unfamiliar sequences not planned or unexpected). Complex systems are described as systems characterized by proximity, common-mode connections, interconnected subsystems, limited substitution, feedback loops, multiple and interaction controls, indirect information and limited understanding. Due to the increased interaction of ICT and SCADA systems in IO, the increased exploration of real time data and different organizational silos of competence between ICT and SCADA – it is clear that the interactions are complex. A security (or safety) incident in the ICT/SCADA systems may have complex and unanticipated consequences.

Coupling is described as varying from loose to tight. A tight coupling has no buffers or slack between two items and what happens in one directly affects what happens in the other. Loose coupling have flexible performance standards and can incorporate failures, delays and changes without destabilization. Tight Coupling are described as systems characterized by: delays in processing not possible, invariant sequences, only one method to achieve goal, little slack possible (in supplies, equipment, personnel), buffers and redundancies are designed-in (deliberate) and substitution (of supplies, equipment, personnel) limited and designed in. In the traditional operation when platform operated generally on its own, there were more flexibility, and it was easier to adapt to changes without destabilization. However, as IO is implemented, production planning is made with external experts and the ICT system is linked with the SCADA system, there is less flexibility and small deviation might be enlarged by the interaction of various systems and cause destabilization. Thus, we the systems may become more tightly coupled. As a consequence, the platform may have an increasing risk of normal accidents as IO is implemented.

3. Prior Research

Here, we briefly introduce the prior research efforts and how this work is positioned. System dynamics have been used for two reasons: First, it serves as a communication platform through which to elicit information from clients and experts and to provide feedback on the model insights to the clients. System dynamics group model building workshops were conducted for problem identification and model conceptualization [14][8]. Second, system dynamics is an important modeling tool to help advance our scholarly understanding of the dynamics associated with the long-term operation transition and information security risk management during this process.

Eleven hypotheses about the operation transition and the risk change in this process were identified during the first group model building workshop with clients. How the first group model-building workshop was conducted was reported in detail in the paper [14]. These hypotheses form the basis for formal model development. These eleven hypotheses were first presented in [15] and illustrated with conceptual models and explanations. Here we summarize them in Table 1.

Table 1 - The Eleven Dynamic Hypotheses

H1	A Knowledge Gap Drives Risk
H2	A Work Process and Capacity Gap Drives Risk
H3	Collaborative Workplaces Close Knowledge and Work Process Gaps
H4	Resistance to Change Traps Collaborative Workplaces
H5	CSIRT Capacity Creates New and Mature Security Procedures
H6	Detection Capacity Reduces Damage
H7	Misperceptions of Risk Create Detection Traps
H8	Mitigation Capacity Reduces Damage and Promotes Learning
H9	Evaluation Capacity Creates Long Term Learning.
H10	CSIRT operations may create a Mitigation Trap
H11	Compliance Dynamics Further Increase Risk

There are two approaches to manage the risk [17]. One is to control the threat by reducing the likelihood of occurrence, i.e. to reduce the vulnerability of the system. The other is to reduce potential impact and/or ensure that the organization can handle the result of a realized risk, i.e. to increase the IR capability. Our prior research has built a formal system dynamics model to simulate hypotheses 1-4. This modeling effort focused on the first approach, looking for ways to reduce the vulnerability of the system so that threats are less likely to penetrate and become incidents. The model and behavior analysis were reported in [16][19].

