An Evaluation of BOF4WSS and the Security Negotiations Model and Tool used to Support it

Jason R. C. Nurse and Jane E. Sinclair
University of Warwick, Coventry, CV4 7AL, UK
{*jnurse, jane.sinclair*}*@dcs.warwick.ac.uk*

***Abstract*—As online collaboration between businesses increases, securing these interactions becomes of utmost importance. Not only must entities protect themselves and their electronic collaborations, but they must also ensure compliance to a plethora of security-related laws and industry standards. Our research has focused in detail on the cross-enterprise security problems faced by collaborating businesses. Apart from our most recent work which investigates a novel model and tool to support e-businesses' security negotiations, we previously defined a comprehensive development methodology to aid companies in creating secure and trusted interactions. This paper aims to advance those proposals by presenting and discussing a key stage of their evaluation. This stage uses interviews with industry-based security professionals from the field, to gather critical, objective feedback on the use and suitability of the proposals in fulfilling their aims.**

***Keywords*-Business-oriented framework, e-business collaborations, security negotiations, security ontology, XML security language, interview evaluation**

I. Introduction

Inter-organizational e-business, endorsed by a wide suite of enabling technologies (e.g., Web services, ebXML, RosettaNet), is now one of the most promising and lucrative business paradigms. To sustain these online interactions, security researchers and professionals have investigated numerous technologies, processes and best practices. Apart from our most recent research in [1], in previous other work we have also contributed to this area by defining the Business-Oriented Framework for enhancing Web Services Security for e-business (BOF4WSS) [2], [3]. BOF4WSS' uniqueness stems from its emphasis on a detailed cross-enterprise development methodology, to aid collaborating e-businesses in jointly creating secure and trusted interactions. This particularly refers to the creation of a multilayered security solution, which encompasses technologies, processes, policies and strategies, and spans the interacting companies.

Further to the comprehensive guidance supplied by BOF4WSS, our research has explored the provision of a range of useful support systems. These would assist in the framework's application to business scenarios, and seek to streamline various essential, but often arduous or problematic development tasks. One such support model and resulting system, which we recently developed can be seen in [1]; formally, this paper extends that work. That proposal specifically targeted the difficulties incurred during companies' negotiations on security actions and requirements; a prerequisite activity before the joint systems are developed. Here, a *security action* is defined as any high-level way in which a company handles a risk it faces (e.g., 'the risk of ensuring the security of a server is to be outsourced'), whereas a *security requirement* is a high-to-medium level desire, expressed to mitigate a risk (e.g., 'the integrity of personal data must be maintained'). Security actions thus encompassing security requirements.

The problem area highlighted above and discussed in subsequent sections, relates to the organizational, practical and physical hardships incurred when transitioning from the individually completed Requirements Elicitation stage, to the subsequent Negotiations stage in BOF4WSS. In this latter stage is where interacting companies meet to present, negotiate and reconcile their security actions and requirements. Attempting to address these hardships, the Solution Model and resulting tool for security negotiations support in [1] were created. These proposals specially aimed at streamlining various negotiations tasks and significantly easing framework phase transition for parties. Initial evaluation results in [1] and to a larger extent in [4] have provided a good start in demonstrating Model and tool compatibility with existing security approaches used in businesses.

Having defined the framework and outlined a key support tool in previous works, this paper aims to report on the findings from one of the more substantial, initial evaluation stages. This stage used in-depth interviews with industry-based security professionals from the field, to gather critical, objective feedback on the use and suitability of the proposals in fulfilling their aims. Another prime goal of this evaluation was to gain further insight into industry and business scenario realities before planning and conducting the final evaluation of BOF4WSS and the supporting tools. This final evaluation would constitute a thorough case study analysis.

This paper is organized as follows. Section II recaps BOF4WSS inclusive of its aims and the goals of its phases. This review was seen necessary in the interest of completeness considering the detailed analysis of the framework in the forthcoming evaluation. Work in [2], [3] form the main references for the framework's review. Next, Section III assesses the difficulties incurred in cross-enterprise security

negotiations, and discusses the Model and tool proposed to tackle them. With the main proposals outlined, Section IV reports on the interview-based evaluation of both the framework and the Model and tool. The feedback gathered will be an important finding regarding the use and suitability of the proposals. Conclusions and future work are presented in Section V.

