On the adoption of usage control technology in collaborative environments

Åsmund Ahlmann Nyre  
nyre@idi.ntnu.no  
Martin Gilje Jaatun  
martin.g.jaatun@sintef.no

Abstract:  
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. Businesses employ non-disclosure agreements, but have no means to prevent or detect violations of these. Usage control has been proposed as the means to protect information even after its distribution. However, despite the efforts to develop new usage control technology and the apparent need for it, the industry is less enthusiastic. In this paper we investigate existing theories of technology adoption in order to better understand the industry-perspective and to improve technology development. We base our study well-known general theories on protection motivation, innovation diffusion and technology acceptance. We then utilize these theories and preliminary results of a case study to build a new model for understanding usage control technology acceptance.

1 Introduction

While traditional access control is focused on providing or denying access to resources, it is currently unable to restrict and control how those resources are being used. That is, once the information has left the system any restrictions on its use are solely at the receiver’s discretion. For instance, suppose a consultant has been granted access to an incident report from an organisation in order to analyse the cause of the incident. What is there to prevent the consultant from leaking the report to public media or a competitor? In order to remedy this, the research community have proposed usage control [PS04], which may be seen as a extension of access control beyond system borders to control usage on the client-side. Returning to our example, usage control could have granted the consultant rights to read the report for the duration of the assignment while ensuring that copying or forwarding was prohibited.

As we have previously shown [Nyr11] there is an ample body of research on technology to specify, organise and enforce usage control polices. Despite the researchers’ firm beliefs that businesses should employ usage control technology, there is to the best of our knowledge no empirical support for its appropriateness. This paper represents a starting point to identify why the industry does not share researchers’ view on the necessity of distributed
To this end, we attempt to combine different technology adoption theories and models as well as preliminary results of an ongoing case study in a collaborative environment in order to explain this discrepancy.

The remaining parts of this paper is organised as follows. Section 2 gives a brief introduction to theories and models to explain the adoption of technology. We provide both general theories and some more specific to protective technologies. Next, we review some of the previous approaches to explaining security technology (or behaviour) adoption in Section 3. In Section 4 we develop and describe our new model for usage control technology adoption. Finally, we provide a brief discussion of the model and its appropriateness and give our concluding remarks in Section 5.

2 Background and theories on technology adoption

Technology adoption and how innovations diffuse in a social system has been a subject of interest for many years. What is it that causes some technology to have a wide uptake while other, seemingly good innovations fail? And, perhaps more interesting for market analysts: is it possible to predict the adoption rate of new technology before it enters the market? Before we return to these questions for usage control technology we provide a brief overview of the main general purpose theories and models that have been developed.

In his theory on diffusion of innovations, Rogers [Rog03] outlines five main categories of factors that influence, and possibly can predict, the decision to adopt new technology. A lot of consideration is devoted to factors outside the innovation itself, such as promotion efforts and use of communication channels. We however limit our discussion here to the intrinsic characteristics of the innovation, termed the perceived attributes of the innovation.

- Relative advantage
- Compatibility
- Complexity
- Observability
- Perceived risk

Placing attributes within one of these attribute categories may not be straightforward. In a review by Tornatzky and Klein [TK82], they found that there was considerable dispute among researchers regarding the contents of the attribute categories, in part due to the lack of separation between the attributes. In one study profitability is seen as a separate factor, whereas in another it is seen as part of the relative advantage. Similarly, the compatibility attribute may denote both the degree to which it fits with the ideas/norms of the current system and the degree to which it fits with the operational aspects of the current system (i.e. the way things are done). Although these differences made it difficult to assess the dominant attributes in predicting innovation diffusion, the meta-analysis found that compatibility and relative advantage were positively related to adoption whereas complexity
was negatively related. Other attributes did not display significant relation to adoption, however as noted by the authors this might be due to the inconsistency in attribute definition.

From behavioural psychology there are also theories that may be utilised in order to describe, understand and predict how innovations (in our case, technology) may be adopted by users and organisations. The Theory of Reasoned Action (TRA) [FA75] is based on the idea that attitude towards a behaviour and the subjective norm (i.e. others’ attitude) affect the intention to behave a certain way, which in turn affects the actual behaviour. The theory was later extended by Theory of Planned Behaviour (TPB) [Ajz91] to include users’ perceived control of the behaviour or the degree to which the action is perceived as voluntary. It can be seen that a user’s attitude towards a behaviour, or in our case: use of technology, is to a great extent affected by Roger’s attributes of the innovation. Notice however the difference between Roger’s focus on the innovation itself and the theory of planned behaviour’s focus on its usage. However, as demonstrated by Moore and Benbasat [MB91], a slight change of wording in Roger’s attribute definitions would yield a more behavioural theory.

