Usage Control in Inter-organisational Collaborative Environments – A Case Study from an Industry Perspective

Åsmund Nyre, Martin Jaatun

Usage control in inter-organisational collaborative environements - a case study from an industry perspective

Åsmund Ahlmann Nyre[1] and Martin Gilje Jaatun[2]

[1] Norwegian University of Science and Technology
nyre@idi.ntnu.no
[2] SINTEF ICT
martin.g.jaatun@sintef.no

Abstract. Sharing information between collaborators without relinquishing control of that information has for many years been a tantalizing goal in the research community, but despite application support, the concept of usage control has failed to take hold in the business community. In this paper we present the results of a case study in the Norwegian oil & gas domain. The purpose of the study is to better understand the reasons for the slow adoption rate of usage control technology to control shared information. To this end we investigate risk perception, existing control measures and the attitude towards usage control technology. The study shows that although participants in the case study do not think their information is properly protected, there are several practical challenges that prevent them from adopting usage control technology as a means to improve protection.

1 Introduction

The extensive collaboration across system boundaries facilitated by the Internet is unfortunately also increasing the potential for misuse of shared information. While mechanisms to protect assets from active attackers (such as firewalls, intrusion detection systems and anti-virus software) are commonplace, the availability of commercial software to protect information from misuse remains limited.

From the research community, *usage control* has been proposed as a potential remedy to let businesses retain control of information beyond their systems' boundaries [1]. Since the initial proposition from Park and Sandhu [1], several usage control models have been proposed, with different strategies of enforcement. Some of the models have even been implemented as prototypes and tested for computational overhead [2]. From a researcher's perspective, it seems obvious that usage control would help those that share potentially sensitive information with others. There are even some commercially available products that offer some of the concepts of usage control. Examples in this respect include the

EMC[2] Documentum Information Rights Management client[3], which basically extends the access control policy of the Documentum repository to include all receiving devices. The client verifies in real time that the subject has access to the documents, regardless of whether the document is a copy or not. Similarly, the Microsoft Information Rights Management system for the Office suite integrates with Sharepoint server and offers the same kind of functionality.

However, despite the belief of researchers and the fact that there are commercially available tools to help, the industry seems to be reluctant to adopt usage control technologies. A natural response therefore would be to ask "why"? What is it that makes this seemingly attractive technology not attractive enough? It is exactly this question that formed the basis for our case study.

This paper contributes new knowledge on the perceived usefulness of usage control technology within the oil and gas sector. More specifically, the target of investigation is the vision of *Integrated Operations* of the oil and gas sector, and thus this is the domain where we will elicit requirements for such mechanisms to ease the transition to technology-based enforcement of usage control. To this end, the study will identify the current measures used to control and restrict shared information together with the perceived threats and opportunities provided by usage control enforcement mechanisms.

The remaining parts of this paper is organised as follows: Section 2 provides a brief introduction to the concept of usage control and distributed enforcement. Section 3 gives an overview of the context of the study - Integrated operations in the oil and gas industry. The design of the case study is detailed in Section 4, including procedures on data collection, analysis and measures to mitigate threats to validity. Section 5 presents our analysis and findings from the study, before we give our concluding remarks and possible future directions in Section 6.

2 Usage control

Usage control has been proposed as a means to remedy the information misuse problem by extending common security mechanisms beyond single systems such as PCs, servers or entire corporate systems. The idea is to provide a model for expressing and enforcing restrictions on how the information is to be *used* . Current mechanisms such as access control, Digital Rights Management, confidentiality and privacy protection all attempt to restrict information in one way or the other. The focus of usage control is to create a holistic approach to restricting information, and thus it may be used for any of the purposes listed above.

When introducing usage control Park and Sandhu stressed the notion of a continuous access decision and mutability of attributes as the two most important factors of what they called the UCON$_{ABC}$-model [1]. Later, Pretschener et al. included *obligations* as a fundamental concept of distributed usage control

[3] http://www.emc.com/products/detail/software/information-rights-management.htm

[3]. Unlike the UCON model, the authors define obligations to be concerned with the future, e.g. "data d must not be further distributed" [3]. For the purpose of this study, we focus on the enforcement of usage control policies, particularly with respect to these three central aspects of usage control:

- *Continuity of access decision*: The decision on whether the subject should be granted access to the requested object is not considered a discrete-time event when requesting access to the object. Instead, the access decision is considered to be continuous, so that any context change (e.g. attribute values) may immediately affect the access decision.
- *Mutability of attributes*: The usage decision may alter attribute values of both subject and object. This will allow for frequency limitations on usage, such as "use at most 3 times".
- *Obligations*: Upon granting usage rights to an object, constraints may be imposed on future usage. Examples include having to delete the information within x days, not being able to forward the information, etc.