II. The Framework

BOF4WSS [2], [3] is an approach for cross-enterprise security and trust within e-businesses that employ Web services (WS) technology. The prime novelty of this framework is found in its emphasis on providing an expanded formalization of a development methodology that focuses on security and trust. This methodology also accommodates multiple autonomous businesses working together. There are two main shortcomings of existing approaches targeted by the framework. These stem from: (i) an overly reliant emphasis on technology, alluding to standards and systems as the complete solution to WS security in e-business; and (ii) an overly isolated security stance, focusing on the process *one* company should follow to secure itself internally, therefore ignoring the cross-enterprise security issue (discussed in Hartman et al. [5]) introduced by WS use.

To address these outstanding issues, BOF4WSS aims at three aspects. First, to consider the full nature of WS and its security implications within e-business. Second, appreciating that security, irrespective of the context, is a multilayered phenomenon encompassing aspects such as practices, processes and methodologies, in addition to technologies. And finally, to promote the use of a collaborative approach to provide enhanced levels of security and trust across partnering companies.

As seen in [3] and depicted in brief below, the framework and its phases give detailed guidance on what should occur and how, and its pertinence in attaining desired levels of holistic security for these cross-enterprise interactions. This will involve defining the expected inputs to stages, along with their required outputs/outcomes, but especially the recommended low-level goals, activities, and steps within those stages that can help achieve the outcomes. Where suitable, this guidance aims to reuse existing methods and practices—both from industry and academia—thus concentrating on the compilation of these into a coherent, well-defined process.

With the framework's background discussed, Figure 1 displays a pictorial representation of its nine phases. These are then described.

The first phase is **Requirements Elicitation** and within it each business works largely by itself. The tasks conducted include analyzing internal business objectives, constraints, relevant laws, security polices and so on, to determine their high-level needs for the foreseen WS business scenario. Existing methods such as those proposed by Demirörs [6] are used to aid in this task. This technique (that is, [6]) focuses

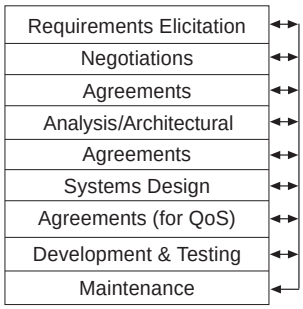

Figure 1. BOF4WSS Overview

on the definition and analysis of business process models to elicit requirements. This type of approach is preferred mainly due to its innate emphasis on business processes—the culmination of the expected service interactions.

In the **Negotiations phase** next, teams consisting of project managers, business and systems analysts, domain experts, and IT security professionals from the companies meet, bringing together their requirements from the previous phase for discussions. The purpose is to use the stage inputs as a basis to chart an **agreed** path forward especially considering the varying expectations each company is likely to have towards security. Expectations (and requirements) could vary with regards to whether a process (or set of service interactions) needs to be secured, to what level is it to be secured, how will security be applied, and so on. Work in [7] clearly highlights that in forming these partnerships of companies, this integration task is formidable. Nonetheless, this is a pivotal step in engaging in interactions.

The **Agreements phase** which follows, uses the completed negotiations to clearly define agreements thus far. The first task suggested by the framework is a legal contract to cement the understanding of the requirements between companies. This legal document is followed by a novel construct called the Interaction Security Strategy (ISS). The ISS as opposed to the contract, is a less rigid management structure that defines high-level, cross-enterprise security directives to guide the interactions. This would form the basis for all the scenario's security decisions instead of individual company's policies or requirements. Another prime goal of the strategy is fostering trust amongst business partners through predictability and transparency in security approaches, by outlining a structure that all entities agreed to adopt and follow. This trust aim is discussed in more detail in [3].

Within the **Analysis/Architectural phase**, the aim is to enable businesses to draw upon the previously agreed requirements and jointly define conceptual business process models for the expected interactions. The directives (policies, best practices, and so on) from the ISS are also then applied to create secure process models. This stage's expected output is a blueprint for the high-to-medium level

process flow and respective security architecture.

Following formal process definition, BOF4WSS advises the use of another **Agreements phase**. This time the goal is towards a more thorough legal contract reflecting detailed requirements and expectations of the companies involved. At this point, contracts are used primarily as a safety net, and should leave the role of governing day-to-day interactions to the ISS.