In the realm of information systems the Technology Acceptance Model (TAM) [Dav89] has been one of the main models for predicting technology uptake. It defines two main factors affecting technology adoption: perceived usefulness and perceived ease of use. It builds on both TRA and TPB as it attempts to explain the actual technology acceptance based on the attitudes towards using the technology. However, the main factors are also very similar to Rogers’ perceived relative advantage and perceived complexity of an innovation. Further, Venkatesh and Davis [VD00] argue that the other factors defined by Rogers are mediated by perceived ease of use and usefulness. It is a very simple yet powerful model for explaining and predicting use of information systems. Still, the simplicity has also motivated an extension to TAM, denoted TAM2 [VD00], by extending the original TAM with many of the factors defined in Rogers’ innovation model. Thus, social constructs such as subjective norm, image and voluntariness and cognitive constructs such as job relevance, output quality and result demonstrability are included as factors directly or indirectly affecting technology acceptance. In an effort to synthesise the strong points of the various models for technology adoption, Venkatesh et al. proposed the Unified Theory of Acceptance and Use of Technology (UTAUT) [VMDD03].

Another approach to explaining human behaviour is the rational choice theory [Sco00], popularly referred to as the cost-benefit tradeoff. The theory has been extensively used both in economics, criminology and social sciences [Sco00]. Basically, the theory states that when faced with choices, humans will select the option that maximises the utility. Hence, a rational choice is one that adheres to this rule. McCarthy describes the requirements of being “rational” in more detail [McC02]. Referring to the relative advantage as defined by Rogers, it is possible to see this as indeed a cost-benefit analysis.

While the above mentioned theories all seem to describe functional technology, the situation for non-functional technology is somewhat different. For example, the usefulness of a firewall is very much dependent on the perceived risk of not using it. Thus if the risk of intrusions is high, the firewall is perceived to be more useful. Conversely if the risk of intrusions is low, the firewall is not that useful. It is exactly this notion that the Protec-
tion Motivation Theory (PMT) [Rog75] attempts to describe. The essence of the theory is that the intention to behave in a certain manner and consequently the actual behaviour is affected by the risk perception (vulnerability and severity) and the degree to which the coping measure (that mitigates the risk) is efficient or not. Jointly, these two factors may be viewed as the relative advantage of the protective technology, and hence the links to Rogers’ theory on innovation diffusion as well as TAM are quite clear. Additionally, the tradeoff between perceived risk and perceived efficacy of the coping response may also be viewed in relation to the cost-benefit tradeoffs of the rational choice theory. Protection motivation theory has been extensively used in campaigns for health related issues and traffic safety [IFPDR00].

Deterrence theory has also been used in order to understand adoption of non-functional technology. The general deterrence theory (GDT) [HWF05] is based on the idea that if abusive behaviour is likely to be detected and severely punished, humans will refrain from such activity. Although it is possible to view deterrence as a means to force people to use a certain technology, we instead view deterrence as one of the primary theories behind any audit or monitoring-based usage control technology.

While the above theories on technology acceptance and usage are different both in focus and viewpoint, it is evident that they do share some fundamental concepts. Theories on the adoption of functional technology uses usefulness, relative advantage or benefit to describe the users’ need for the technology, whereas the theories on adoption of protective technology use the combination of threats and response efficacy to convey the same. All theories do however consider other factors in varying degree of detail such as social complexity, compatibility, social norm, etc.

3 Related work

We have noted earlier that empirical evidence of actual use of information and usage control technology is to a large degree absent [Nyr11]. However, by regarding usage policies as similar to security policies we can draw upon the work on security policy compliance. The problem in this area is to determine and predict the degree to which users adhere to the security policies they are subject to.

Siponen et al. [SPM06] apply a combination of the theory of reasoned action (TRA) [FA75] and the protection motivation theory (PMT) [Rog75] in order to identify the factors affecting information systems security policy compliance. The study was conducted within five companies and a total number of respondents of 919. The results demonstrate that normative beliefs and visibility significantly influences both the threat appraisal and coping appraisal, which in turn affects the intention to comply and the actual compliance with the security policy. Although both the theoretical and empirical evidence are sound, the granularity of the factors makes it somewhat difficult to apply to usage control. For example, vulnerability is defined as “the employees’ assessment of whether their organization is vulnerable to IS security threats” [SPM06] and the corresponding response-efficacy is to what extent the security policy mitigates the threat. In a follow-up study [SPM07], the
authors also employed the general deterrence theory and demonstrated that sanctions have a significant effect on the actual policy compliance. This is supported by other studies as well [HR09b, HR09a].