One of the fundamental questions when identifying users' attitudes towards usage control is how to enforce it? How can the aspects described above be enforced for distributed information? While there are several proposed enforcement models [2] , we focus on the two main strategies of enforcement: *proactive* and *reactive* enforcement [2]. That is, whether enforcement should attempt to prevent misuse of information or merely detect it. The proactive approach is the predominant strategy for current access control mechanisms as well as commercial Digital Rights Management (DRM) systems, and since usage control may be viewed as an extension of both, proactive enforcement is a natural choice. However, unlike common DRM systems, usage control may also be reactive. The analogy to law enforcement is apparent and also companies' use of Non-Disclosure Agreements (NDAs) follow this principle. Hence, the industry is well acquainted with the reactive approach from existing protection measures. Usage control may contribute a more accurate and cost-effective way of detecting violations.

3 Context - Integrated Operations

Integrated Operations is a term used in the oil and gas industry in Norway to denote a future state in which work processes, information and people are integrated across geographical and organizational boundaries. Thus, information can flow without unnecessary obstacles from one organisation to another. This is not to say that everything should be open and accessible to everyone; on the contrary, the vision is that the flow of information is secure and only accessible to authorized personnel.

To reach this state of collaboration is not trivial, especially since the relationships between companies are extremely complex and dynamic. To provide a glimpse of this complexity, we provide a brief overview of the main categories of companies.

1. *Operators* are commonly oil companies and are responsible for the actual production of an oil or gas field. Due to the specialised expertise required for oil field development and production, operators to a large extent use *integrators* and suppliers to perform specified tasks.
2. *Licence owners* are oil companies that own a share of the license to develop an oil field. Commonly licences are shared between several oil companies. Thus both costs, risks and future revenue are divided according to the license share.
3. *Integrators* (sometimes called *contractors*) deliver complete products and services to operators by combining solutions from different *suppliers*.
4. *Suppliers* develop and deliver a specialised product or service for specific tasks, sometimes by incorporating products or services from other suppliers. The distinction between integrators and suppliers is blurred, however the term supplier is used when most of the development effort is done in-house.
5. *Consultancies* or consultancy firms may be used by any of the above-mentioned actors as support for their activities. For example as ICT developers, technical assessments or advisors.

These categories are by no means exhaustive nor mutually exclusive, and therefore there may be companies that do not fit any description, while others fit several. Still, they serve the purpose of illustrating the complex business relations that currently exist in the oil and gas sector. For example oil companies are competing to gain market share, but at the same time they are collaborating to explore and produce oil. There are even circumstances in which the Norwegian government demands cooperation in order to exploit minor oil fields, that would not be profitable if requiring a separate installation. Similarly, there are several companies that interchangeably between projects acts as both suppliers and integrators. Hence, integrators often find themselves in the position that they are dependent on one of their competitors for delivering according to their contract.

> *There are certainly other sectors where situations occasionally occur where you have to collaborate with your competitors, but here, this happens constantly. We both cooperate and compete with them simultaneously.*
>
> *(Engineer from the study)*

In addition to the constant collaboration with competitors, there is also a struggle among the companies to extend their product portfolio to get a bigger slice of the cake. With the amount of money involved in the industry, both oil companies, suppliers and integrators may be looking to increase their share of the operation at the others' expense, making the climate for trust a very fragile one.

4 Case study design

4.1 Research questions

The main goal of this study is to *identify the factors influencing adoption of usage control enforcement mechanisms in collaborative environments.*

1. What are the main perceived threats to shared information?
2. Which measures are currently deployed to protect shared information from misuse?
3. To what extent are the current protection schemes believed to be adequate?
4. What are the main opinions on usage control enforcement technology?

These research questions are inspired by the main principle of the Protection Motivation Theory [4, 5]. That is, the perceived risk and the perceived efficacy of the mitigating measures influence the decision to adopt the mitigating measures, which in our case is usage control technology. However, since we anticipate that there may be existing mechanisms in place, we have also considered the *relative advantage* of usage control technology compared to the existing measures [6]. As the focus of this paper is the case study outcome, we will not elaborate more on theoretical underpinnings of the study. For a more complete discussion of the relations to existing theory on technology adoption, we refer to [7].