The aim of the **Design phase** is aiding businesses in defining a logical, low-level systems view of exactly how the conceptual model from the Architectural phase will be achieved. Examples of objectives that constitute this aim are the identification of relevant WS standards, trade-off analysis of their use, and the actual standards application where appropriate. In addition to standards agreement, harmonizing process and data semantics is also an issue worthy of consideration when discussing inter-company interactions as stressed in Papazoglou [8]. A semantics framework including shared vocabularies are therefore to be specified in this framework phase. On the completion of these tasks, the stage is complete. A specification document is therefore output that is appropriate for systems and software developers to implement.

With the low-level processes and functional services specified, the subsequent phase focuses on the **Agreements** at the lower, quality-of-service (QoS) level. The goal is to specify the mutual understanding of the priorities, responsibilities, and guarantees expected by each company regarding the actual Web services. QoS elements typically emphasized encompass performance requirements (e.g., average response time of 30 milliseconds),service availability needs (e.g., uptime of 99.96%), and so on. Apart from formal natural language statements which form what is commonly known as a Service-Level Agreement (SLA), this specification is done using relevant policy and service agreements WS standards such as WS-Policy.

The penultimate stage in the framework is the **Development & Testing phase**. This phase is largely carried out by companies individually, however occasional joint interactions are appreciated for testing, and system verification to previously established requirements. The input to this stage is the agreed systems design specifications (natural language and standards-based) and the service-level agreements. These documents are intended to be used by each individual company (and their personnel) to steer their internal systems implementation.

In the interest of supporting this internal process, the framework builds on current research and suggests the use of guidelines from more detailed and tested approaches such as [9], [8]. In the former work the goal is towards the development process for secure WS. Whereas, the latter article presents a lifecycle methodology that focuses on critical aspects such as application integration, migration from old to new Web services-based processes, and the 'best-fit' ways of implementation which appreciate company constraints, risks, costs and returns on investment. Another benefit to using these particular approaches is that information gathered and produced earlier in BOF4WSS can be reused to quickly complete their initial stages. Such data includes functional, security and QoS requirements, risk assessment data, and business process models. The last step in this phase is to verify that developed systems have achieved the requisite amounts of application-level security. To aid in this, an evaluation is advocated through the use of penetration testing and WS-specific approaches such as those presented in Yu et al. [10].

With the development of this multilayered security solution complete, its upkeep is the next crucial undertaking. BOF4WSS addresses this and other typical monitoring and preservation tasks in the **Maintenance phase**. This stage will involve functional system enhancements, but additionally will stress the continued updating and enforcement of security measures, both in developed systems and the ISS. Cross-enterprise teams both in terms of functional and security aspects are essential to this process. Regarding security specially however, they would be entrusted with monitoring the internal and external environments, and considering new threats, laws, and business requirements, and how these will be included in solution updates.

Having recapped the framework, the next section moves on to consider supporting the transition between two of BOF4WSS' stages, namely Requirements Elicitation and Negotiations phases. Specifically, the section assesses the difficulties incurred in cross-enterprise security negotiations during these stages, and discusses the Model and tool proposed to tackle them, and thereby support phase transition.

III. Supporting BOF4WSS and the Transition Between its Phases

A. The Stage Transition Problem

Sharing, comparing and negotiating on security actions and requirements across companies, even at a high-level, has always been a complex matter. Tiller's work ([7]) gives insight into this issue as he labels the related process, "security mayhem", because of the variety of security aspects (e.g., specific polices, service-level agreements, legal obligations, unique access requirements) to be considered in forming business collaborations. The reality of this problem is underlined by Dynes et al. [11] who set out a research agenda with a core question being: how can a shared vision on risks and security for interacting companies be achieved which appreciates their range of differences?

To investigate the specific issues surrounding stage transition and the negotiation of security actions as they pertain to BOF4WSS, a case scenario was used. This scenario featured companies using the framework during the Requirements Elicitation and Negotiations phases, and especially focused

on how security actions were determined, how these actions were documented/expressed, and how parties compared and negotiated on them. To strengthen the practicality of the scenario, security professionals knowledgeable in external company interactions were interviewed and their input used to guide case development. After defining the case scenario, it was analyzed to identify areas which proved difficult, problematic, or overly tedious for companies. Some of the most prominent areas are discussed below.

