Managing Information Security Risks during New Technology Adoption

YING QIAN, Shanghai University
YULIN FANG*, City University of Hong Kong
JOSE J. GONZALEZ, University of Agder

In the present study, we draw on previous system dynamics research on operational transition and change of vulnerability to investigate the role of incident response capability in controlling the severity of incidents during the adoption of new technology. Towards this end, we build a system dynamics model using the Norwegian Oil and Gas Industry as the context. The Norwegian Oil and Gas Industry has started to adopt new information communication technology to connect its offshore platforms, onshore control centers, and suppliers. In oil companies, the management is generally aware of the increasing risks associated with operational transition; however, to date, investment in incident response capability has not been highly prioritized because of the uncertainty related to risks and the present reactive mental model of security risk management. The model simulation shows that a reactive approach to security risk management might trap the organization into blindness to minor incidents and low incident response capability, which can lead to severe incidents. The system dynamics model can serve as a means to promote proactive investment in incident response capability.

1. INTRODUCTION

For today's organizations, connecting to a complex environment is not a choice, but a necessity in order to survive and thrive. Even businesses such as oil and gas production, where incidents could have major consequences, are moving towards this direction. Intense competition requires organizations to be more effective, often by adopting new or advanced information and communication technologies (ICTs) (Baker and Wallace 2007). The cost to organizations is that more complex technology requires specialized support and resources, and creates a rich environment for breeding vulnerabilities and risks (Allen 2005). The contribution of advanced ICTs is often compromised, because of the unacceptably high levels of security breaches experienced (Dohertya, Anastasakisa, and Fulford 2011).

According to the 2008 Computer Security Institute/Federal Bureau of Investigation (CSI/FBI) Computer Crime and Security Survey, 47% of the 522 respondent firms experienced computer security incidents, such as virus, insider attacks, laptop thefts,

This work is supported by the Research Council of Norway, under Grant 164384/V30 and supported by grants from National Natural Science Foundation of China (project No. 90924030, No. 71103118).

Author's addresses: Y. Qian, Management School, Shanghai University; Y. Fang, Department of Information Systems, City University of Hong Kong; J.J. Gonzalez, Faculty of Engineering and Science, University of Agder, Norway

* Corresponding author's email: ylfang@cityu.edu.hk

denial of service attacks, unauthorized access of data or networks, and bots. The survey also showed that incidents have occurred frequently over the past 12 months, with 47% of the respondents experiencing 1–5 incidents, 14% experiencing 6–10 incidents, and 13% experiencing over 10 incidents. The average financial loss per respondent was USD 288,618. Information security is a major concern of today's firms (Richardson 2009).

However, most organizations view information security control as an overhead and adopt a reactive management approach. Indeed, "actions taken to secure an organization's assets and processes are typically viewed as disaster-preventing rather than payoff-producing" (Dhillon 1999). In simpler terms, the management addresses security concerns only when security incidents occur and are discovered. Note that not all incidents are discovered, some stay latent in the system and become threats to organizations. Several reasons account for the reactive management approach. One is the misperception of information security risks. In the early 1990s, when the use of the Internet began to spread in business organizations, Loch, Carr, and Warkentin (1992) conducted a survey of information systems managers and found that the respondents were aware of the threats, but naively viewed their risks to be low. Another reason is the lack of financial justification, given that investment in information security seeks to prevent an incident from occurring. What would happen and how much it would cost without the investment is hard to predict. Caralli and Wilson (2004) pointed out that "organizations do not routinely require return on investment calculations on information security investments, nor do they attempt to measure or gather metrics on the performance of such investments."

In this paper, we argue that the reactive approach to security risk management could trap enterprises into blindness to minor incidents and low incident response capability, which could finally result in severe incidents. We do so by building a system dynamics model that captures 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 system dynamics model reported in this paper captures how investment in information security is made and subsequently takes its effect on incidents detection and security perception. It extends the existing literature on information security management by modeling the dynamics between incident detection and handling capability and security perceptions. This study also makes a practical contribution in that the simulation of the model provides a means for management to observe misperception and underinvestment, thus effectively illustrating the need for promoting proactive effort in building incident detection capability.

The remainder of this paper is organized as follows: the research context and research design are reported in Section 2; and the system dynamics (SD) model is presented in Section 3. In Section 4, we use the SD model to compare the proactive security risk management approach with the reactive approach; and we discuss our findings in Section 5.

2. RESEARCH METHOD

To build a system dynamics model, we chose the recent transition to Integrated Operations (IO) of the Norwegian Oil and Gas industry as the empirical context for model building.

2.1 Research context—Transition to Integrated Operations

The Norwegian Oil and Gas Industry is transitioning into 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 (Integrated Work Processes: Future work processes on the Norwegian Continental Shelf 2005). Such a transition requires operating companies to adopt new ICT solutions, including collaborative videoconferencing, remote control of hardware, and real-time decision support to link different actors (e.g., onshore operators, offshore operators, suppliers, external experts, among others) through high-capacity computer networks (On the petroleum activity (Om Petroleumsvirksomheten) 2004).

Profound changes are expected to take place. In traditional operation, an offshore platform is essentially a closed system, such that all skilled resources need to be on-platform at significant cost and some risk to personal safety. In the IO paradigm, onshore centers normally closely collaborate with offshore personnel through ICT solutions that share real-time data and provide real-time collaboration facilities. Comparison of the characteristics of traditional operation and Integrated Operations are listed in Table 1.