4.2 Rationale for case selection

A case selected for a case study is often either a *typical* case or an *extreme* case. With our goal of attempting to understand why companies adopt (or don't adopt) usage control technologies in collaborative environments, we chose the extreme case. The rationale behind this was the idea that companies that extensively share potentially sensitive information are more likely to have a conscious opinion on the risks involved. Hence, we assume that in the extreme cases we are more likely to actually identify factors influencing adoption, than in more moderate settings. Indeed, as described in the previous section, the oil and gas industry in Norway in general (and Integrated Operations in particular) fits this description.

4.3 Data collection procedure

This study has used interviews as the data collection method. Other options we considered were workshops and focus group interviews. However, requiring people to participate at a certain time and place seemed to be a major obstacle to recruiting participants. This, coupled with our worry that group interviews potentially could prevent people from being sincere about their perception of risk, caused us to settle for individual interviews. We followed a semi-structured interview type on four main topics; shared information, risk perception, current security measures and attitude towards usage control enforcement technology. The interview guide given in Appendix A was used both as a starting point of discussion and as a means to ensure that all four topics were addressed.

Six companies, both national and international, within the oil and gas industry in Norway were selected to ensure a good coverage of categories of actors. Table 1 shows the distribution of participants with respect to both company category and the role of the participants in their company. We sought to cover the

Category	Companies	Interviews
Operator	1	3
Licence owner	1*	1*
Integrator	1	3
Suppliers	3	5
Consultancy	1	1
Total	6	12

(a) Number of organisations and interviews per category of actor

Role	Interviews
Engineer	6
Security professional	2
Manager	4

(b) Number of interviews for each participant role

*) The operator was also a licence owner. Hence these numbers are duplicates of the above

Table 1: Distribution of participants with respect to company category and participant role

three different viewpoints from Engineers, Security Professionals and Management. However, it may sometimes be difficult to separate these three, especially for intermediate managers within R&D departments. The interviews were all held during the winter and spring of 2012, nearly half were conducted face-to-face while the rest were done by telephone interview. Although we initially tried to avoid telephone interviews, it turned out to be difficult to schedule multiple interviews on a single day, as would have been required due to travel costs and time.

4.4 Analysis procedure

All interviews were recorded and later transcribed in full. The transcribed interviews were then analyzed and coded using the constant comparison method [8] to extract the collective view on risks, existing measures and attitude towards usage control enforcement. The process of coding and labeling text was assisted by the use of NVivo^{TM}, a software tool for qualitative analysis.

4.5 Validity, bias and limitations of the study

There are several aspects of this study that potentially could have a negative impact on the result. Here we outline the most important ones, and describe our efforts to neutralize the negative effect they would have.

Bias from theory may result in a bias in favour of data supporting the theory on the expense of the data contradicting it [9]. We have therefore refrained from detailing our theoretical framework in advance, in order to reduce the likelihood of theory bias in the interpretation of the results.

Truthfullness of participants' answers may be questioned since the topic of information security by many is regarded as sensitive. There is a chance that

participants restrain themselves from revealing problems or anything that might be bad for their reputation. We have therefore made it clear up front that neither participants nor companies would be identified when publishing results. Additionally, since the interviewer is a security , there is a chance that participants may adapt answers to what they believe the interviewer would like to hear or seek confirmation from the interviewer. We have therefore stressed to participants in advance, that the important part of this study is their subjective beliefs. During the interviews we have also strived to remain as neutral as possible (without appearing uninterested), to any of the statements made by the interviewees.

The generalisability of the case may be limited since, as described in Section 4.2, it is an extreme case of sharing sensitive information. That being said, we argue that the size of the oil and gas industry could still provide a great impact even if only considering internal generalisation [9], i.e. generalization within the setting of the study. Admittedly, generalizing on the basis of a relatively small study is not without danger, which is why we have chosen to interpret most of our findings as *views* rather than *facts*. A larger scale study or survey based on our findings are likely to provide more statistically sound data for generalization.

5 Analysis

In this section we present our findings from the case study on the four main topics addressed; information sharing, risk perception, existing security measures and attitude towards usage control enforcement technology. In order to assess the outcome of this study, we also provide a profile of the interviewed participants.