- **Understanding the security actions documents of the other companies "as is"**: In the Negotiations phase, companies supply their security actions to their business partners for perusal and discussion. A major difficulty even at this early stage was gaining an appreciation of what exactly companies meant (i.e., a semantic issue) when they outlined a security action or requirement in a few brief, informal statements, often with little justification. Included in this, is the reality that companies may use different terminologies for security actions, associated risks, threats, and vulnerabilities. These problems were further compounded by the variety of techniques (e.g., requirement listings, generic checklists, graphical representations) used by businesses to document their security actions. The core issues at this point therefore link to the *semantic gap* likely to be prevalent across companies, and the *disparity in formats* used to document actions. Both of these aspects resulted in the need for companies to spend considerable time and effort understanding actions and requirements before any negotiations could take place.
- **Understanding the motivation behind other companies' security actions and requirements**: From the summary documentation which constituted companies' security actions and requirements, it was often somewhat challenging for other businesses to determine exactly why that security desire existed. Even if the security situation/risk which the security action intended to address was included in the description, there might have been a plethora of other aspects (e.g., laws and regulations, security policies) considered in the preceding risk assessment that were not specified in the action description. These aspects are important because they provide insight into security actions that form the basis for companies negotiations. As a result of this *incomplete information*, companies usually had to enter further discussions to determine these aspects before making decisions on individual security actions.
- **Comparison of companies' security actions and requirements**: This task entailed parsing through other companies' actions and requirements documents to note and question any existing conflicts across businesses. Included in this task was the implicit or explicit matching of security actions from companies which targeted the same situation or risk. Even in the cases where security actions were classified into groups beforehand, the task of *parsing through documents*, and the various *back-and-forth communications* necessary to match and compare actions even at a basic level, resulted in the consumption of a vast amount of man-hours. An additional issue at this point was ensuring that all aspects motivating security actions (e.g., laws, security policies, contractual obligations) were gathered, documented and readily available for consideration, to support actual comparison and negotiations. Any streamlining of the aforementioned processes would save time, money, and effort for parties.

Having presented some of the core problems discovered from the case analysis, Section III-B outlines the conceptual Solution Model for the system to support stage transition.

B. Solution Model

The Solution Model, shown in Figure 2, contains four components: Security Actions Analysis, Ontology Design, Language Definition and Risk Catalogue Creation. The prime aim of this model is to outline a notional base on which a tool that would actually support the negotiation of security actions across companies, could be implemented. A description of the components is given below.

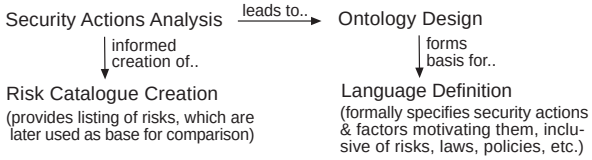

Figure 2. Solution Model

Security Actions Analysis: As a first step to addressing the problems related to the semantic gap and the disparity in formats used to document actions (identified in Section III-A), an in-depth analysis of the security actions and requirements domain was required. This assessment focused on security literature particularly in the security risk management field (as this area was viewed as key to determining security actions), and critically examined how security actions and requirements were derived. From that analysis, common critical factors, especially those that constituted and motivated their derivation were then identified. This component stage's findings allowed for a thorough understanding of that domain, and furnished the foundation for following stages.

Ontology Design: Ontologies are widely known for their ability to specify a shared understanding about a particular domain. In this case, an ontology was used to provide a common understanding of the security actions (and generally, security risk management) domain, based on findings from the Security Actions Analysis stage. Establishing this common semantic bridge was a critical prerequisite in creating the overall solution, when considering how different the terminologies, methods, and influential factors internal to each business were likely to be. It was also important

that the ontology was encompassing, and therefore allowed for an easy semantic mapping of concepts onto it from typical security action determination (or simply, security risk management) methods used by companies. Readers should note that the ontology designed here is high-level and mainly diagrammatic (i.e., there is no formal ontology language). As such, it is more of a communications tool, which can also be built on in future components. An ontology draft, and the Analysis component were previously presented in [12].

Language Definition: Two of the core issues identified in Section III-A center around the numerous formats used for security actions, and the incomplete information initially presented regarding the motivation for those actions. The Language Definition stage addressed these issues by defining a formal language to be used by companies at the end of Requirements Elicitation. The benefit of a formal language as opposed to a shared text-based template, or graphical representation is the automation it would allow; encoded data could now be processed by a machine. This language would enable the formal expression of parties' security actions, and the factors that motivated them (e.g., risks, laws, security policies and so on) in a common format. By having these motivational factors initially included and specified, this negates the need to enter lengthy discussions to determine these aspects later. An XML-based language was preferred to facilitate encoding due to its wide acceptance, XML's platform independence, and the variety of systems support options (numerous APIs for parsing and validation) available. To define the language's syntax, the ontology was an invaluable asset. Aiding in language definition was one of the original purposes of the ontology, as its use ensured that the language was grounded in accepted literature and supported by some common semantics across companies.