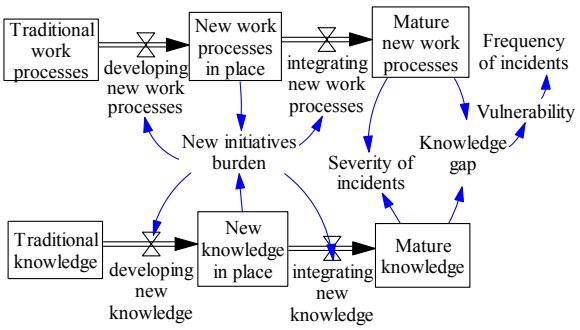

Figure 3 Model focus on vulnerability

Figure 3 presents the simplified structure of the formal model based on hypotheses 1-4. The operation transition is represented by the two chains of changing work processes and knowledge. Knowledge takes longer time to mature than work processes. Therefore, a knowledge gap will be generated and it drives vulnerability (H1). Capacity is an abstract concept that was not included in the formal model. Thus, H2 could not be identified. The practice of the new work processes in collaborative workplaces makes new work processes and knowledge mature and close the gap between them (H3). Change is difficult; new work processes and knowledge represent a burden to people. This new initiative burden traps the operation transition (H4). (Refer to [16][19] for details). The main conclusions of the papers are 1) hurrying an implementation can result in significant risks; 2) special care should be given to knowledge development during the operation transition; and 3) knowledge maturation could help to reduce the vulnerability.

The model effort in this paper focuses on Hypotheses 5-8, seeking to show how a proactive approach to invest in IR capability before the operation transition starts can help control risk. With simulation, we also investigate why reactive thinking does not work well in controlling risks.

As stated in H5, CSIRT (Computer Security Incident Response Team) capacity creates new and mature security procedures. In the model, these security procedures are all presented in IR capability. IR capability reduces damage (H6). When the IR capability is low, fewer incidents could be detected, leading to misperceptions of risk. This results in under investment in IR capability and even lower detection (H7). As new work processes and knowledge mature, the platform would be more resilient, reducing the damage from incidents and promote learning (H8).

4. Model of incident response (IR) capability

Our formal model is mainly based on hypotheses 5 to 8 in Table 1, and is presented on Figure 2.

IR capability measures how many incidents could be handled per month. This has two aspects: one is how many resources (people*time) are devoted to the work, and the other is how productive these resources are. A decision to increase incident response capability could be to add more resources to the work or to improve the productivity of the existing resources, e.g. by training. For simplicity, in the current version of the model, we do not disaggregate these two aspects. IR knowledge and capability becomes obsolete over time. New threats, such as new attack tools, new vulnerabilities, and new viruses, emerge quickly in the area of information security. We assume that knowledge and capability of IR will become obsolete after one year, and need to be updated.

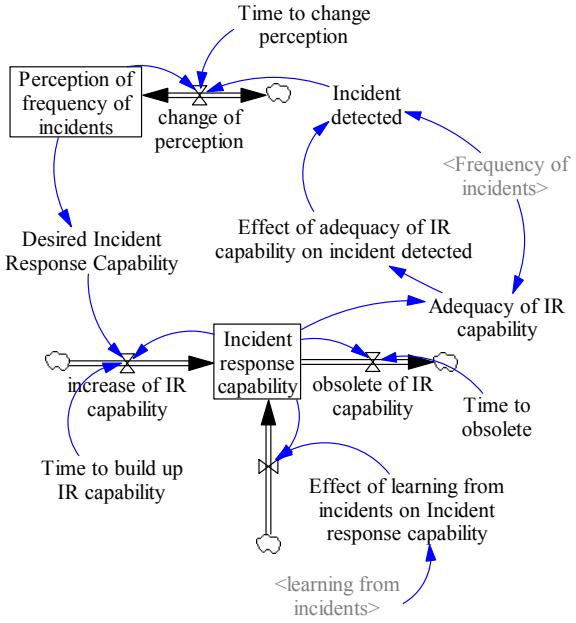

Figure 4 Incident response capability

The lower part of Figure 4 focuses on the change in IR capability. The increase in IR capability is mainly from the management's investment, which is based on the desired IR capability. The management invests to adjust the IR capability to the desired level. Note that this adjustment takes time. If the desired IR capability level is lower than the real IR capability, no further investment will be made. As IR capability obsoletes, it will be reduced.

The desired IR capability is based on the perception of the frequency of incidents. The upper part of Figure 4 focuses on the perception of the frequency of incidents. Not every incident is detected; there is always a fraction that goes unnoticed. How large this fraction is depends on the adequacy of the IR capability (see equation 1).