5.1 Participant profiles

Table 1b provides an overview of the participants according to the roles they currently have in their company. Notice however, that the distinction between the three types of roles are in some cases a bit blurred. For example, within the engineering discipline there are also managers, and hence separating managers from engineers may not be trivial. We have however attempted to distinguish managers as the ones whose primary role is to manage others. The same table also indicates that only two people interviewed were considered security professionals, i.e. where information security was their primary task. That being said, there were several of both the engineers and managers that had prior experience from securing information systems as part of product development.

Participants' experience from the oil and gas industry ranged from 2 to 20 years, with an average of approximately nine years. Further, all participants had at least a bachelor's degree or equivalent, while the majority additionally held master's degrees.

In terms of security awareness, the participants reported they would rate their security awareness in the upper end of the scale. As one of the managers stated *"I am professionally paranoid"*.

5.2 Shared information

The kind of information that is shared among partners within Integrated Operations vary considerably depending on the production phase and the type or category of company. Although the information in itself is perhaps not essential to understand attitudes towards usage control enforcement technology, it does help to understand the risk perception of participants.

For integrators and suppliers the most sensitive information is shared either prior to a project contract or in the planning phase of the project. The most important information shared is information on pricing, offers and technical details required by the operators or partners in the bidding process. Additionally, integrators and suppliers may be required to share technical details and product information in order to integrate their solutions with others.

For operators and license owners, the most sensitive information is shared during the operational phase of the project, whether it is exploration or production of oil fields. Integrators and suppliers will often collect a vast amount of data on the operational status through their systems and transport this information to the operator. Although the data in several cases originates from suppliers and integrators, the data is still considered owned by the operators and is shared with other partners at the operators' discretion. Thus, integrators and suppliers consider it to be information shared by the operators, rather then by them. There is a tremendous amount of real-time data on the status of the operation, such as production volumes, pipeline capacities, disruptions or other events, and status of sensors and actuators and for exploration activities also geological information. Some of which may influence stock prices for oil companies while others may be devastating in terms of company reputation.

5.3 Risk perception

Users' perception of risk is believed to influence their motivation for protecting themselves and therefore constitutes the cornerstone of the Protection Motivation Theory [5]. The idea is that without any risks, there is no need for protection either. In this section we aim to identify the specific risks related to sharing potentially sensitive information with business partners.

Potential impact There are fundamentally four kinds of potential impact from misusing shared information that seem to be causing concern:

- *Reduced competitive power* - Shared information on products and technology may be utilized by competitors to improve their products and technology, and thereby reducing the competitive power of the owner of the information.
- *Reduced market share* - Shared information on pricing, tender details and strategies may be utilised by competitors to adapt their pricing in order to gain an advantage in the bidding process.
- *Reduced reputation in the industry* - Especially suppliers and integrators are concerned with the devastating effect it would have if they were responsible

for leaking information obtained from customers and partners. Operators also see this as a concern, since it could reduce their suppliers willingness to collaborate to solve future problems. The industry is very much built on trust, and thus if the basis for this trust should disappear, the effects could be dramatic.

– *Reduced reputation in general* - Security incidents resulting from lack of control of information could potentially be very damaging to the reputation of a company from the viewpoint of citizens, government and the world at large. This is particularly due to the potential environmental hazard of oil production.

Threat	Threat agents	Threat sources	Potential impact
Industrial espionage	Competitors, Intelligence agencies	Information on products, solutions and technology	Reduced competitive power
Corporate espionage	Competitors, Suppliers, customers	Information on pricing, bidding and strategies	Reduced market share
Economic espionage	Employees, general public	Information on operational situation, production and field development	Reduced reputation
Terrorism and activism	Hackers, environmental activists	Information on incidents, status and business	reputation, production
Unintentional disclosure	Own and partner employees	Any information	Any of the above
Intentional disclosure	Own and partner employees	Any information	Any of the above

Table 2: Identified threats, agents, sources and their potential impact

Table 2 lists the main threats with corresponding threat agents (attackers), threat source and potential impact as seen by the participants. Industrial espionage is the single threat that is mentioned most frequently by the participants. It occurs when companies take advantage of technology or product specific information received directly or indirectly from its competitors. The primary effect is that companies lose their competitive advantage relative to their competitors and thus potentially also their market share. For integrators and suppliers, the degree of severity vary with the kind of information abused. According to one of the participants, even interface descriptions might reveal functionality that can be copied. However, acknowledging the need for open interfaces in a competitive

industry, the effort is placed on preventing descriptions of the inner workings of their products from being misused by their competitor. Some of the participants have even experienced attempts from foreign national intelligence agencies trying to steal sensitive information.

