An Empirical Evaluation of Information Security Awareness Levels in Designing Secure Business Processes

Fergle D’Aubeterre
FT Services
Suite 3000, 715 5th Avenue, SW Calgary, Alberta T2P 2X6, Canada
001-403-718-3772
DAubeterref@ft-serv.com

Lakshmi S. Iyer
The University of North Carolina at Greensboro
Greensboro, NC 27402, USA
001-336-334-4984
Lsiyer@uncg.edu

Rahul Singh
The University of North Carolina at Greensboro
Greensboro, NC 27402, USA
001-336-256-0260
Rahul@uncg.edu

ABSTRACT
Information Systems Security (ISS) is critical to ensuring the integrity and credibility of digitally exchanged information in business processes. Information systems development methodology that considers security requirements in the early phases of systems development is essential for ISS. In the context of ISS, information security awareness (SA) can play a vital role in minimizing end-user related security faults and maximizing the efficiency of security techniques. This information security awareness should be present in the requirements gathering phase of the software development process so that analysts become more aware of security constraints and possible violations resulting into secure business processes. In this paper, we extend the work by D’Aubeterre et al. (2008b) to evaluate the utility of Secure Activity Resource Coordination (SARC) artifacts in generating three levels of security awareness: perception, comprehension and prediction. The experimental evaluation shows that using SARC artifacts analysts are able to better explain the current state of security of a business process. Should violations occur, analysts are able to explain the nature of security violation in terms of segregation of duties, non-repudiation, and authorization.

Categories and Subject Descriptors
D.2.1: Software, software engineering, requirements specification.

General Terms
Secure design process.

Keywords

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

DESRIST’09, May 7-8, 2009, Malvern, PA, USA.
Copyright 2009 ACM 978-1-60558-408-9/09/05...$5.00

1. INTRODUCTION
Given the increased reliance on computer systems for exchange of business process information, information systems security (ISS) is critical to ensure the integrity and credibility of the available and exchanged inter-organizational information (Siponen & Iivari, 2006). Despite the importance of ISS, the 2006 CSI/FBI Computer Crime and Security Survey identified that authorization violations are the second largest cause of economic losses (Gordon et al., 2006). In the context of ISS, Siponen (2000) emphasizes that information security awareness plays a vital role in minimizing end-user related security faults and maximizing the efficiency of security techniques. This information security awareness should be present in the requirements gathering phase of the software development process so that analysts become more aware of security constraints and possible violations resulting into secure business processes (D’Aubeterre et al., 2008b).

In depth information security analysis and understating have proved and become a difficult goal to attain in many security sensitive industries such as defense, banking, and health care. Using design science (Hevner et al 2004) approach, In our prior work (D’Aubeterre et al., 2008b), we developed the modeling concepts and grammar for Secure Activity Resource Coordination (SARC) based on the Semantic approach to Secure Collaborative Inter-Organizational eBusiness Processes (SSCIOBP) (D’Aubeterre et al., 2008a) to represent a secure business process. Baskerville et al. (2007) suggest that rigorous evaluations of design science artifacts are of vital importance to show that the design artifacts are complete and effective and add value to the problem and knowledge domain. While our prior work (D’Aubeterre et al., 2008b) demonstrated the utility of SARC in generating greater awareness of security requirements in the analysis of business processes, the study did not provide details regarding the aspects and levels of security awareness generated by using SARC artifacts. In this study, we extend the study by applying the three different levels based on situational awareness (SA) theory (Endsley 1995) to evaluate different levels of security awareness. Situational Awareness (Endsley 1995) is the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status within the near future.
The first level of SA is the ability to perceive the status, attributes and dynamics of relevant elements in the environment and forms a basis for decision making. Perception of security elements and security policies violations in eBusiness process is important so that analysts capture the security elements in the early phases of systems development. The second level of SA goes beyond awareness, into comprehension and includes an understanding of the significance of elements for pertinent goals. A novice may achieve the same level of SA as an expert, but fall short of also being able to integrate various data elements along with pertinent goals to comprehend the situation. Here, we posit that situational awareness can be used to define security awareness as “the state where subjects are capable to receive information security elements such as segregation of duties, non-repudiation, and authorization in their environment leading to a better understanding and prediction of security conditions”. Thus, it is important to examine if SARC artifacts help increase the comprehension of security elements and security policy violations in an eBusiness process. At the highest level, SA includes the ability to project the future actions of the elements in the environment within temporal constraints of the problem domain forms based on knowledge achieved through the first and second levels of SA. In the security awareness context, we examine if SARC artifacts help analysts predict security violation in an eBusiness process.