Table 1 Characteristics of traditional operation and Integrated Operations

	Traditional Operations	Integrated Operations
Operation decision	Daily operational decisions are made offshore with limited onshore support;	Decisions are made together by operators on/offshore and consultants at vendors' onshore expert centers; Several work processes and decisions are automated
Operation plan	Plans are made and changed fragmentally and at fixed times;	Operation plan could be changed when necessary with support from onshore experts and vendors;
IT solutions	IT solutions are specialized and silo-focused;	IT solutions are standardized and the vendors deliver their services digitally (i.e., over "the net");

During implementation of IO, there is a need to integrate ICTs and the supervisory control and data acquisition (SCADA) systems (Qian et al. 2009). SCADA systems are globally accepted as a means of real-time monitoring and control of electric power systems. Currently, operators onshore monitor the operation offshore remotely. In cases of emergence, operators onshore could activate ESD (Emergency Shut-Down) system or PSD (Process Shut-Down) system remotely. There has been a vision on changing from today's manned platforms towards future's unmanned platforms. The technology for remote control and remote operation is already present. But how to utilize the technology on

platforms in a safe and secure way still needs further research.

Operational transition is expected to increase production by 5%–10% and reduce operational cost by 20%–30%. Based on estimates, the net present value of IO on the Norwegian Continental Shelf (NCS) is approximately NOK 300 billion (approx. USD 50 billion) (Integrated Work Processes: Future work processes on the Norwegian Continental Shelf 2005). However, despite the huge financial benefits of IO, operational transition is filled with challenges, including the major challenge of increased information security risks.

From a technological aspect, the prevalence of standard PC hardware and commercial off-the-shelf software, in combination with the availability of remote control technology, has created a new opening through which malware can infect (and ultimately control) a system. The increased interconnections between SCADA and office networks create more points where the combined network may fail or be exploited by outsiders and other external attackers.

From a human aspect, change is a difficult and painful process. When advanced technology is set in place and new work processes are implemented, people need time and effort to familiarize themselves with the new system. Unfamiliarity is one reason for human error (Straub, Goodman, and Baskerville 2008). The new operation is based on effective communication and collaboration via a virtual environment which is completely different from the traditional operation. Thus, learning to communicate effectively in a computer network is a challenge for most operators. In addition, those who are moved from offshore to onshore must learn new skills necessary to perform their new tasks.

From an organizational aspect, new work assignments and new work locations can disrupt the social structures and their associated "know-who" networks in a company. Rebuilding such structures takes time. Above all, the company is moving into an uncharted territory where no prior experience and precedent exists. What to do, how to do it, and when to do it are the questions that must be carefully considered.

Compared with the traditional operation, Integrated Operations generates much higher information security risks. For example, an unintended incident from an insider could occur if an onshore operator – believing that the system is in test mode – inadvertently closes valves, thus causing down-time. An unintended incident from an outsider could occur if a contractor – connecting to the intranet to do maintenance work –inadvertently introduces malware from his PC to the intranet. Such incidents could be also intended if the outsider agrees to act as "Trojan Horse" for malicious agents. An intended incident could be a planned cyber attack, exploiting offshore operation via internet connection (Sveen et al. 2006).

The Norwegian Oil and Gas Industry is generally aware of the high information security risks underlying operational transition. To address these, they used several oil platforms as pilots for operational transition, one of which is the model building focus of the current study.

2.2 Research design—Group model-building workshops

Minimal data can be referred to for the current study because IO is a new operational method, and as such, no historical data is available for reference. We decided to use group

model-building workshops to elicit data (both qualitative and quantitative) from the client (Andersen and Richardson 1997; Richardson, Andersen, and Luna-Reyes 2005; Vennix 1999; Andersen et al. 2007). Two group model-building workshops were held. The purpose of the first workshop was to develop an in-depth understanding of the case and articulate the problem associated with incident response capability. The purpose of the second workshop was to collect specific data for model formulation. The details of the two group model-building workshop were reported in the papers (Qian, Gonzalez, and Sveen 2005; Qian and Gonzalez 2006).

Seven people attended the first group model-building workshop, including the leader of the operational transition project, who is also a specialist in incident response management, information security experts and etc. Twelve people participated in the second group model-building workshop. Aside from those who attended the first workshop, the newcomers included the Chief Information Security Officer (CISO), the platform chief, and managers from the ICT department.

In the first group model-building workshop, the participants provided us with detailed information on operational transition regarding the transition plans, benefits, and concerns, among others. The participants identified more than 40 stakeholders, among whom the most interested and influential ones were the incident response team, the control room manager and the operator, the operator in the onshore support center, and the CISO. In another exercise, the participants listed nearly 40 variables and identified their behaviors over time, including new work processes, new knowledge, knowledge gaps, number of incidents, and average severity of incidents, among others. The key model variables were based on the information provided in this exercise, and the behavior patterns supplied by the participants served as the reference modes for model development. Some variables listed by participants were of little relevance to this project and were not used in our model.

Furthermore, the participants suggested more than 30 policies, such as creating a formal incident response team, monitoring/measuring risk change, improving incident reporting, and observing annual awareness champion measures on security practices. These policies pointed out the possible policy scenarios for our model. We identified that some of the policies are related to a proactive investment in incident response capability, such as creating a formal incident response team, training for information security. In this paper, we explore how proactive and reactive investment in incident response capability could affect the severity of incident and incidents cost. Other policies will be discussed in forthcoming papers using different models.

Eleven hypotheses about the operation transition and the risk change in operation transition were identified during the second group model building workshop with clients. These hypotheses form the basis for the SD model development. These eleven hypotheses were presented in (Rich and Gonzalez 2006) and illustrated with conceptual models and explanations. Here we summarize them in Table 1.

Table 2 - 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

Our prior research has built a system dynamics model mostly based on hypotheses 1 and 4. This modeling effort looked for ways to reduce the vulnerability of the system so that threats are less likely to penetrate the system and become incidents. The model and behavior analysis were reported in (Rich et al. 2009; Sveen et al. 2006).