Participants also highlight the threat of corporate espionage, which is not about IPR or theft of new technology, but rather information on bids, pricing and strategies. Thus, for competitors to gain market share they can adapt their product pricing, bid requirements and strategy to their competitors. While on the one hand participants argued the probability of this occurring, they simultaneously argued that this kind of information was treated with the utmost discretion. Even project members in a bidding process did not know the pricing of the products they were to deliver.

Economic espionage is when the actors exploit operational data and other knowledge of the companies to predict future pricing in the stock market. While participants noted that this threat meant that the operational data was treated as sensitive data, none of them argued that it would be particularly devastating for the company.

Similarly, hacking and activism was not seen as a great threat, at least not to shared information. While this could cause some reputation problems, it was considered to be improbable. One participant noted however that although a lot of the sensitive information would be impossible for hackers to exploit, they could potentially sell the information to competitors that could exploit it.

Several participants however argued both for the probability and possible impact of unintended disclosure of information. That is, that authorized personnel, either in their own company or their partners, would release sensitive information by mistake. For instance by releasing an entire specification rather than just the interface specification to customers. One of the subjects even claimed that *"if we could only get rid of the human mistakes, we would probably reduce the incident occurences by 80%"*, although not all of these incidents would be related to shared information. Another stated that when treating sensitive information *"What is really challenging for me is to keep track of the people that already know the secret, and with whom I can discuss matters"*. Hence, unintentional disclosure may result from simple mistakes, not necessarily lack of security awareness. For integrators and suppliers, it is perhaps even worse if this should occur with an operator's data. As noted earlier, during the production phase much of the data shared by these companies are actually owned by the operator. Being liable for misuse of information is potentially more damaging to companies as it may damage the trust of the customers they are dependent on.

5.4 Current security measures

In order to properly assess the *relative advantage* of any new security measures it is important to know existing mechanisms and understand their strengths and limitations. Thus, we asked respondents to name existing mechanisms for controlling shared information usage.

We have no control, as far as I know, of information and what happens to it, other than agreements and mutual trust.

(Participant in the study)

This statement is representative for all participants in the study. As one of them noted *"there are access control mechanisms, but once you have access we have no [usage] control, technical control that is"*. The predominant strategy is the use of Non-Disclosure Agreements (NDAs) or other contractual agreements restricting the usage of information. Some company policies will not even allow discussions of cooperation without a signed NDA. They are therefore used extensively, and particularly whenever companies share product information. However, for integrators and suppliers this tends to be less important towards new customers.

NDAs used within Integrated Operations are to a large extent kept general and signed on management level, but occasionally, depending on the sensitivity of the data, NDAs are also signed by individual employees for a certain specific project. Needless to say, the employees' knowledge of the actual content of an NDA signed at the company level is not very good. Still, participants claim to have a fairly good idea about what is acceptable and what is not, and that this to a large extent boils down to common sense and contents of security policies.

Within research and development projects, where new technology is developed in collaboration, descriptions of Intellectual Property Rights (IPR) is an important part of the contracts. By explicitly stating the owners of IPR for each component in the system any doubts regarding the ownership are removed and the climate for sharing expertise considerably improved.

Contractual measures seem to be the norm throughout the industry, since only one of the participants had ever experienced that other partners had required any form of usage control technology to be used prior to information disclosure. That being said, one of the companies have introduced usage control technology internally, but this has thus far not been widely used.

The contractual measures are in general viewed to be appropriate and not excessive. However, the process of getting NDAs signed can be time-consuming and tedious, particularly in situations were there are disagreements between companies. And although they provide legal protection from misuse, most participants state that it is not enough. It is considered very difficult to get someone convicted for violating an NDA. As one of the participants argue that *"you would have to misuse patentable techology if you were to be convicted in court for telling your new employer"*. This is also backed up by the fact that none of the participants had ever been involved in either prosecuting or being prosecuted for violation of NDAs or other such contracts. To some extent they therefore do question the practical consequences of protecting information using solely *"social and legal measures"*. That being said, utilizing sanctions as a means to coax people into complying with policies has been shown to effective [10].