Specifically, we attempt to answer the following research questions:

i) Can SARC artifacts be used to increase the perception of security elements and security policies violations in the context of an eBusiness process?

ii) Can SARC artifacts lead to better comprehension of security elements and security policies violations in the context of an eBusiness process?

iii) Can SARC artifacts be utilized to predict possible security violations in the context of an eBusiness process?

Empirical evaluation show that SARC design artifacts generate greater level of security perception, comprehension and prediction than best known design approaches proposed by Siponen et al. (2006) i.e. Enriched-Use Case and UML-Activity Diagram. Findings show that SARC design artifacts allow subjects to make better inferences about future security states of a business process and to perform what-if type analyses of security violations. When security requirements are incorporated as functional requirements in the analysis of business processes, analysts become more aware of security constraints and possible violations resulting into secure business processes.

2. THEORETICAL FOUNDATIONS

In this section, we summarize the main information systems security design methods and analyze the situational awareness (SA) theory (Endsley 1995) levels.

2.1 Information Systems security Design Methods

Baskerville (1988) states that “the best approach to the development of security analysis and design methodology, would essentially be to nest it as a component part of an existing, established, successful overall information systems analysis and design methodology” (p. 88). Holistic information systems methodology that includes security aspects in all of its stages is still needed (Baskerville, 1988). Chung and Nixon (1995) developed a process oriented approach that allows developers to represent security requirements as non-functional requirements. Lee et al. (2005) proposed an integrated software lifecycle process with Security Engineering (SE). Apvrille and Pourzandi (2005) proposed a methodology to produce secure applications by extending the general project life cycle methodology and inserting security concerns at each phase. Mouratidis et al. (2005) extended the TROPOS development methodology incorporating security concepts such as security constraints, secure entities, and secure dependencies. Jürjens (2001) extend UML to include modeling of security requirements (UMLsec). While UMLsec allows modeling access control mechanisms and aspects of information confidentiality, this work primarily focuses on the design phase. Mc Dermott and Fox (1999) proposed the use of abuse cases that capture and analyze security requirements. An Abuse case is an extension of object-oriented use case technique and specifies interactions between system and actors where the results of the interaction are harmful (Mc Dermott and Fox, 1999). An abuse case provides a mechanism to model systems security threats in the requirements analysis phase of the SDLC. Sohr et al. (2005) explain that several classes of authorization constraints can be represented and specified using UML and the Object Constraint Language (OCL). Sohr et al. (2005), using the UML Specification Environment (USE), demonstrate how authorization policies such as role-based access control (RBAC) policies can be modeled using UML/OCL.

Dhillon and Backhouse (2001) analyze IS security research using a conceptual framework of four paradigms: functionalist, interpretive, radical humanist, and radical structuralism paradigm. They find that while most IS security research focuses on formalized rule structures in designing security, IS researchers are moving away from the security technical viewpoint towards a socio-organizational perspective. This movement may lead to more holistic IS security research where organizational security aspects are incorporated in the design and development of secure information systems. Attempts to incorporate security as a functional requirement in the early stages of requirement specification and analysis are worthwhile (van Wyk and McGraw 2005). Current research identifies security requirements in the requirement specification stage, but fails to show how these requirements can be incorporated in the design of secure business processes. D’Aubeterre et al (2008) introduce security constraints that incorporate access control mechanisms in the conceptualization of business processes to model the secure exchange of information resources in coordinated business processes.

Siponen et al. (2006) propose a meta-notation framework to represent and analyze information systems security requirements. They extend the UML-Use Case; to incorporate security requirements into the design phase. Field study and action research were used to validate their proposed framework. Table 1 shows the meta-notation for the Enriched-Use Case (Siponen et al., 2006). Enriched-Use Case incorporates security constraints, security subjects, and security actors into the design of IS.
Table 1. Enriched- Use Case (Adopted from Siponen et al., 2006)

<table>
<thead>
<tr>
<th>Use case: Booking.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version: 1.0</td>
</tr>
<tr>
<td>Functional Summary: A booking clerk books journeys for customers.</td>
</tr>
<tr>
<td>Frequency: Several times a day</td>
</tr>
<tr>
<td>Usability requirements: Any database query and booking must be able to complete in less than 30 seconds</td>
</tr>
<tr>
<td>Actor/security subject: A clerk.</td>
</tr>
<tr>
<td>Security classification of the subject: confidential</td>
</tr>
<tr>
<td>Security objects and access types to security objects: Object: customer file (the clerk must be able to read, update and delete the customer information); Object: booking database (the clerk must be able to read, update and delete the customer information on the database)</td>
</tr>
<tr>
<td>Security policy/Specific security restrictions: The clerk is only allowed to access security objects classified as confidential with the booking department.</td>
</tr>
<tr>
<td>Preconditions: Booking and customer databases exist. The identity of the booking clerk/security subject has been validated.</td>
</tr>
<tr>
<td>Exceptions: If information on a certain journey is not available, an appropriate error message is produced.</td>
</tr>
</tbody>
</table>

Note: Security semantics are illustrated in italics and boldface.