A more complex model was developed by Bulgurcu et al. [BCB10] including security policy awareness and general security awareness as important factors affecting the compliance with security policies. By basing their model in part on the rational choice theory, the authors include perceptions of benefits and costs of both compliance and non-compliance with the security policy. The security policy awareness is only self reported, as opposed to a knowledge quiz to determine the awareness. Thus, it is perceived security policy awareness, rather than actual awareness that is found to affect intention to comply.

One of the few studies on security technology adoption utilized Protection Motivation Theory to explain users’ attitude and behaviour towards home wireless security [WTL05]. The study used a knowledge quiz to determine respondents’ security awareness with respect to wireless security and possible coping measures. Of the factors identified by Rogers [Rog75], perceived vulnerability was the single factor that did not demonstrate a significant effect on determining whether the user actually had enabled the prescribed security measures. A similar approach was taken by Chenoweth et al. [CMG09] in order to study the use of anti-spyware software. In this study, the authors did not only seek to identify factors affecting intention to utilize the coping response, but also maladaptive coping. That is, to identify the factors that lead users to deliberately not utilize the coping behaviour. Perhaps not surprisingly, the response cost was the only factor that significantly affected the maladaptive behaviour. Whereas the threat appraisal was shown to positively affect the intention to use security technology, the response cost was shown to negatively affect it.

Common to all of these approaches is that they consider only the collective threat and the collective response efficacy as perceived by users. For instance in the study by Woon et al. [WTL05], perceived severity is measured on three different threats; identify theft, e-mail eavesdropping and privacy breaches, whereas perceived vulnerability is only measured in total. None of them consider how different attackers may influence both the severity and vulnerability (or probability) of a specific threat. And in the study by Siponen et al. [SPM06] they only consider the collective threat “employees’ assessment of whether their organization is vulnerable to IS security threats” [SPM06], which does not consider whether the employees consider the threats that the security policy is supposed to mitigate.

4 A model for usage control technology adoption

In this section we elaborate on our work to apply the existing theoretical models of technology and innovation adoption to the area of usage control technology in collaborative environments. To this end, we have conducted a case study within the oil and gas sector in Norway to identify important factors influencing adoption of usage control technology as seen by the industry itself.

We start by providing a brief background on the case study conducted and a description of characteristics of the oil and gas industry that makes this industry ideal for the type of
collaborative environments we are to study.

4.1 Case study

The motivation for the case study is to better understand the perceptions of risk and coping technology in the IO community context. Through interviews we have sought to identify potential risks, appropriateness of current security measures and the perceived efficacy of usage control technology as the coping response. Currently, we have conducted 9 interviews with key personnel from both oil companies, contractors and consultancy businesses. While we are unable to make definitive statements based solely on these interviews, they do provide insights on the problems and perceptions of the industry that can well be used to build and extend our theoretical models.

The term Integrated Operations (IO) has been used by the oil and gas industry on the Norwegian continental shelf to denote a state in which information and services are integrated across onshore and offshore, across different locations, and across organisations. This vision of seamless integration requires collaboration on an unprecedented level. While collaborative efforts are common in many sectors, the special case of the oil and gas sector is the mixture of competition and collaboration. For example: Oil companies are competing to find, produce and ship oil, but at the same time they are collaborating on exploration activities and remote field developments. Thus, it is vital that information shared in one context is not misused in another. Which of course puts heavy demands on the ability to control information flow and information usage. The combination of collaboration and competition coupled with seamless data integration is what makes the oil and gas industry particularly interesting for the adoption of usage control technology.

4.2 The basic model

Our basic model is depicted in Figure 1. As can be seen, it is primarily based on the Protection Motivation Theory but adapted to information security. The model also includes some elements from the theory of innovation diffusion as well as the Technology Acceptance Model.

Risk appraisal is used instead of the original threat appraisal in PMT. This is primarily due to different definitions of the concepts. Within information security, risk is commonly used to denote the combined likelihood and effect of a threat action performed by a threat agent. Thus, we therefore let system vulnerability be a contributing factor to the likelihood of a threat action.