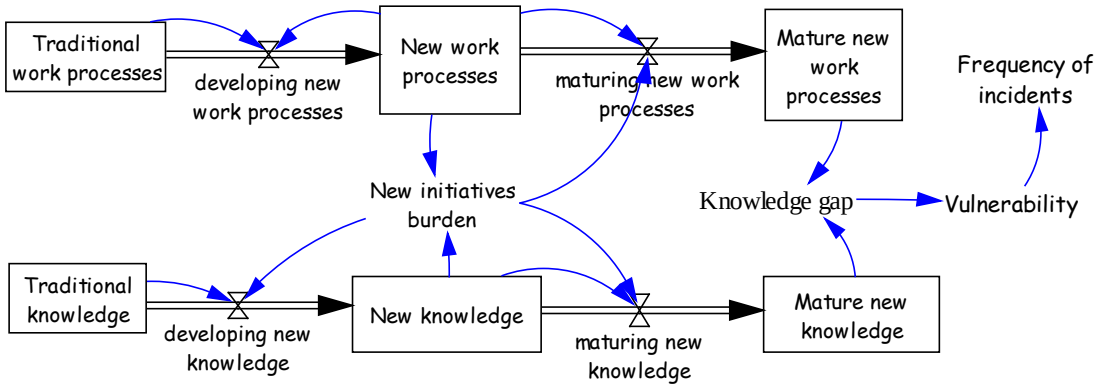

Fig. 1 Model focus on vulnerability

NB: Variables with boxes are stock variables which represent the level of the variable at each time step. Variables under the valve are flow variables which bring things into, or out of a stock. They are the changing speed of the stock variables. Variables with no boxes or valves are auxiliary variables. They are affected by the variables whose arrow head are pointing to them.

Fig. 1 presents the simplified structure of the SD model. 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***, thus ***frequency of incidents*** (H1). The practice of the ***new work processes*** in collaborative workplaces makes new work processes and knowledge mature and will close the gap between them. Change is difficult; ***new work processes*** and ***new knowledge*** are burden to people, which is represented by the variable ***new initiatives burden*** in the model. Meanwhile, the ***new initiatives burden*** traps the operation transition (H4), slowing down the maturation of ***new work processes*** and ***new knowledge***. 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.

Earlier research predominantly focused on addressing information security risk by

examining the vulnerability of the firm. However, two approaches are generally used in managing information security risks (Ryan 2004). One is to reduce the likelihood of occurrence by reducing the vulnerability of the system. Faced with external threats, a system with low vulnerability can better prevent incidents from happening. The other approach is to reduce the potential impact of incident, i.e. to ensure that the organization can handle the consequence of a realized risk through investment in the incident response capability.

During operational transition, policies related to the transition, such as adjusting the transition speed and enhancing knowledge maturation, can affect the vulnerability of the system and information security. However, the link establishing that incident response capability can reduce the severity of incidents has not been considered. Adding a feedback loop of incident response capability-building and understanding its influence on the severity of incidents can complete the information security risk management picture.

3. MODEL OF INCIDENT RESPONSE CAPABILITY

3.1 Theory of incident response capability

One of the main findings of the group model-building workshop is a theory about the incident response capability, mostly related the hypothesis 6 "detection capacity reduces damage" and hypothesis 7 "misperceptions of risk create detection traps". This theory is conceptualized in Fig. 3. Investment in incident response capability leads to better detection of incidents. As more incidents are detected, perceived information security risk rises, resulting in more investment in incident response capability. Such reinforcing feedback loop can cause overinvestment in incident response capability. However, the more serious problem would be a situation where the reinforcing loop operates in the opposite direction—low investment in incident response capability leads to less detection of incidents. People may misperceive the system to be secure and safe, which, in turn, leads to less investment in incident response capability. The latent incidents in the system may actually lead to severe incidents with low incident response capability to control them. This whole dynamics of incident responses capability is the focus of our model-building effort.

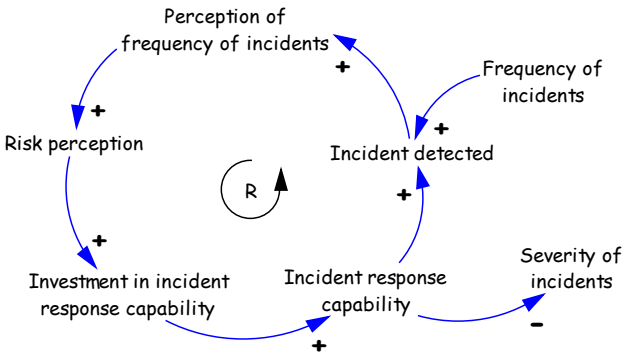

Fig. 2 Reinforcing loop on investment in incident response capability

3.2 Formal Modeling of Incident Response Capability

Based on the dynamic hypothesis, a system dynamics model was developed to address

incident response capability. The SD model is presented in Fig. 3.

The lower part of Fig. 3 focuses on the change in incident response capability. The increase in incident response capability is mainly due to the investment of the management, which is based on the desired incident response capability. Management makes investments to adjust the incident response capability to the desired level. Building incident response capability takes time. If the investment is for adding more human resources to the incident response team to increase incident response capability, announcing openings for the roles, interviewing candidates, and signing contracts take time. If the investment is for improving the knowledge level of the current incident response team, identifying the proper training program, signing the contract for the program, and conducting the training session/s also take time. Normally, the delay in building incident response capability is approximately three months. If the desired incident response capability level is lower than the actual incident response capability, no adjustment is made. Incident response capability becomes obsolete over time. New threats, such as new attack tools, new vulnerabilities, and new viruses, emerge in the field of information security. We assume that the incident response capability obsoletes after two years. Learning from incidents can increase such capability.

The desired incident response capability is based on the perception of the frequency of incidents. The upper part of Fig. 3 focuses on the perception of the frequency of incidents. Not every incident is detected; a fraction always goes unnoticed. How large this fraction is depends on the adequacy of the incident response capability. When the number of detected incidents increases, the management perceives that more incidents are occurring and that the information security risk is high. Therefore, a desire to have more incident response capability to handle all these incidents will arise. Change in the management's risk perception occurs over time. Incidents occur because of various exogenous factors. When managers first encounter an increasing number of incidents, they perceive these as random occurrences. However, when they repeatedly encounter more incidents, they will perceive high information security risk.