D’Aubeterre et al. (2008) develop and evaluate a Secure Activity Resource Coordination (SARC) design method based on role base access control (RBAC) (Sandhu 1996), coordination mechanisms (Malone et al., 2003; van der Aalst and Kumar 2003), and the view of business process (Singh and Salam, 2006; Oh and Park, 2003; Raghun and Vinze 2007). SARC provides the modeling concepts and grammar needed to model and analyze secure business processes. The following rules represent the modeling concepts and grammar for SARC secure business processes (D’Aubeterre et al, 2008a).

1. Actors fulfill organizational roles.
2. Organizational Roles are authorized to perform Business Activities.
3. Business Activities are permitted to read, write, delete or create Information Resources
4. Dependencies do not exist directly between Business Activities. Business activities cannot directly produce or consume another business activity.
5. Activities have a sharing, fit or flow dependency with an information resource.

2.2 Situational Awareness Theory

Situational Awareness (SA) Endsley (1995) is the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status within the near future. Endsley (1995) defined three level of situational awareness (SA). The first level of SA is the ability to perceive the status, attributes and dynamics of relevant elements in the environment and forms a basis for decision making. The Second level of SA goes beyond awareness, into comprehension and includes an understanding of the significance of elements for pertinent goals. At the highest level, SA includes the ability to project the future actions of the elements in the environment within temporal constraints of the problem domain forms. This is achieved through knowledge of the status and dynamics of the elements and comprehension of the situation, achieved through the first and second levels of SA.

Conceptual modeling is the activity of formally describing aspects of the physical and social world around us for purposes of understanding and communication (Mylopoulos, 1992). In this study, we apply SA theory to define and measure the levels of situational awareness of security policies and constraints generated by using the SARC conceptualization of a secure eBusiness process.

In the context of ISS, Siponen (2000) emphasizes that information security awareness plays a vital role in minimizing end-user related security faults and maximizing the efficiency of security techniques. We posit that situational awareness can be used to define security awareness as “the state where subjects are capable to perceive information security elements such as segregation of duties, non-repudiation, and authorization in their environment leading to a better understating and prediction of security conditions”. Consequently security awareness is a three-level construct that includes security perception, security comprehension, and security prediction.

3. EMPIRICAL EVALUATION

In design science research, experimental evaluations assess the utility of design artifacts. Evaluating the proposed design artifacts using an experiment empirically demonstrates the qualities of the artifact (Hevner et al., 2004) and allows for the generalizability of the findings. Walls et al. (1992) suggest an experimental design where the performance of the experimental group using the IT artifact is compared against the performance of the control group not using the IT artifact. We use Situational Awareness theory (Endsley) to define and measure the levels of situational awareness of security policies and constraints generated by using the SARC conceptualization of a secure business process.

Business process models (BPM) are used to increase the awareness and knowledge about business processes and to decouple organizational complexity (Davenport, 1993; Hammer and Champy, 1993). Existing methods for the design of secure information systems still lack a conceptualization of secure business process. We evaluate the utility of SARC design theory in representing security constraints in the conceptualization of a secure business process. We use situational awareness theory (Endsley, 1995) to empirically evaluate the SARC design artifacts against the Enriched-Use case (Siponen et al., 2006) and UML-activity diagram. We assess how SARC design artifacts help in developing a greater level of security awareness.

We argue that when security specifications are incorporated as functional requirements early in the modeling and analysis of business processes, analysts become more aware of security constraints and possible violations resulting into more secure business processes. This, in turn, leads to the incorporation of security policies and constraints in subsequent stages of information systems development, including modeling, analysis, and design.
We expect that SARC design artifacts lead to greater security awareness, including the perception, comprehension, and prediction of security requirements and constraints in business processes. Figure 1 shows the research model.