The response cost, response efficacy and self-efficacy are all taken from PMT. We have however added the ease of use concept form the Technology Acceptance Model and the compatibility from the diffusion of innovations theory. Since the original PMT model seems to only consider a coping response versus no response, we have introduced the relative advantage concept from the diffusion of innovations theory. We have discovered
that there are often existing coping responses in use. Therefore the coping response must not only be effective and efficient, it must also surpass any currently implemented response. In the following subsections we elaborate further on the various parts of our model and provide justifications for them based on the case study.

4.3 Risk perception

The original PMT model only handles threats collectively, both with respect to severity and vulnerability. However, as we discovered through our interviews, there are a wide range of threats to shared information that are virtually impossible rate collectively for severity and vulnerability. Additionally, as already mentioned in Section 4.2, the perceived severity and likelihood of a threat action is greatly dependent on the threat agent (or attacker), something that the original PMT model does not consider. In classical safety thinking, which is where PMT originated, threats are assumed to be unintentional, such as getting cancer from cigarette smoke or being seriously wounded in a car accident. However, within information security, the attacker is quite central when determining both the probability and severity of an attack. If a competitor steals a company’s source code, that would be much more severe than if a random teenage hacker did it. We therefore included three new concepts from the OWASP approach to determining risk [OWA08] as part of our model: Technical impact, business impact and threat agents.

The technical impact describes the objective effect of the attack, such as compromised source code. However, since the business impact of compromised source code may vary considerably, this is treated separately. For some companies it may be devastating while for
<table>
<thead>
<tr>
<th>Threat</th>
<th>Threat agents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Industrial espionage</td>
<td>competitors, intelligence agencies</td>
</tr>
<tr>
<td>Corporate espionage</td>
<td>competitors, suppliers, customers</td>
</tr>
<tr>
<td>Economic espionage</td>
<td>suppliers, customers</td>
</tr>
<tr>
<td>Terrorism and activism</td>
<td>political, environmental activists</td>
</tr>
<tr>
<td>Unintentional disclosure and human mistakes</td>
<td>own and partner employees</td>
</tr>
<tr>
<td>Insiders’ intentional disclosure</td>
<td>own and partner employees</td>
</tr>
</tbody>
</table>

Table 1: The case study participants most frequently mentioned threats against shared information and their corresponding threat agents

others it may not be that important. On the likelihood, the threat agent is the one actively carrying out an attack while the vulnerability is the probability that an attack would be successful.

As part of the interviews we asked the subjects to name the threats to shared information they perceived to be the most severe, the most probable and which actors they considered to pose the greatest threat to their company. In Table 1 we have listed the most frequently mentioned threats (either for severity or probability) with corresponding threat agents. Note however that the lists are unordered with respect the risk they pose.

Espionage is clearly something that the case study participants are worried about. We have separated three different kinds of espionage based on the underlying motive and the kind of information subject to the threat. *Industrial espionage* considers misuse of technical information, Intellectual Property Rights (IPR), innovations and systems. The severity of this kind of threat was perceived to be high since it potentially could reduce the company’s competitive advantage towards competitors or foreign nations. *Corporate espionage* considers misuse of corporate information such as strategies, price information, priorities and such. This threat could also reduce the competitiveness of the company as the threat agents could adapt their behaviour. *Economic espionage* considers information on the financial situation of a company such as production volumes and contract negotiations. Misuse of financial information may affect stock market and prices, and hence is of high importance to companies even if threats may not directly harm the company.

Terrorism and activism was mentioned by several as something to be aware of, but all of the interviews regarded successful attacks to be highly unlikely. Still, the severity could potentially be high in terms of damaged reputation.

*Unintentional disclosure and human mistakes* was also quite frequently mentioned. One of the subjects even claimed that “if we could only get rid of the human mistakes, we would probably reduce the incident occurrences by 80%”, although not all of these incidents relating to shared information. It is therefore important to consider the amount of information that is compromised due to mishaps by employees. The severity of the disclosure may of course vary considerably, but in worst case it may be very high and pave the way for any type of espionage. *Insiders* may cause similar impact, but are distinguished by the fact that information disclosures are intentional.
4.4 Usage control technology appraisal

Through the interviews we attempted to identify the key factors of the coping response, in our case usage control technology, that would influence its adoption. As mentioned previously, the four main groups of factors are relative advantage, response efficacy, self-efficacy and response costs. All but the first are also part of PMT, although with slightly different contents.