Adequacy of incident response capability = Incident response capability / Frequency of incidents [Equation 1]

If we have a high adequacy of IR capability, then a higher fraction of incidents will be detected. If we have a low adequacy IR capability, a low fraction of incidents will be detected. The incidents detected will change the management's perception of frequency of incidents over time, which relates to the perception of risk.

With a low IR capability, fewer incidents will be detected, and the perception of frequency of incidents will be low, as well as the desired IR capability, As a result, investment in IR capability will not be enough, which might cause severe incidents in the future. This is the capability trap identified in the group model-building workshop.

5. Model scenarios analysis

This model of IR capability is linked into the model of operation transition, making an extended platform model. This model went through the standard model validation tests, including direct structure test and structure oriented behavior test. Moreover, we interviewed experts in information security management showing model behavior of different scenarios. Their recognition of the model behavior added confidence to our model.

With this model, we investigate two different scenarios: (1) reactive information security management — raise IR capability when seeing incidents happen, and (2) proactive information security management — raise IR capability before major changes – such as operation transition. Only one parameter is changed, that is the initial IR capability. In the traditional operation, the IR capability was quite low because there was little information security incidents. The IR capability is to prepare for around 1 incident/year, which is approximately 0.1 incident/month. In the first scenario (the reactive approach), the management keeps the IR capability level despite their concern about increasing information security risk. In the second scenario (the proactive approach), the management raises the IR capability to 0.3 incident/month before the operation transition starts. In IO, the IR capability is to prepare for at least three

incidents a year. In this scenario, we first try with the amount of 0.3/month, which is three times as high as the original IR capability. Of course, different parameters could be tested using the system dynamics model. However, in reality, even being proactive, the management will not raise the IR capability very high considering the limited resources available to the organization.

Table 2 Parameter setting for scenarios

Scenarios	Initial IR capability	Meaning
Reactive	0.1 incident/month	0.1 incident could be handled in a month
Proactive	0.3 incident/month	0.3 incident could be handled in a month

The simulation behavior is presented in Figure 5-12. The blue line with number 1 represents the reactive scenario and the red line with number 2 represents the proactive scenario.

The IR capability affects the severity of incidents (H6). It does not influence the operation transition. It could be argued that when severe incidents happen, the operation transition will be delayed or even stopped. However, this linkage is not included in the current model. As a result, we can see that mature new work processes and mature new knowledge behave exactly the same for the two scenarios.

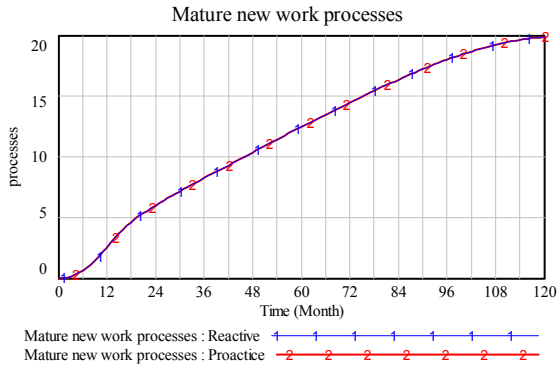

Figure 5 Mature new work processes

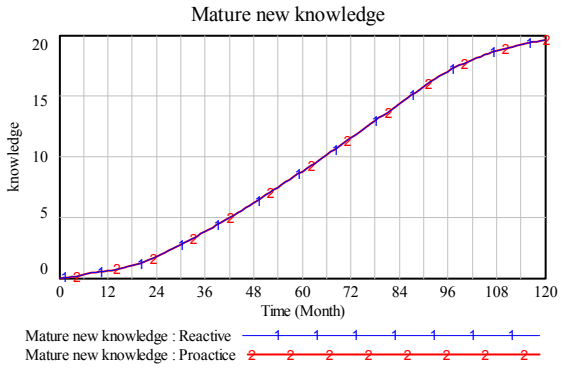

Figure 6 Mature knowledge

As mentioned above, vulnerability of the system (called vulnerability index in the model) is affected by new work processes, new knowledge and knowledge gap. As the two scenarios have exactly the same speed of operation transition, these three factors do not differ for the two scenarios, this leads to identical model behavior of vulnerability Index. Vulnerability Index is one important factor influence the frequency of incidents. As a result, the frequency of incidents remains unchanged for the two scenarios.