<table>
<thead>
<tr>
<th>Security Design Methods</th>
<th>Security Awareness</th>
</tr>
</thead>
<tbody>
<tr>
<td>• SARC Artifacts</td>
<td>• Perception of Security Elements in Current Situation</td>
</tr>
<tr>
<td>• Enriched Use Case and Activity Diagrams</td>
<td>• Comprehension of Security in Current Situation</td>
</tr>
<tr>
<td></td>
<td>• Prediction of Future Security State</td>
</tr>
</tbody>
</table>

Figure 1. Research Model

Based on this research model, we attempt to answer the following research questions:

i) Can SARC artifacts be used to facilitate the perception of security elements and security policies violations in the context of an eBusiness process?

ii) Can SARC artifacts lead to comprehension of security elements and security policies violations in the context of an eBusiness process?

iii) Can SARC artifacts be utilized to predict possible security violations in the context of an eBusiness process?

3.1 Research Hypotheses

According to Larkin and Simon (1987, p. 67) “two representations are informationally equivalent if all the information in the one is also inferable from the other, and vice versa”. Even though SARC and the Enriched-Use Case and UML-Activity diagrams provide two different representations for the same business process, SARC design artifacts must be at least informationally equivalent to Enriched-Use Case and UML-Activity diagrams in capturing the dynamics of business processes. Only then can one guarantee that the new approach is at least as good as existing approaches and does not create any loss of information about the business process. D’Aubeterre (2008b) had already shown that the two approaches are informationally equivalent. This was tested by comparing the inferences that users make about the business processes represented using SARC design artifacts and the Enriched-Use Case (Siponen et al. 2006) combined with the UML-activity diagrams.

Since our primary goal is to evaluate the different levels of security awareness, we hypothesize:

H1: BPM developed using SARC Artifact creates a more accurate perception of security elements (i.e., segregation of duties, non-repudiation, and authorization), in a business process than those using the Enriched Use Case and Activity Diagram.

H2: BPM developed using SARC Artifact creates a more accurate comprehension perception of security elements (i.e., segregation of duties, non-repudiation, and authorization) in a business process than those using the Enriched Use Case and Activity Diagram.

H3: BPM developed using the SARC Artifact creates a more accurate prediction of the future security state of the business process, that those using the Enriched Use Case and Activity Diagram.

3.2 Design and Data Collection

Using an experimental design (see Table 2) with repeated measures and counter-balanced design, subjects were randomly assigned to two groups.

<table>
<thead>
<tr>
<th>Group</th>
<th>Enriched Use Case and Activity Diagram (Treatment 1)</th>
<th>Secure Activity Resource Coordination (SARC) (Treatment 2)</th>
<th>Observation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group 1</td>
<td>Observation</td>
<td>Secure Activity Resource Coordination (SARC) (Treatment 2)</td>
<td>Observation</td>
</tr>
<tr>
<td>Group 2</td>
<td>Secure Activity Resource Coordination (SARC) (Treatment 2)</td>
<td>Observation</td>
<td>Secure Activity Resource Coordination (SARC) (Treatment 2)</td>
</tr>
</tbody>
</table>

Experimental designs with repeated measures have several benefits. First, they have high statistical power, due to the fact that there will be a positive correlation between treatments (Keren, 1993). Second, under repeated measures designs, subjects act as their own control and the confounding effects due to different subjects’ background are minimized. Finally, repeated-measures designs require fewer subjects as compared to a between-subject design to achieve the same statistical power level (Brooks, 1980). However, the danger with repeated-measured design is the existence of a carry-over or learning effect (Greenwald, 1976), where the former treatment effects are confounded with the results of the first treatment. To address this potential negative effect, we follow a counter-balance repeated-measures design. The effect of the counterbalancing is to spread the unwanted variance arising from the treatment by practice or sequence interaction among the different treatments (Laitenberger et al. 2001).

Specifically, subjects (undergraduate and graduate students enrolled in business process information technology, information systems analysis and design, and advanced information systems courses) in each group were presented with a detailed scenario describing a specific business process (See Appendix A). One group of subjects was given an enhanced use-case description following Siponen et al. (2006) and an activity diagram for the business process using the standard UML Activity diagram approach (See Appendix B), then the group was presented with SARC conceptualization of the same business process (See Appendix C). For the second group the sequence of the treatment was changed to minimize the carry-over or learning effect.

Subjects were asked to identify elements of security in the models presented to them including the authorization constraints and security policies. A 30 minute cut-off was used to determine whether or not the subjects answered the questions
conscientiously. Only 84 responses out of 154 were useful (response rate 54.4%).

Specifically, to test the level security perception, the first level of situational awareness, subjects answered five questions aimed at identifying elements of security in the models presented to them including the authorization constraints and security policies.

To test the second stage of situational awareness, subjects were asked to explain plausible violations of access control requirements included in the detailed scenario. Subjects answered five questions aimed at identifying the reasons of security violations. Since comprehension involves some type of explanation power, we use a “why/because” type questions.