Relative advantage was added as a factor since we believed it to be crucial that usage control technology be superior to the mechanisms that are currently implemented in the organisations. Although we acknowledge that some of this could be expressed through response efficacy, it is important to show the perceived superiority of the new approach. As part of the case study we asked respondents to identify existing measures taken to control the use of information they shared with others. Inline with our assumptions, the primary protection measure employed was the use of Non-Disclosure Agreements (NDAs) or other contractual measures to safeguard confidentiality. NDAs were used at very different level of granularity. Some were signed by the management group as a contract between companies, whereas others would be signed by individual employees on individual projects. Thus, a considerable amount of information handled by employees are governed by an NDA they have never seen. Instead, it is assumed that the companies’ security policy will ensure proper conduct. One of the companies involved in the case study had implemented the Microsoft Rights Management System [Mic03], but so far it had only been used internally on a hand-full of projects. None of the respondents considered the use of NDAs to be burdensome in any way, and did not think of it as reducing their job efficiency. However, they all noted that relying solely on legal measures may not be adequate to protect against the identified threats. Or as one of the participants stated: “We have a lot of socio-cultural and legal control, but we realise that we need more technological control”.

The case study participants did not agree on the response efficacy of usage control technology, but it is evident that this is an important factor affecting the adoption of technology. Particularly whether the technology should be proactive (prevent misuse) or reactive (detect misuse) seemed to be an area of debate. Also, as noted by one of the participants, “if there is a way to bypass the usage control technology, people will do it and start distributing unprotected versions instead”. The response costs are very much related to the response efficacy. That is, by being too strict, the usage control technology could make important information unavailable and hence greatly reduce the job performance. Particularly since, as one participant noted “we have currently a lot of problems categorising information, perhaps only 50% of all documents have correct classification”. Thus, if applying strict preventive usage control to information that has not been accurately categorized would result in a lot of information being unavailable. Further, participants claimed that the administrative burden caused by having to maintain usage rights and monitor usage policy violations would definitely impose additional costs for the companies.

Self-efficacy and the practical issues of day to day use were stressed by several of the participants. “It is important to strike a balance between protecting information and getting the job done”. Participants were also concerned that specifying the usage policy would be troublesome, if it would have to be done independently for each document made. This
might be mitigated if the usage control policy somehow could be inferred from the access control policy of the document management systems currently deployed (compatibility).

5 Discussion and conclusion

Our adapted model has yet to be verified through proper evaluations. Until then, existing research on protection motivation for security technology at least indicate circumstantial evidence for its fitness of use. Additionally, the protection motivation theory have been proven quite successful in health protection measures [MSO00].

We further argue that it is virtually impossible to speak of any relative advantage of security technology without at the same time considering the threats or risks they are to mitigate. Hence, the usage control technology can only be perceived to be useful if there is a threat from which it can protect its users.

One may argue that the entire process of understanding how usage control technology is adopted is very similar to conducting a mere risk analysis. To a certain extent it is true, it does resemble a risk analysis. However, the crucial point in understanding protection motivation lies in the individuals and the focus on users’ perception of risk and threats. The risk assessment is often the security professionals opinion, whereas the protection motivation is the lay-men’s individual perception.

We have thus far concentrated on the primary elements of protection motivation and the attributes of the innovation as the factors influencing usage control adoption. For future revisions of our model we do however believe factors outside the technology to also be highly relevant when explaining or predicting the adoption of usage control technology. Usage control technology is to certain extent similar to Digital Rights Management - a technology that continues to be controversial - and therefore the concepts of attitude and subjective norm from TRA could be important. Further, it also seems that previous major changes that have occurred within the oil and gas industry have either been driven by the oil companies or the industry associations, and so the role of change agents in the theory of innovation diffusion could provide additional input. Although the case study material contain some information on these aspects, it remains to be further analysed and interpreted. Finally, we are also working on having the model verified through an experiment on a larger population within the oil and gas industry.

This paper has shown the usefulness of technology adoption theories in order to better understand the users’ perception of protection technology. In the future we will continue to develop our initial model and will also subject it to evaluation by the industry.

References


SESSION 5

Technology for Cloud Computing and Future Internet

David Bouck-Standen, Jörg Cassens, Michael Herczeg

Lazy Disclosure – Mixing Cloud and Local Storage .....................................................155

Martin Gilje Jaatun, Christian Askeland, Anders Salvesen

Drizzle: The RAIN Prototype .........................................................................................165

John Krogstie

The Role of Modeling in Innovative Business and Community Information Systems ....177