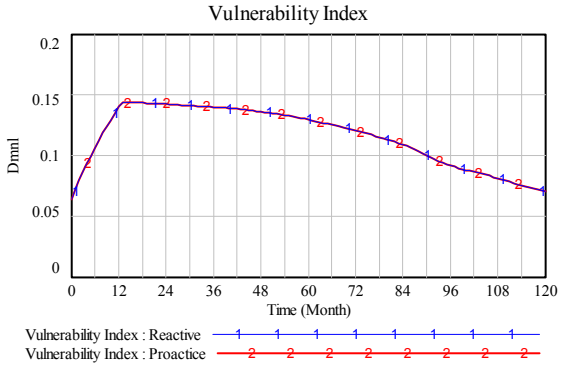

Figure 7 Vulnerability Index

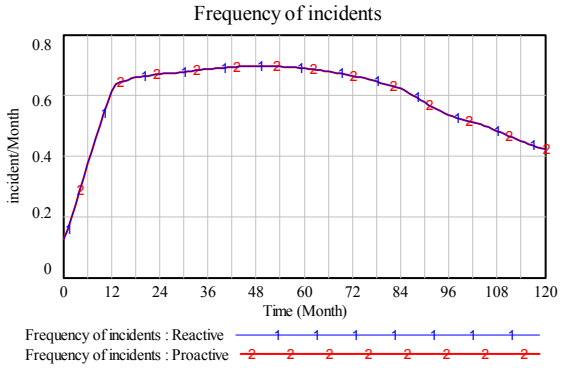

Figure 8 Frequency of incidents

Yet the severity of incidents reduced from peaking at 1.7M/incident in the reactive scenario to

peaking at 1.2M/incident in the proactive scenario, leading around 30% reduction. Suggested by the information security experts in this project, incident cost from 100K-2M NOK is ranked level 3 (level 5 for most serious incident), labeled as "dangerous", and cost from 2M-20M NOK is ranked level 4, labeled as "critical". We can see that in the reactive scenario, the incident severity is approaching critical level. For the proactive scenario, the severity of incidents stays in the middle of dangerous level.

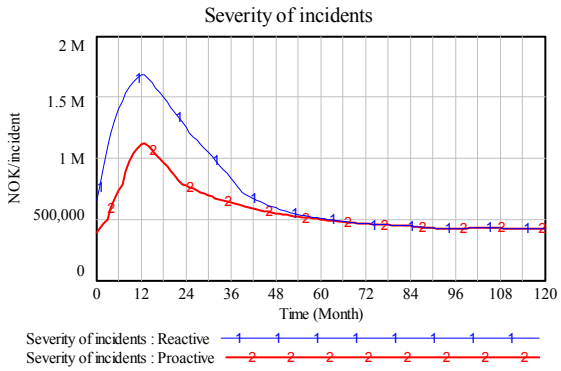

Figure 9 Severity of incidents

Expected incident cost is the product of frequency of incidents and severity of incidents. Frequency of incidents is tightly related to the vulnerability of the system, which is the same for the two scenarios. The severity of incidents is lower in proactive scenario. As a result, the expected incident cost peaks about 30% lower in the proactive scenario compared to the reactive scenario.

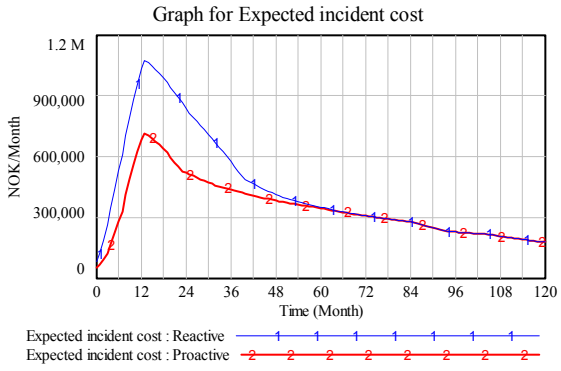

Figure 10 Expected incident cost

In the reactive scenario, the IR capability starts from 0.1 incident/month. As the operation transition starts, the frequency of incidents increases sharply in the first year as new work processes and knowledge are implemented and a knowledge gap generated. However, the IR capability increases slowly (see Figure 11), much more slowly than the increase of frequency of incidents (see Figure 8).