To test security prediction, subjects were presented with an access control violation scenario and were asked to predict how the business process conceptualization would prevent the threat from propagating through the business process. To assess security prediction, we asked “what would happen if” type of questions.

Analysis and Results

The descriptive statistics for each treatment are broken down into security perception, security comprehension, and security prediction items. Tables 3 and 4 present the minimum (Min), maximum (Max), Mean, Standard Deviation, Skewness, and Kurtosis for each treatment.

Table 3. Descriptive Statistics for the Enriched-Use Case combined with UML-Activity Diagram

<table>
<thead>
<tr>
<th></th>
<th>Min</th>
<th>Max</th>
<th>Mean</th>
<th>Std. Dev.</th>
<th>Skewness</th>
<th>Kurtosis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Perception</td>
<td>0</td>
<td>5</td>
<td>1.607</td>
<td>0.905</td>
<td>0.769</td>
<td>1.605</td>
</tr>
<tr>
<td>Security Comprehension</td>
<td>0</td>
<td>4</td>
<td>1.083</td>
<td>1.132</td>
<td>0.802</td>
<td>-0.187</td>
</tr>
<tr>
<td>Security Prediction</td>
<td>0</td>
<td>4</td>
<td>1.488</td>
<td>1.124</td>
<td>0.238</td>
<td>-0.970</td>
</tr>
</tbody>
</table>

Table 4. Descriptive Statistics for the SARC artifacts

<table>
<thead>
<tr>
<th></th>
<th>Min</th>
<th>Max</th>
<th>Mean</th>
<th>Std. Dev.</th>
<th>Skewness</th>
<th>Kurtosis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Perception</td>
<td>0</td>
<td>5</td>
<td>4.095</td>
<td>1.001</td>
<td>-1.448</td>
<td>2.971</td>
</tr>
<tr>
<td>Security Comprehension</td>
<td>1</td>
<td>5</td>
<td>3.654</td>
<td>1.023</td>
<td>-0.568</td>
<td>0.016</td>
</tr>
<tr>
<td>Security Prediction</td>
<td>0</td>
<td>5</td>
<td>2.547</td>
<td>1.206</td>
<td>-0.240</td>
<td>-0.200</td>
</tr>
</tbody>
</table>

A common rule-of-thumb for normality test is to compute the Skewness and Kurtosis values for the sample. Based on the Skewness and Kurtosis values, several cut-off points are suggested for normality test. For instance, the most stringent criterion is to use a range of -1 to +1 for Skewness and Kurtosis. In addition, some authors suggest a range of -2 to +2. And some more moderate authors suggest a range of -3 to +3 (Boneau, 1962). Based on those cut-off points for normality test, it seems appropriate to conclude that the collected data for both treatments fall within the normally distribution range.

Next, we had to ensure that there was no carryover effect before analyzing data from both treatments in the usual manner (Grizzle 1965). Carryover, residual, or learning effect is defined as the effect of the treatment from the previous time period on the response at the current time period. It occurs when the effect of a treatment given in the first time period persists into the second period and distorts the effect of the second treatment. Only if the preliminary test for carryover is not significant, the data from both periods are analyzed in the usual manner (Grizzle, 1965). Following Grizzle’s procedure to test for carryover effect, we conducted an ordinary least squares (OSL) analysis of variance test with a standard a-level of 0.05 to determine whether there is a carryover effect for the different stages of the security awareness and business process coordination.

We failed to detect a carryover effect for all three, i.e. security perception (p-value= 0.0614), comprehension (p-value= 0.1100), and for security prediction (p-value= 0.1068) for the different sequence of treatments. As a result, the order in which the treatments are applied (i.e.: Enriched-Use Case combined with UML-Activity Diagrams vs. SSeBP artifacts vs. SSeBP artifacts combined with UML-Activity Diagram) does not have an effect over the observed results for the security perception, comprehension, and prediction.

To test our hypotheses, we need to determine whether the mean of one group is statistically significant greater than the mean of another group. A paired t-test is suitable to test mean differences between two groups for repeated measures (Westgard and Hunt, 1973). In addition, t-test statistic is robust against violations of normality and homogeneity of data (Aron and Aron, 1994). We test our hypotheses using a paired t-test with a power level of at least 0.8 as a threshold value (Cohen, 1988). Studies with power levels higher than 0.8 have a high probability of rejecting the null hypotheses if they were false (Cohen, 1988). In addition, it is an accepted practice to set an α level of 0.05 to test hypotheses (Fisher, 1948). We adopt a power level of 0.80 and an α level of 0.05.