5.5 Attitude towards usage control enforcement technology

> *I want to help protect the information by helping users so that they do not have to think for themselves. Use technology in such a way that end-users cannot make mistakes.* *(Security specialist)*

Based on an introduction to the concept of usage control enforcement, similar to that of Section 2, participants were asked to provide their opinion as to whether this could actually improve the control of shared information.

Apparent benefits Most participants state that usage control enforcement technology definitely would improve control of information, but that these benefits always must be viewed in context with the challenges introduced. We treat the risks and challenges of usage control technology below, but first we outline the main benefits of the technology, as seen by the participants.

- Relieve employees of the need to think.
- Prevents employees from being tempted to misbehave or take short-cuts.
- Ease the process of invalidating obsolete information.
- Revoke usage rights automatically.
- Restrict actual usage of information as opposed to mere access to it.
- Effective detection/prevention of usage policy violations.

Several participants mention that the reliance on employees to enforce usage policy is not optimal. Therefore, it is no surprise that allowing for automatic enforcement is seen as a benefit. Also, participants seem to think that people might be tempted by circumstances to take short cuts or circumvent systems for convenience. Revoking usage rights of potentially distributed information is something that several participants find interesting, since it reduces the gap between centralized and local information. The exact same functionality may be exploited to invalidate obsolete information distributed to partners. Several participants state that one of the fundamental problems of shared information is ensuring that all collaborating partners have the latest revision of it. Hence, if one could invalidate information that would force people to obtain the latest revision. Restricting usage (e.g. printing, forwarding, copying) is also mentioned as a clear benefit together with the improved effectiveness of detecting or preventing (depending on the type of enforcement) usage policy violations.

Some participants argue that although the benefit is clear, there are other things that are more pressing than usage control enforcement. For instance access control policies could be improved. Participants have experienced collaboration projects where the entire document repository was accessible to all, since managing access control policies was considered a burden. As a result, a lot of sensitive information could not be stored in the repository, and hence alternative parallel systems had to be established for this kind of information exchange.

Risks and challenges

There are a few strengths, but there are also some extreme inconveniences
(Engineer in the study)

The greatest potential risk of utilising usage control enforcement technology, according to participants, is that information may not be available to personnel when they need it. That is, that usage rights have been revoked, or network connectivity prevents you from obtaining necessary authorizations. There is a fear that such a system would be more strict than existing access control systems and additionally extended with ubiquitous enforcement. Since the technology to some extent resembles Digital Rights Management (DRM) systems, many also draw parallels to some of the unfair restrictions that commonly apply to downloadable media files. Thus, participants foresee information lock-in as a direct consequence of adopting usage control technology.

And then there is the management of usage rights. Participants point to the management overhead and costs of specifying, maintaining and deleting usage rights and usage policies. In the event that authorised personnel cannot access information, then either the assigned usage rights are wrong or the policy is incorrect. One of the participants stated that even with their current four-scale classification scheme for sensitive information *"... the probability that a document is correctly classified is about 50%"*.

Another serious issue with usage control technology is the handling of real-time data and legacy systems. Operational data collected at an oil field need to travel through a wide range of different systems for analysis, some of which are legacy systems that are difficult, not to say impossible, to change. As illustrated by one of the security specialists: *" We have state of the art systems, but it is state of the art from 1985 in some cases"*. Additionally, with real-time remote control of operations, there is a general fear that latencies caused by the additional security may be intolerable.

While using information in unforeseen ways or contexts are commonly regarded a threat, it is also how creative solutions to difficult problems come about. One of the participants fear that creativity may suffer as a result of stricter usage control enforcement.

On a general basis, the lack of flexibility that participants see in usage control technology is of great concern and many fear that as a result employees will go to great lengths to bypass the technology.

Regarding whether the enforcement strategy should be proactive or reactive, the participants tend to disagree. To some, the entire value in the technology lies in the prevention of information misuse. The majority however sees the reactive strategy as a way to mitigate most of the challenges identified above, particularly regarding information being unavailable. This of course comes at the price of not being able to prevent misuse. Additionally, by introducing logging mechanisms for all handling of sensitive information, several participants express great concern of being subject to surveillance by both their own and collaborating companies. Furthermore, by being held accountable for their actions,

some employees fear that if being ordered to violate a policy, they are accepting the responsibility of the commanding officer.