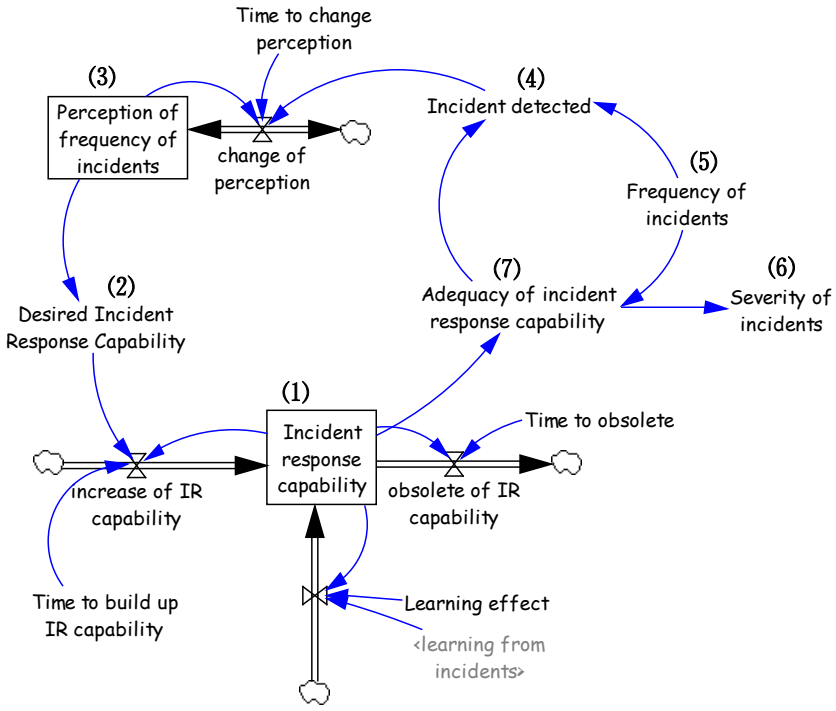

Fig. 3 Model of incident response capability

3.3 Key variables definition and parameter values

Fig. 3 presents the system dynamics model on incident response capability. The definitions of the model variables, how they are measured, and how we set values to the model constants are discussed below.

Incident response capability (1) is a capability set up for the purpose of providing assistance in responding to computer security-related incidents (NIST 2006). This variable measures how many incidents can be handled per month (unit: incident/month). This variable includes two aspects: one refers to how many resources (people × time) are devoted to the work, and the other refers to how productive these resources are (incident/people). A decision to increase incident response capability could be to add more resources to the work or to improve the productivity of existing resources (e.g., by implementing information security technology such as personal firewalls, host-based intrusion detection and prevention systems, workstation access control software, file integrity checkers, and patch management systems; or by training programs to raise the productivity of the incident response team). In the current version of the model, we do not disaggregate these two aspects. Incident response capability increases as investment in it is made and learning from incidents occurs, whereas it becomes obsolete over time.

$$\text{Incident response capability} = \int (\text{increase of IR capability} - \text{obsolete of IR capability} + \text{learning from incidents} * \text{Learning effect} * (1 - \text{Incident response capability})) \quad [1]$$

$$\text{increase of IR capability} = (\text{Desired Incident Response Capability} - \text{Incident response capability}) / \text{Time to build up IR capability} \quad [2]$$

$$\text{obsolete of IR capability} = \text{Incident response capability} / \text{Time to obsolete} \quad [3]$$

The ***desired incident response capability*** (2) is the level of incident response capability that management deems necessary, i.e. able to handle all the incidents properly. Therefore, this variable measures how many incidents need to be handled per month (unit: incident/month), which equals to the ***perception of frequency of incident*** (3). If the ***incident response capability*** is lower than the desired level, an investment is made to ***increase incident response capability***.

The ***perception of frequency of incidents*** (3) means that in management's view, the number of incidents that occur in a month (unit: incident/month) and it is based on the ***incident detected*** (4), which measures how many incidents are detected in a month (unit: incident/month). The ***Perception of frequency of incidents*** is normally smaller than the number of incidents that actually occur as, usually, not all incidents are detected. The ***incident detected*** (4) is affected by the actual number of incidents that occur i.e. the ***frequency of incidents*** (5) and the capability to detect them, the ***adequacy of incident response capability*** (7).

The ***adequacy of incident response capability*** (7) is measured by comparing the ***incident response capability*** (the number of incidents that can be handled) to the actual ***frequency of incidents*** (the number of incidents that occur). This dimensionless variable ranges from 0 to 1.

Desired Incident Response Capability = Perception of frequency of incidents [4]

Incident detected = Frequency of incidents × f(Adequacy of IR capability) [5]

0.1<=f(Adequacy of IR capability)<=1, f'>=0, f"=<0 [6]

Adequacy of incident response capability = Incident response capability / Frequency of incidents [7]

The ***severity of incidents*** (6) represents the average consequence of incidents, i.e., how much total financial loss is incurred per incident, which is measured in Norwegian Krone (unit: NOK/incident). This variable is mostly affected by the ***adequacy of incident response capability***.

Severity of incidents =Normal severity of incidents*f(adequacy IR capability on severity of incidents) [8]

0.5< f(adequacy IR capability on severity of incidents)<5, f'>=0, f"=<0 [9]

The management goal is to prevent severe incidents from happening. Minor incidents are tolerable. According to the severity of incident, the management has divided incidents into 5 levels: level 1, minor incidents: less than 10K NOK/incident; level 2, serious incidents, between 10K NOK/incident and 100K NOK/incident; level 3: dangerous incidents, between 100K NOK/incident and 2M NOK/incident; level 4: Critical, between 2M NOK/incident and 20M NOK/incident; Level 5: disaster incidents, above 20M NOK/incident. According to the management of the platform, incidents in level 4 and 5 must be prevented. Actions will be taken to improve the system to reduce incidents above level 3. Incidents in level 1 and 2 will be fixed but not necessary in need of actions to improve the system.