For H1, we empirically compared the mean of the 5 security perception questions for each treatment. Using a paired t-test, the data support H2a with a p-value<<0.001 and an observed power of 0.999.

For H2, we empirically compared the mean of the 5 security comprehension questions for each treatment. Using a paired t-test, the data support H2b with a p-value<<0.001 and an observed power of 0.999.

Finally, for H3, we empirically compared the mean of the 5 security prediction questions for each treatment. Using a paired t-test, the data support H2c with a p-value<<0.001 and an observed power of 0.999. Table 5 summarizes the hypotheses testing results.
4. DISCUSSION

Business process modeling methods are intended to support the capture, representation, organization, and storage of knowledge on the state of an organization. The use of formal process modeling methods provides standardized semantics and representation and forms a bridge between process analysis and design and process implementation (Glassey, 2008).

Hypotheses H1, H2, and H3 were all supported by the data. This demonstrates that SARC design artifacts assist subjects to identify security constraints in a business process. SARC design artifacts clearly represent who (agents/roles) has access to what (information resources) and under what conditions. In fact, when subjects used the SARC design artifacts treatment, they were able to correctly answer 82% of the security perception questions in comparison to only 32% when they used the Enriched-Use Case and UML-Activity diagram treatment. In other words, hypotheses H1 indicates that SARC design artifacts effectively represent access control policies that comply with inter and intra-organizational security requirements. This, in turn, shows that SARC design artifacts are more useful to subjects to decouple the association between agents and resources permissions and incorporates roles, permissions, access, and security of information and knowledge resources from the business process perspective. According to the situational awareness theory (Endsley, 1995), perception of relevant elements of environment is needed to comprehend and project their status within the near future. It is worthwhile to point out that although this finding relates to the security perception aspect of the security awareness, it is significant because it forms the basis for the security comprehension and prediction.

The support of Hypothesis H2 indicates that SARC design artifacts can be used to provide a better understanding of the different security aspects of a business process. Interestingly, when subjects used the SARC design artifacts treatment they were able to correctly answer 73% of the security comprehension questions in comparison to only 22% when they use the Enriched-Use Case and UML-Activity diagram treatment. SARC design artifacts can be used to explain why certain activities have particular permissions over an information resource and can be only executed by specific roles fulfilled by specific agents. In addition, SARC design artifacts assist subjects in understanding which resources are need to complete a specific business activity.

Finally, the support of Hypothesis H3 shows that SARC design artifacts allow subjects to make better inferences about future security states of a business process. Specifically, when subjects used the SARC design artifacts treatment they were able to accurately answer 51% of the security predictions questions in comparison to only 30% when they use the Enriched-Use Case and UML-Activity diagram treatment. Using SARC design artifacts, subjects were able to infer that when an activity did not have the right permission to read, write, or delete an information resource, the execution of the remaining activities may fail, as result the business process could not be completed. In addition, the finding from H2c shows how SARC design artifact can be utilized to perform what-if type analyses of security violations. In summary, business process models developed using SARC design artifacts generate a greater level of security prediction that those models developed using Enriched-Use Case and UML-Diagram.

In summary, subjects not only perceived SARC design artifacts to be superior, but also they performed better when they used SARC design artifacts to identify, comprehend, and predict security requirements and constrains of a business process. The experimental evaluation demonstrates that SARC design artifacts can be used to effectively represent security aspects of a business process. SARC design artifacts represents a method to effectively incorporate security requirements in the conceptualization of business processes, which in turn leads to a better understanding and awareness of how to incorporate security as a functional requirement in the modeling, analysis, and design of information systems that enable secure business processes within and across organizations.

5. CONCLUSION

When security requirements are incorporated as functional requirements in the analysis of business processes, analysts become more aware of security constraints and possible violations. Using the SARC conceptualization of a business process, analysts are able to better explain the current state of security of a business process. Should violations occur, analysts are able to explain the nature of security violation in terms of

<table>
<thead>
<tr>
<th>Hypothesis</th>
<th>p-value; Observed power</th>
<th>Supported/Not Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>H1: BPM developed using the SARC Artifacts creates a more accurate perception of security elements (i.e.: segregation of duties, non-repudiation, and authorization), in a business process than those using the Enriched Use Case and Activity Diagram.</td>
<td>p-value&lt;=0.001; observed value=0.999</td>
<td>Supported</td>
</tr>
<tr>
<td>H2: BPM developed using the SARC Artifacts creates a more accurate comprehension perception of security elements (i.e.: segregation of duties, non-repudiation, and authorization) in a business process than those using the Enriched Use Case and Activity Diagram</td>
<td>p-value&lt;=0.001; observed power=0.999</td>
<td>Supported</td>
</tr>
<tr>
<td>H3: BPM developed using the SARC Artifacts creates a more accurate prediction of the future security state of the business process, that those using the Enriched Use Case and Activity Diagram</td>
<td>p-value&lt;=0.001; observed power=0.999</td>
<td>Supported</td>
</tr>
</tbody>
</table>