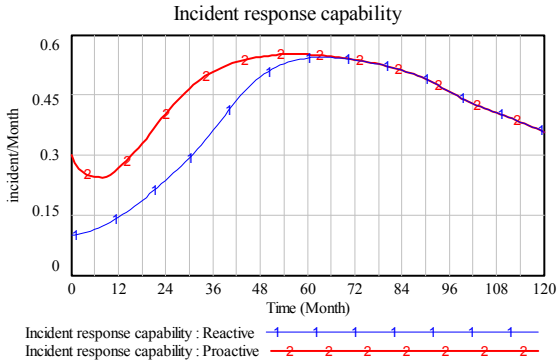

Figure 11 Incident response capability

There are two reasons that account for this slow growth of IR capability. First, there are delays in the system. It takes time for the management to perceive the increase of incidents. In our model, there is a three-month delay before the perception of frequency of incidents is changed. This is because the incident data are reported and reviewed quarterly. There is another time delay to build IR capability. The IR capability will not be immediately ready when the investment decision is made. If the decision is to add people to IR work, then it will take time to announce an opening, find the proper person through interviews, and train the people to the specific work. If the decision is to make the existing people more productive, then it will take time to find a proper training program and let people learn.

However, what contributes more in the slow development of IR capability is that with low IR capability, a large fraction of incidents is not detected, as stated in Hypothesis 7. Only the detected incidents can be reported. Therefore, the management's perception of frequency of incidents is much lower than it actually is, and so is the desired IR capability. This leads to underinvestment in IR capability, which results in high severity of incidents later. Figure 12 reports in one chart the frequency of incidents (blue line with F), incident detected (red line with I), desired incident response capability (green line with D) and incident response capability (purple line with C). It clearly shows how incidents detected grow slowly along with the desired IR capability, and the real IR capability follows with another delay. After several years of slow development, the incidents detected gradually approaches the frequency of incidents.

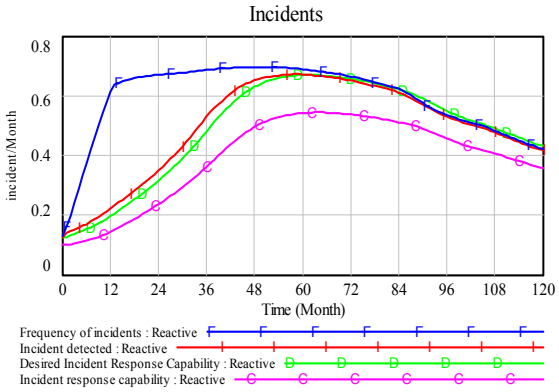

Figure 12 Related variables of the development of IR capability

As we discussed above, severe incidents on an oil platform might have a huge impact, ultimately threatening human life and the environment. The management of companies in the oil and gas industry is keen to avoid severe incidents. However, as we see from the simulation result, reactive thinking could lead to an IR capability trap, which could lead to critical incidents during the operation transition.

With a proactive thinking, the IR capability starts higher and a larger portion of the incidents could be detected. The desired IR capability will also be higher, which leads to less underinvestment. Therefore, the severity of incidents is largely reduced in the proactive scenario (see Figure 9).

Being proactive seems to be a good policy. However, having more IR capability means more money to be invested in IR. The management team is concerned with the financial impact of a policy. We evaluate the overall financial impact of these two scenarios.