6 Conclusions and future work

Through this case study of a collaborative environment with extensive sharing of sensitive information, we have shed some light on the reasons why usage control technology adoption is not picking up the pace. From our analysis it seems clear that the participants are conscious about the risks and the shortcomings of existing measures to restrict usage of shared information. Still, the study demonstrates some of the practical challenges that needs to be tackled in order for the industry to embrace the technology. Some of this might be alleviated through adding flexibility to the enforcement mechanisms, while others require other enabling technology such as decision support on policy specifications.

It seems however, that there is no *silver bullet* for usage control technology either. There are situations in which proactive designs are superior to reactive designs, and vice versa. Still, the lessons learned from this cases study is the need to focus on practical issues that need to be addressed in order to promote all variations of this technology to great masses.

This case study forms a basis for which a more quantitative approach may be taken to gain insights into the relative importance of the different risks and features of usage control technology. Additionally, we believe that it will be worth while to investigate further the effect of decision support systems for both policy specifications and handling of sensitive information.

Acknowledgements

We would like to express our sincerest gratitude to the participants in this study. As part of the research project Integrated Operations in the High North (IOHN), this study has received funding from the Research Council of Norway.

References

1. Park, J., Sandhu, R.: The UCON$_{ABC}$ usage control model. ACM Trans. Inf. Syst. Secur. **7**(1) (2004) 128–174
2. Nyre, Å.A.: Usage control enforcement - a survey. In Tjoa, A.M., Quirchmayr, G., You, I., Xu, L., eds.: MURPBES. Volume 6908 of Lecture Notes in Computer Science., Springer (2011) 38–49
3. Pretschner, A., Hilty, M., Basin, D.: Distributed usage control. Communications of the ACM **49**(9) (2006) 39–44
4. Norman, P., Boer, H., Seydel, E.R.: Protection motivation theory. In Conner, M., Norman, P., eds.: Predicting Health Behaviour: Research and Practice with Social Cognition Models. Open University Press, Maidenhead (2005) 81–126
5. Rogers, R.W.: A protection motivation theory of fear appeals and attitude. Journal of Psychology **91**(1) (1975)

6. Rogers, E.M.: Diffusion of Innovations. 5th edn. Free Press (2003)
7. Nyre, Å.A., Jaatun, M.G.: On the adoption of usage control technology in collaborative environments. In: Proceedings of the 12th International Conference on Innovative Internet Community Systems, Trondheim, Norway (June 13-15 2012) Accepted for publication
8. Seaman, C.B.: Qualitative methods. In Shull, F., Singer, J., Sjøberg, D.I.K., eds.: Guide to Advanced Empirical Software Engineering. Springer London (2008) 35–62
9. Robson, C.: Real World Research. 3 edn. John Wiley & Sons (2011)
10. Siponen, M., Pahnila, S., Mahmood, A.: Employees' adherence to information security policies: An empirical study. In: New Approaches for Security, Privacy and Trust in Complex Environments. Volume 232 of LNCS. Springer Boston (2007) 133–144

A Interview guide

Introduction

1. What is your age, education and professional background?
2. What is your current position in the company?
3. Do you have experience from securing information systems?
4. For how long have you been working within the oil and gas industry?
5. How would you rate yourself regarding general information security awareness on a scale from 1(very conscious) to 7 (completely oblivious)?

Shared information

6. With which partners do you (most often) share information?
7. What kind of information do you (most often) share?

Risk perception

8. How do you think information shared with partners can be misused/abused?
9. What kinds of misuse/abuse do you consider to be the most harmful to your organisation?
10. What kinds of misuse/abuse do you consider most likely to happen?
11. Which actors do you think pose the greatest threat of misusing/abusing information?

Current security measures

12. What security measures do you (or your organisation) currently use in order to control how information is used when shared with partners?
13. What security measures do your partners currently use in order to control usage of information they share with your organisation? (security policies, NDAs, contracts)
14. Are there any situations where you find these security measures to be unnecessary?
15. Are there any situations where you find a lack of protection alarming?
16. Do you believe that the current security measures overall are adequate?

Enforcement technology

17. How do you see enforcement technology improving the control of information?
18. What enforcement strategy (proactive/reactive) would you have preferred for your company?
19. What would you consider the greatest risk in adopting enforcement technology?