During further model development and formalization, we had several discussions with

our client about the parameters and their values. In Table 3, we list the constants used in the model, together with their definition, value, unit, and validity (how they were obtained).

Table 3 List of model constants

Parameter	Definition	Value (unit)	Validity
Time to change perception	Time required to change the perception of how frequent incidents happen	3 month	Suggested by client, experts
Time to obsolete	Time required for incident response capability to become obsolete	12 month	Suggested by client, experts
Time to build up IR capability	Time required for to build up incident response capability	3 month	Suggested by client, experts
Initial incident response capability	Incident response capability at the beginning of the operation transition	0.1 incident/month	Suggested by client, experts
Initial perception of frequency of incidents	Management's perception of how frequently incidents happen at the beginning of the operation transition	0.125 incident/month	Suggested by client, experts

4. MODEL SCENARIO ANALYSIS

This model of incident response capability is linked to the model of operational transition (focusing on work processes, knowledge, and vulnerability), completing the model of information security issue during operational transition. The full model went through the standard model validation tests, including direct structure and structure-oriented behavior tests (Barlas 1996; Barlas and Kanar 2000). Due to lack of historical data, we were unable to conduct a behavior test, which requires comparison of the model-generated behavior with historical data using statistical tools to assess the point-by-point fit. Alternatively, we interviewed experts in information security management showing model behavior in different scenarios. Their recognition of the model behavior added confidence to our model.

From the group model-building workshops, it is well acknowledged that changing the platform from a closed, self-sustain system into a connected system means more information security threats to the platform. However, little has been done to cope with such increasing threats. The investment in incident response capability will not be made until the management see an growing number of incidents really happen. Therefore, we use this model to investigate two different scenarios: (1) reactive information security management—invest in incident response capability when seeing more incidents occur, and (2) proactive information security management—invest in incident response capability before major changes, such as operational transition. Only one parameter is changed: the initial incident response capability. In traditional operation, the incident response capability is quite low because there are few information security incidents. The incident response capability prepares for approximately one incident per year, which is equal to approximately 0.1 incident/month. In the first scenario (the reactive approach), management keeps the incident response capability level despite its concern on increasing information security risks. In the second scenario (the proactive approach), management raises the incident response capability to 0.3 incident/month before operational transition

starts. In IO, the incident response capability prepares for at least three incidents a year. In this scenario, we first use 0.3/month, which is three times the original incident response capability. Different parameters can be tested using the system dynamics model. In reality, however, even when being proactive, management will not raise the incident response capability very high considering the limited resources available to the organization.

Table 4 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 following figures. The blue line (1) represents the reactive scenario and the red line (2) represents the proactive scenario.

The implementation of new work processes is scheduled as 5 new work processes the first year and 2 new work processes each year after. The maturation of new work processes takes around 4 months. The new knowledge is introduced together with the mature new work processes, while it takes even longer time (8 months) to mature. For detailed explanation of these figures, please refer to (Rich et al. 2009). The change of initial incident response capability does not influence operational transition. As a result, the behavior of mature new work processes and mature new knowledge (Fig. 4) is the same for the two scenarios.

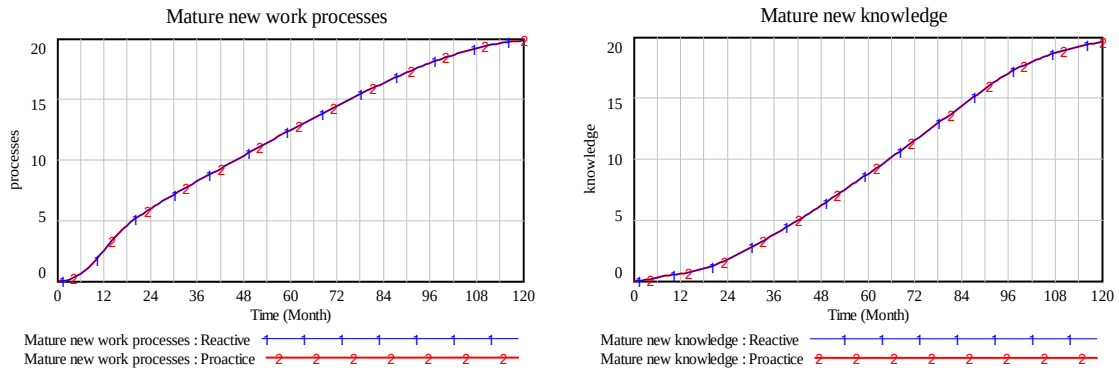

Fig. 4 Mature new work processes vs. mature new knowledge

The vulnerability of the system, so-called vulnerability index in the model, is affected by new work processes, new knowledge, and knowledge gap. The vulnerability index peaks at the end of the first year when 5 new work processes are introduced. It slowly reduced as people learn to work with the new work processes. For detailed explanation of these figures, please refer to (Rich et al. 2009). Given that new work processes and new knowledge are the same for these two scenarios, this leads to identical model behavior of vulnerability index. In addition, given the same information on security threats, the vulnerability index is the only factor that influences the frequency of incidents. As a result, the frequency of incidents remains unchanged for the two scenarios (Fig. 5).