> Overall financial impact = Expected incident cost + Cost for Incident response capability. [Equation 2]

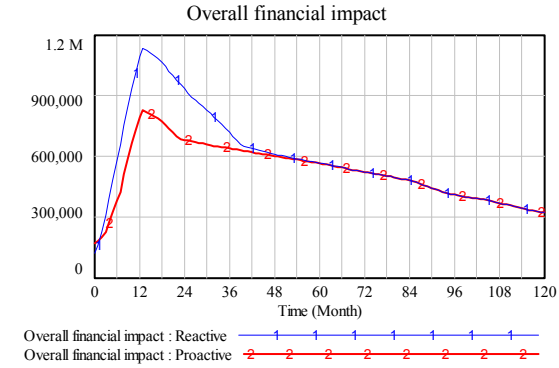

Figure 13 Overall financial impact

In the long run, being proactive generates a much lower total cost than being reactive. (Initially there is a small perturbation). Of course, this result is highly sensitive to the cost of IR capability and the amount of incident cost IR capability could reduce. Yet in a high–risk environment such as an oil platform on the brink of a transition to Integrated Operation when increasing risks is obvious, it is most likely that being proactive would be the optimal choice for the organization.

6. Discussion and Conclusion

This paper uses the system dynamics model to demonstrate how proactive thinking and reactive thinking in information security risk management could generate a different risk picture in the long run. In the reactive scenario, when the IR capability is low at the beginning of the operation transition, fewer incidents are detected, leading to misperceptions of risk. This causes underinvestment in IR capability, and the IR capability might become even more inadequate in the face of increasing information security risk as the operation transition moves on. This IR capability trap could lead to undetected incidents hidden in the system, which makes the system more vulnerable. Furthermore, when incidents happen, the inadequate IR capability might not handle the incident efficiently, thus leading to severe incidents. Being proactive, raising the IR capability before the operation transition starts, would lead to better incident detection and a better risk perception, leading to more realistic investment decisions and better management of the information security risks in the long run. And the model proves that proactive method is cost-beneficial in the long run.

6.1. Contribution to research

This paper builds upon and extends the prior research by building a formal model of IR capability building during the operation transition. The prior research on this case focuses on reducing vulnerability to reduce the frequency of incidents. The link that IR capability could reduce the severity of incidents has not been previously considered. Adding a feedback loop of IR capability building and its influence on severity of incidents completes the information security risk management picture. During the operation transition, policies related to the transition, such as changing the transition speed and changing the resource allocation, will certainly affect information security. At the same time, policies on IR

capability will also have an impact on information security.

A system dynamics model is used to compare cost-effectiveness of proactive versus reactive approach. Many scholars have proposed a proactive approach for information security, such as [7][20]. Yet they do not have quantitative analysis on cost-effectiveness of proactive approach. Allen has suggested the following changes in information security management [5].

Table 3 Shifts in Perspective

From:	To:
Security is a technical problem.	Security is a enterprise-wide problem
Security has a technical owner.	Security is owned by the enterprise.
There is an intermittent focus on security.	Security is integrated.
Security is an expense.	Security is an investment.
The goal is security.	The goal is business continuity and ultimately resiliency.

If the perspective of security has changed from an expense to an investment, it would become easier to justify the proactive investment in IR capability. However, the shifts in perspective take a long time. Meanwhile, we can use system dynamics models to justify the proactive investment and help people to realize that security is an investment, or at least cost beneficial.

6.2. Contribution to practice

In this highly competitive world, companies try to cut any cost that might be unnecessary. Therefore, it is seldom that management is proactive in information security management. The platform under study is one case among many. A recent study of Johnsen shows that risk awareness on offshore oil installations is poor [10]. “Only 5 of the 46 installations had performed a risk and vulnerability analysis, to identify the most dominating risks related to integration between SCADA and ICT systems.” This low awareness leads to poor incident reporting, misperception of risk and low IR capability, which is a dangerous situation. Through model simulation, we can see that without raising initial IR capability, the severity of incidents sharply increases, approaching critical level (the second most severe level). Considering that the severity of incidents in the model is an average figure, this means that there is potential of highly critical incidents happening. If anything on such a scale should happen, it will have huge impact on the reputation of the oil company and hinder the operation transition processes.