Table 5. Testing results
segregation of duties, non-repudiation and authorization. In addition, analysts can use this understanding to predict the future security state of the business process in the event of a security threat. Security Awareness generated by SARC artifacts will allow business and systems analysts to minimize end-user related security faults and maximize the efficiency of security techniques. This is particularly important in the design of inter-organizational business processes, where the lack of security knowledge regarding authorized access to resources hinders the development of trust between the partner organizations.

6. ACKNOWLEDGMENTS
Our thanks to ACM SIGCHI for allowing us to modify templates they had developed.

7. REFERENCES

The “create order forecast” business process takes place between a retailer (buyer) and a manufacturer (seller) organization. The retailer and manufacturer work together to estimate future order needs. They determine the right products and quantities to be ordered for the next planning period. Accurate order forecasts drive sales increases, improve customer service, and support better inventory decisions. The process is triggered at the beginning of each planning period. Here, the retailer (buyer) consolidates its point of sales (POS) data and generates an initial sales prediction for the next planning period. This initial sales prediction information, along with the available stock, the promotions and event calendars (i.e.: weather, school season, holidays, etc.), and historical order shipment data is retrieved by the manufacturer (seller) and used to generate an initial sales forecast.

Now, the buyer and seller organizations use a collaborative information system to compare their initial estimates and reach an agreement. The collaborative system retrieves information on buyer inventory strategies, seller order shipment data, and collaborative policies (i.e.: Collaborative Planning Forecast and Replenishment (CPFR) policies), to identify any differences or errors in the initial sales forecast. The collaborative system produces exceptions resolution data, used to make adjustments to the seller and buyer sales forecasts.

**Appendix B: Enhanced Use Case (Adopted from Siponen et al. 2006; D’Aubeterre et al. 2008b)**

<table>
<thead>
<tr>
<th>Use Case:</th>
<th>Create Order Forecast</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scenario:</td>
<td>Create a new Order Forecast</td>
</tr>
<tr>
<td>Brief Description:</td>
<td>Determining the right products and quantities that must be ordered for the next planning period</td>
</tr>
<tr>
<td>Actors/Security Subjects:</td>
<td>Buyer and Seller</td>
</tr>
<tr>
<td>Security Classification of the subject:</td>
<td>All Data Sources are confidential</td>
</tr>
</tbody>
</table>
| Security Objects and Access Types to Security Objects: | Object: Buyer Forecast and Inventory Database (the buyer must be able to read and write sales forecast, point of sales (POS) Data, and to read Inventory Strategy)  
Object: Seller Forecast and Inventory Database (the seller must be able to read sales forecast, POS Data, Available Stock, Events Calendar, Historical Order Shipment Data)  
Object: Collaborative Planning and Replenishment Database (the collaborative systems must be able to read order shipment, CPFR policies, Inventory Strategy and Item Management Data. The collaborative system must be able to read and write the seller and buyer adjustment forecast and the order forecast) |
| Security Policy/Specific Security Restrictions | Buyer and Seller are only allowed to access security objects classified as confidential with the planning and replenishment department |
| Preconditions:    | All the Data Sources exists |
| Flow of Events:   | Actor: |
|                   | 1. The buyer generates and consolidates its point of sales (POS Data)  
2. The buyer generates the initial Sales forecast  
3. The seller retrieves the buyer’s POS data, available stock, events calendars, and historical order shipment data.  
4. The seller generates an initial Sales forecast  
5. The buyer sends its inventory strategy  
6. The seller sends the order shipment data and retrieve CFPR policies and Item Management Data  
7. The collaborative system generates the exceptions resolution data  
8. The collaborative system generates the adjustments to the seller and buyer Sales forecast |
| Exception Conditions: | If information about any object is not available, an appropriate error message is produced. |
Activity Diagram (Adopted from D’Aubeterre et al. 2008b)
Appendix C: Secure Activity Resource Coordination Diagram (Adopted from D’Aubeterre et al. 2008b)

Appendix D: Sample questions for perception, comprehension, and prediction of security requirements.