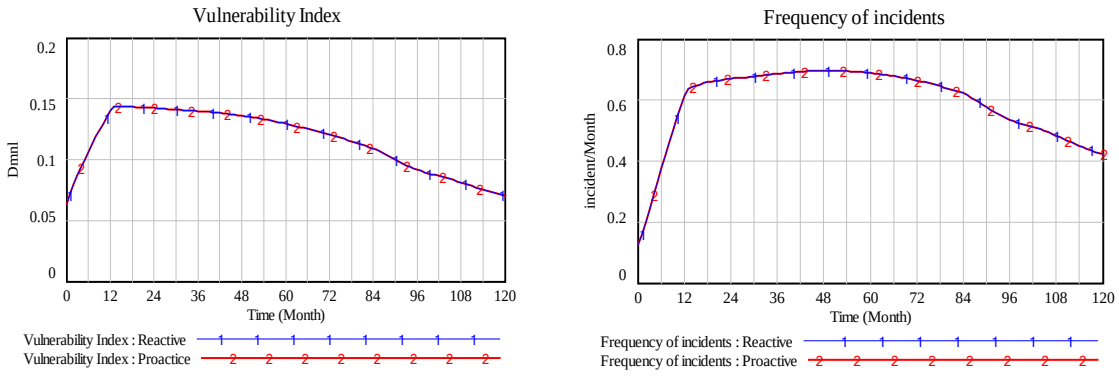

Fig. 5 Vulnerability index vs. Frequency of incidents

The average severity of incidents at the start of the IO is around 0.6M NOK/incident, calculated by the data supplied by the platform. If more incidents happen, without more incident response capability, the severity of incidents will increase. Under the same amount of incidents, more incident response capability will lead to reduced severity of incidents, as incidents are handled more timely and in better ways. With the simulation, we can see that as the operation transition continues, in reactive scenario, the severity of incidents sharply increase to around 1.4M NOK/incident (more than doubled compare to the initial severity of incidents) and then gradually decreases to an equilibrium level at around month 60. In the proactive scenario, the severity of incidents peaks at about 0.9M NOK/incident, approximately 56% reduction from the reactive scenario (Fig. 6). In the reactive scenario, the incident severity approaches a critical level, which the management is keen to prevent incident over 2M NOK/incident. For the proactive scenario, the severity of incidents remains at moderately dangerous level (100K-2M NOK).

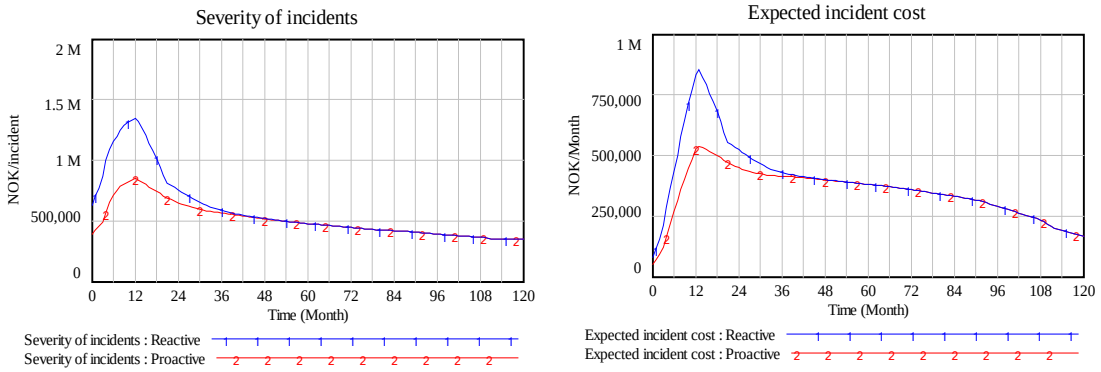

Fig. 6 Severity of incidents vs. Expected incident cost

The expected incident cost refers to the product of frequency of incidents and severity of incidents. Frequency of incidents is the same for the two scenarios. The severity of incidents is lower in the proactive scenario. As a result, the expected incident cost peaks approximately 56% lower in the proactive scenario than in the reactive scenario. The great difference in severity of incident is caused by the incident response capability in Fig. 7.

In the reactive scenario, the incident response capability starts from 0.1 incident/month (Fig. 7). As operational transition starts, the frequency of incidents

increases sharply in the first year as new work processes and knowledge are implemented and a knowledge gap is generated. However, the incident response capability increases much more slowly than the increase of frequency of incidents (Fig. 5). The incident response capability is quite inadequate to handle all the incidents happening. In the proactive scenario, the incident response capability starts from 0.3 incident/month. It decreased a little bit at the beginning when only small part of new technology is implemented and frequency of incidents has not increased to so high. When the frequency of incident quickly increases later on, the incident response capability also increases quickly.

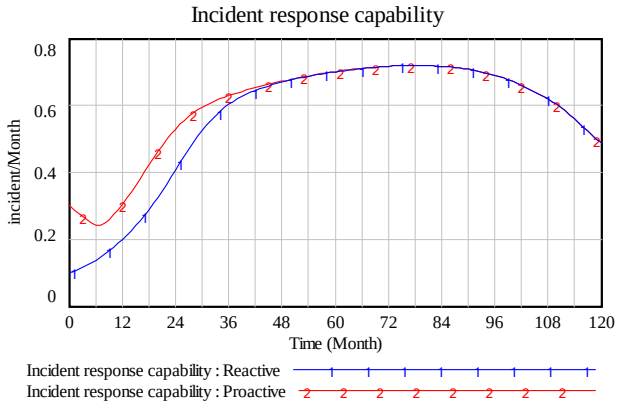

Fig. 7 Incident response capability

Why couldn't incident response capability increase to the level of frequency of incidents immediately? First, it is due to the delays in the system. Time is needed for management to perceive the increase of incidents. In our model, there is a three-month delay before the perception of frequency of incidents changes because incident data are reported and reviewed quarterly. Time delay also exists in building incident response capability, as we explained earlier.

Moreover, there exists another reason for the slow development of incident response capability in the reactive scenario, which can be explained by Fig. 8. With low incident response capability (grey line with +), a large fraction of incidents is not detected. Given that the detected incidents (red line with *) are the only ones that can be reported, management's perception of frequency of incidents (green line with x) is much lower than the actual frequency of incidents (blue line with #); The low perception of frequency of incidents leads to low desired incident response capability and thus, underinvestment in incident response capability. After several years of slow development, the detected incidents gradually approach the frequency of incidents. The huge gap between incident response capability and frequency of incidents around month 12 results in high severity of incidents.