What the model shows is applicable not only to oil and gas companies during the operation transition, but also to other high-risk organizations under normal operation. More and more people are connected to the Internet and even without an operation transition; the companies are facing changing environments and increasing threat. If the company’s data shows a nice picture of few incidents and low risk, it could be that the company has managed its information security risk very well and that it is resilient to threats. However, it could also be that people are not aware of the incidents happening, or they are not reporting the incidents. More detailed analysis of the situation is needed before jumping to a quick conclusion; an audit program for information security would be worthwhile to investigate the real picture of information security risks.

10. References

[1]. Richardson. R, (2009). 2008 CSI Computer Crime & Security Survey

[2]. (2001). Issues and Trends: 2000 CSI/FBI Computer Crime and Security Survey, Comupter Security Institution.

[3]. (2005). Integrated Work Processes: Future work processes on the Norwegian Continental Shelf, Norwegian oil industry association (OLF).

[4]. (2007). CERT Research Annual Report 2007. R. Linger, Software Engineering Institute Carnegie Mellon.

[5]. Allen, J. (2005). Governing for Enterprise Security, Software Engineering Institute: 66.

[6]. Caralli, R. A. and W. R. Wilson (2004). The Challenges of Security Management, Software Engineering Institute, Carnegie Mellon University.

[7]. Dhillon, G. (1999). "Managing and Controlling Computer Misuse." Information Management & Computer Security 7(4): 171-175.

[8]. Gonzalez, J. J., Y. Qian, et al. (2005). "Helping Prevent Information Security Risks in the Transition to Integrated Operations." Telektronikk: 29-37.

[9]. Johnsen, S. (2008). "Mitigating Accidents in Oil and Gas Production Facilities." International Federation for Information Processing 290(Critical Infrastructure Protection II): 157-170.

[10]. Johnsen, S., et al. (2009). Enhancing the Safety, Security and Resilience of ICT and SCADA Systems Using Action Research. International Federation for Information Processing (Critical Infrastructure Protection III): 113-123.

[11]. Loch, K. D., et al. (1992). "Threats to Information Systems: Today's Reality, Yesterday's Understanding." MIS Quarterly 16(2): 173-186.

[12]. Perrow, C. (1999). Normal accidents: living with high risk technologies. Princeton, NJ, Princeton University Press.

[13]. Qian, Y. and J. J. Gonzalez (2006). Adapting Group Model Building Methods to Improve Information Security Data. 24th International Conference of the System Dynamics Society, Nijmegen, The Netherlands, Wiley InterScience.

[14]. Qian, Y., J. J. Gonzalez, et al. (2005). Defining Complex Problems Using Group Model Building and System Archetypes. The Multi-Conference on the Application of System Dynamics and the Disciplines of Management, Shanghai, China.

[15]. Rich, E. and J. J. Gonzalez (2006). Maintaining Security and Safety in High-threat E-operations Transitions. The 39th Hawaii International Conference on System Sciences, Hawaii, U.S.A.

[16]. Rich, E., F. O. Sveen, et al. (2007). Emergent Vulnerability in Integrated Operations: A Proactive Simulation Study of Risk and Organizational Learning. The 40th Hawaii International Conference on System Sciences, Hawaii, U.S.A.

[17]. Ryan, J. J. C. H. (2004). "Information security tools and practices: what works?" Computers, IEEE Transactions on 53(8): 1060-1063.

[18]. Straub, D. W., S. Goodman, et al. (2008). Framing the information security process in modern society. Information Security: Policy, Processes, and Practices. D. W. Straub, S. Goodman and R. L. Baskerville. London, M.E.Sharpe.

[19]. Sveen, F. O., Y. Qian, et al. (2006). A Dynamic Approach to Vulnerability and Risk Analysis of the Transition to eOperations. The 24th International Conference of the System Dynamics Society, Nijmegen, The Netherlands.

[20]. West-Brown, M. J., D. Stikvoort, et al. (2003). Handbook for Computer Security Incident Response Teams (CSIRTs), Software Engineering Institute Carnegie Mellon.