Security perception:
Who has permission to perform the Generate Exceptions Order Forecast activity?

a) Buyer Planning Analyst
b) Buyer Replenishment Analyst
c) Seller Planning Analyst
d) Seller Forecasting Analyst
e) All
f) None
g) It cannot be determined from the information given
h) I do not know

c) All analysts has permission to Create/Write/ Read the Exceptions Resolution information
d) Nobody has permission over the Exceptions Resolution information
e) It cannot be determined from the information given
f) I do not know

Security Comprehension:
Why? Because

a) The Buyer Planning Analyst has permission to Read the Inventory Strategy information
b) The Seller Planning Analyst has permission to Create/Write/ Read the Exceptions Resolution information

c) All analysts has permission to Create/Write/ Read the Exceptions Resolution information
d) Nobody has permission over the Exceptions Resolution information
e) It cannot be determined from the information given
f) I do not know

c) All analysts has permission to Create/Write/ Read the Exceptions Resolution information
d) Nobody has permission over the Exceptions Resolution information
e) It cannot be determined from the information given
f) I do not know

c) All analysts has permission to Create/Write/ Read the Exceptions Resolution information
d) Nobody has permission over the Exceptions Resolution information
e) It cannot be determined from the information given
f) I do not know

c) All analysts has permission to Create/Write/ Read the Exceptions Resolution information
d) Nobody has permission over the Exceptions Resolution information
e) It cannot be determined from the information given
f) I do not know

c) All analysts has permission to Create/Write/ Read the Exceptions Resolution information
d) Nobody has permission over the Exceptions Resolution information
e) It cannot be determined from the information given
f) I do not know

c) All analysts has permission to Create/Write/ Read the Exceptions Resolution information
d) Nobody has permission over the Exceptions Resolution information
e) It cannot be determined from the information given
f) I do not know

c) All analysts has permission to Create/Write/ Read the Exceptions Resolution information
d) Nobody has permission over the Exceptions Resolution information
e) It cannot be determined from the information given
f) I do not know

Security Prediction:
What would happen if the Replenishment analyst from the buyer organization does not have permission to perform the Generate Exceptions Order Forecast?

a) The Generate Exceptions activity would not be performed
b) The execution of the remaining activities would not be affected
c) The Generate Buyer Initial Sales forecast activity would not be performed
d) It cannot be determined from the information given
e) I do not know

Security Prediction:
What would happen if the Replenishment analyst from the buyer organization does not have permission to perform the Generate Exceptions Order Forecast?

a) The Generate Exceptions activity would not be performed
b) The execution of the remaining activities would not be affected
c) The Generate Buyer Initial Sales forecast activity would not be performed
d) It cannot be determined from the information given
e) I do not know

Security Prediction:
What would happen if the Replenishment analyst from the buyer organization does not have permission to perform the Generate Exceptions Order Forecast?

a) The Generate Exceptions activity would not be performed
b) The execution of the remaining activities would not be affected
c) The Generate Buyer Initial Sales forecast activity would not be performed
d) It cannot be determined from the information given
e) I do not know

Security Prediction:
What would happen if the Replenishment analyst from the buyer organization does not have permission to perform the Generate Exceptions Order Forecast?

a) The Generate Exceptions activity would not be performed
b) The execution of the remaining activities would not be affected
c) The Generate Buyer Initial Sales forecast activity would not be performed
d) It cannot be determined from the information given
e) I do not know

Security Prediction:
What would happen if the Replenishment analyst from the buyer organization does not have permission to perform the Generate Exceptions Order Forecast?

a) The Generate Exceptions activity would not be performed
b) The execution of the remaining activities would not be affected
c) The Generate Buyer Initial Sales forecast activity would not be performed
d) It cannot be determined from the information given
e) I do not know

Security Prediction:
What would happen if the Replenishment analyst from the buyer organization does not have permission to perform the Generate Exceptions Order Forecast?

a) The Generate Exceptions activity would not be performed
b) The execution of the remaining activities would not be affected
c) The Generate Buyer Initial Sales forecast activity would not be performed
d) It cannot be determined from the information given
e) I do not know

Security Prediction:
What would happen if the Replenishment analyst from the buyer organization does not have permission to perform the Generate Exceptions Order Forecast?

a) The Generate Exceptions activity would not be performed
b) The execution of the remaining activities would not be affected
c) The Generate Buyer Initial Sales forecast activity would not be performed
d) It cannot be determined from the information given
e) I do not know

Security Prediction:
What would happen if the Replenishment analyst from the buyer organization does not have permission to perform the Generate Exceptions Order Forecast?

a) The Generate Exceptions activity would not be performed
b) The execution of the remaining activities would not be affected
c) The Generate Buyer Initial Sales forecast activity would not be performed
d) It cannot be determined from the information given
e) I do not know