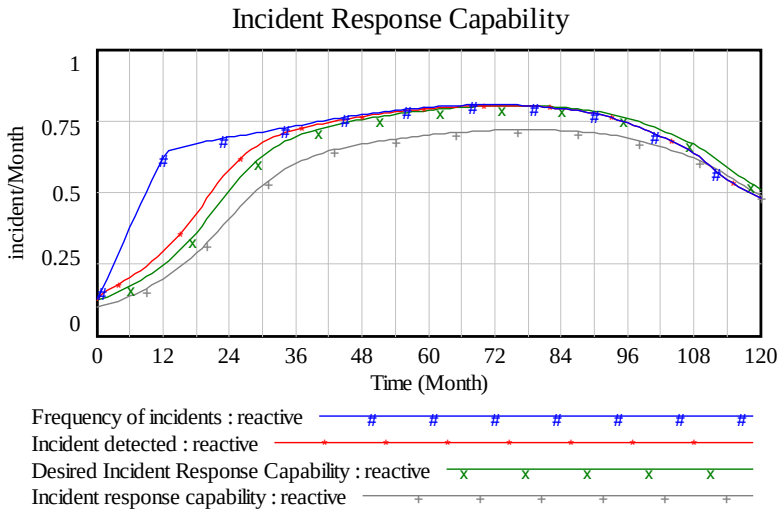

Fig. 8 Related variables of the development of IR capability

Severe incidents on an oil platform may have a huge impact, ultimately threatening human life and the environment. Management of companies in the oil and gas industry is keen to avoid severe incidents. The simulation result shows that reactive thinking can result in an incident response capability trap, which could then lead to critical incidents during operational transition.

With proactive thinking, the incident response capability starts higher and a larger portion of the incidents can be detected. The desired incident response capability can also be higher, which leads to less underinvestment. Therefore, the severity of incidents is largely reduced in the proactive scenario (Fig. 6).

5. CONCLUSION AND DISCUSSION

This paper builds upon and adds to prior research by formulating/constructing a SD model of incident response capability during operational transition. The model simulation results demonstrate how proactive and reactive thinking in information security risk management can generate different risk scenarios over time.

5.1 Implications to information security research

The idea of information security surfaced with the development of early computers in the 1960s. Since computer was a product of advanced technology, computer security naturally came down to technology measures. With the fast growth of personal computer and the widespread of internet, human factors become an imminent issue in information security. A large portion of the computer and internet users have limited knowledge about computer and internet and even less knowledge about information security (Arce 2003; Werlinger, Hawkey, and Beznosov 2009; Yildirima et al. 2011; Dohertya, Anastasakisa, and Fulfordb 2009). Lately, researchers in information security started to look into the organizational factors too. For example, Werlinger et al. pointed out many organizational factors that weaken security. “Tight schedules may result in human errors that could make the organization more vulnerable” (Werlinger, Hawkey, and Beznosov 2009). There are emerging calls for an integrated view of information security, from the technological,

human, and organizational aspects, sometimes referred as MTO (Man, Technology, and Organization). However, methods to tackle the MTO issues in information security are scarce. One of the research focuses is the development of information security checklist and standards aiming to capture the best practice. Another research focuses is risk assessment identifying the threats and vulnerabilities, and then determining the likelihood and impact for each risk. Risk assessment could either be qualitative, categorizing low, medium and high risks, or be quantitative, calculating the value of "Annualized Loss Expectancy", which is similar to the "expected incident cost" in our model. However, static risk assessment method is less relevant for the case of this study, where the organization is going through operation transition, which is a complex, long-term, and dynamic process with feedback, delays, and trade-offs, among others. The risk picture will change along the way. It is necessary to consider how the transition affects the information security risks. Except the work from our research group, such as (Qian, Gonzalez, and Sveen 2005; Qian and Gonzalez 2006; Sveen et al. 2006; Rich and Gonzalez 2006; Rich et al. 2009), we found few previous research investigating information security risks during the operation transition. The previous research considered the technology aspect—more threats with integrated operation, and the human aspect—more human errors when operators do not have enough knowledge and are burdened by operation transition. This paper extends the previous research by adding the organization aspect—management's mental model on investment in information security. The model simulation results show that management's reactive mental model might lead to severe incidents while the proactive investment in information security helps reduce the severity of incidents. Analysis shows that not only delays in the system prevent incident response capability from catching up the desired level slowly, but more importantly, the reactive mental model could cause misperception of information security risks which leads to under-investment in incident response capability and the inadequate incident response capability could result in severe incidents.

5.2 Contribution to information security practice

Though information security has become one of the major concerns of today's firms (Richardson 2009), proactive investment in information security is difficult to "sell.". A paradox exists in information security management. If investment is made proactively, the frequency of incidents and severity of incidents will be reduced, leading low perception of risk and makes it difficult to justify the investment on information security management, just as the old saying goes: "Nobody Ever Gets Credit for Fixing Problems that Never Happened."

In this highly competitive world, companies try to cut any cost that might be unnecessary. Therefore, it is seldom that management are proactive in practice. The platform under study is one case of the many. A recent study of Stig shows that risk awareness of the offshore oil installation is poor (Johnsen 2009). "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 incident response capability, which is a dangerous situation.

System dynamics provides a foundation for developing theories and tools that help

management understand, characterize, and communicate that investment in information security is essential. Such a system dynamics model could be used as a learning environment for the management to raise their awareness of the potential information security risks that they are facing. Even when company data show a nice picture of few incidents and low risks, it is not necessary that information security risk has been very well managed and the company is resilient to threats. There is possibility that people are unaware of the incidents, or are not reporting these incidents.

As a result, corporate should regularly check and analyze its information security risks. Internal audit or external audit program could be one way to evaluate information security risks. As suggested by Yildirim et al. (2011) "The only way of answering critical questions, for information security is to test the security of the information entities (human factor, software, hardware, media, etc.), through 'penetration tests'."

5.3 Future Research Directions

The current model is at a highly aggregated level; however, disaggregating it to include more details about work processes and knowledge would be possible. In addition, some work processes can have a large impact on information security, bringing higher vulnerability into the system. At the same time, the severity of incidents and frequency of incidents are both highly aggregated in that they are the average for all kinds of incidents. The platform has developed a risk matrix that presents the frequency and severity of various kinds of incidents. Incorporating the risk matrix into our model and disaggregating the average frequency and severity of incidents using the data in the risk matrix are possible. By doing so, we would be able to see the development trend of each type of incidents as operational transition affects various types of incidents differently. For example, the change of one work process can have a major impact on the frequency of human errors, but it may not have such an impact on the frequency of terrorist attacks. With sufficient data, the disaggregated model could be used to generate dynamic risk matrix, which is able to show how the risk matrix changes over time.

REFERENCES

Allen, Julia. 2005. Governing for Enterprise Security: Software Engineering Institute.

Andersen, David, and George Richardson. 1997. Scripts for group model building. *System Dynamics Review* 13 (2):107-129.

Andersen, David., Jac. A. M. Vennix, Goerge Richardson, and Etienne A. J. A. Rouwette. 2007. Group Model Building: Problem Structuring, Policy Simulation and Decision Support. *Journal of Operational Research Society* 58 (5):691-694.

Arce, Iván. 2003. The weakest link revisited. *Security & Privacy, IEEE* 1 (2):72-76.

Baker, Wade H., and Linda Wallace. 2007. Is Information Security Under Control?: Investigating Quality in Information Security Management. *Security & Privacy, IEEE* 5 (1):36-44.

Barlas, Yaman. 1996. Formal Aspects of Model Validity and Validation in System Dynamics. *System Dynamics Review* 12 (3):1-28.

Barlas, Yaman, and Korhan Kanar. 2000. Structure-Oriented Behavior Tests in Model Validation. Paper read at 18th International Conference of the System Dynamics Society, August 6-10, at Bergen, Norway.

Caralli, Richard A., and William R. Wilson. 2004. The Challenges of Security Management: Software Engineering Institute, Carnegie Mellon University.

Dhillon, Gurpreet. 1999. Managing and Controlling Computer Misuse. *Information Management & Computer Security* 7 (4):171-175.

Dohertya, Neil Francis, Leonidas Anastasakisa, and Heather Fulford. 2011. Reinforcing the security of corporate information resources: A critical review of the role of the acceptable use policy. *International Journal of Information Management* 31:201-209.

Dohertya, Neil Francis, Leonidas Anastasakisa, and Heather Fulfordb. 2009. The information security policy unpacked: A critical study of the content of university policies. *International Journal of Information Management* 29:449-457.

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

Loch, Karen D., Houston H. Carr, and Merrill E. Warkentin. 1992. Threats to Information Systems: Today's Reality, Yesterday's Understanding. *MIS Quarterly* 16 (2):173-186.

NIST. 2006. Glossary of Key Information Security Terms, edited by R. Kissel: National Institute of Standards and Technology.

On the petroleum activity (Om Petroleumsvirksomheten). 2004. Oslo: Norwegian Ministry of Petroleum and Industry (Det Kongelige Olje og Energidepartementet)

Qian, Ying, Yulin Fang, Eliot Rich, Martin Gilje Jaatun, and Stig. O. Johnsen. 2009. Managing emerging information security risks during transitions to Integrated Operations. Paper read at The Hawaii International Conference on System Sciences, at Hawaii, USA.

Qian, Ying, and Jose J. Gonzalez. 2006. Adapting Group Model Building Methods to Improve Information Security Data. Paper read at 24th International Conference of the System Dynamics Society, at Nijmegen, The Netherlands.

Qian, Ying, Jose J. Gonzalez, and Finn Olav Sveen. 2005. Defining Complex Problems Using Group Model Building and System Archetypes. Paper read at The Multi-Conference on the Application of System Dynamics and the Disciplines of Management, at Shanghai, China.

Rich, Eliot, Jose J Gonzalez, Ying Qian, Finn Olav Sveen, Jaziar Radianti, and Stefanie Hillen. 2009. Emergent Vulnerabilities in Integrated Operations: A Proactive Simulation Study of Economic Risk. *International Journal of Critical Infrastructure Protection* 2 (3):110-123.

Rich, Eliot, and Jose J. Gonzalez. 2006. Maintaining Security and Safety in High-threat E-operations Transitions. Paper read at The 39th Hawaii International Conference on System Sciences, at Hawaii, U.S.A.

Richardson, Robert. 2009. 2008 CSI Computer Crime & Security Survey.

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

Straub, D.W., S. Goodman, and R.L. Baskerville. 2008. Framing the information security process in modern society. In *Information Security: Policy, Processes, and Practices*, edited by D. W. Straub, S. Goodman and R. L. Baskerville. London: M.E.Sharpe.

Sveen, Finn Olav, Ying Qian, Stefanie Hillen, Jaziar Radianti, and Jose J. Gonzalez. 2006. A Dynamic Approach to Vulnerability and Risk Analysis of the Transition to eOperations. Paper read at The 24th International Conference of the System Dynamics Society, at Nijmegen.

Vennix, Jac. A. M. 1999. Group model-building: tackling messy problems. *System Dynamics Review* 15 (4):379-401.

Werlinger, Rodrigo, Kirstie Hawkey, and Konstantin Beznosov. 2009. An Integrated View of Human, Organizational, and Technological Challenges of IT Security Management. *Information Management & Computer Security* 17 (1):4 - 19

Yildirima, Ebru Yeniman, Gizem Akalpa, Serpil Aytacb, and Nuran Bayramb. 2011. Factors influencing information security management in small- and-medium-sized enterprises: A case study from Turkey. *International Journal of Information Management* 31:360-365.