Risk Catalogue Creation: To address the problem of matching and comparing security actions across enterprises, emphasis was placed on identifying an aspect which was common to the actions and could be held constant. Therefore, regardless of the divergent security actions for a situation defined by businesses, a common underlying aspect could be used to quickly (or automatically) match these actions. After reviewing the Security Actions Analysis, it was apparent that in a majority of cases, security actions were established to handle or treat some inherent *risk*. The range of security action determination methods used by companies enforced this reality (see work in [12]). To provide the constant base therefore, a shared risks listing/catalogue was instituted and developed. This catalogue contained an updatable, extensive listing of security risks, and was used by companies as a common input to their risk management processes (i.e., the process that identifies, analyzes, evaluates, and decides treatment for the risks). Although businesses used different processes and derived possibly disparate security actions, they maintained a common base in terms of what risks were addressed by a particular action. Once implemented in a system, this common base would allow for the automated matching of security actions from companies, and thus ease the task of matching and comparing actions.

A general idea of how the implemented Solution Model worked towards significantly easing stage transition, is illustrated in Figure 3. In this diagram `Supplier` and `Buyer` are using BOF4WSS for an online business scenario.

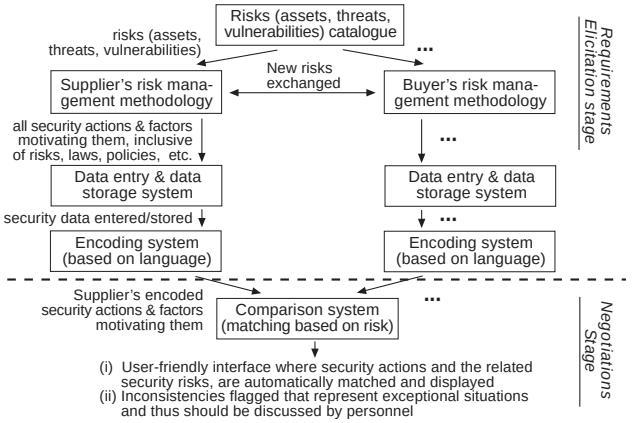

Figure 3. Solution Model in action

A briefly outline is now given on the conceptually implemented model in Figure 3. To begin, risks from the risk catalogue are selected by companies to form input to each entity's risk management methodology (i.e., process to determine security actions and requirements). Once companies determine their individual security actions, these actions and the factors motivating them are transferred into an Encoding system and marked up into the XML-based language defined. When businesses meet in BOF4WSS' Negotiations stage, the encoded documents are then passed to a Comparison system that matches companies' security actions based on the underlying risks they address. Currently, the output of the Comparison system focuses on (i) a user-friendly interface where security actions (supported by related risks, and motivational factors) are automatically matched and displayed, and (ii) flagging of any inconsistencies identified for follow-up by personnel. A noteworthy point is that the Solution Model and resulting tool are especially geared towards *shared* risks faced by entities. Therefore in some regards, emphasis is placed on the shared risks where companies have to agree on how they will be treated i.e., the type of security action (e.g., mitigation, transference, acceptance, avoidance), and actual action to apply. Section III-C formally introduces the tool which embodies the Encoding and Comparison systems above. This is the Security Actions Specification and Comparison System, hereafter SASaCS.

C. SASaCS Tool

1) Overview: The SASaCS tool represents the culmination of this work, in that, it is the software implementation of the Solution Model. SASaCS consists of all the practical components necessary to support the presentation, sharing, comparison and negotiation of security actions across companies. As a result of its tight coupling with the Solution Model, the general process outlined at the end of Section III-B applies to the tool as well. In Section III-C therefore, we provide more detail on the tool by discussing three of its features, the Data Entry interface, Comparison System report output, and the Encoding system (XML language). These aspects were chosen because they allow novel parts of SASaCS to be highlighted, and set the platform for evaluation in Section IV.

Once companies have conducted their risk management activities (which are informed initially to some degree, by the shared risk catalogue) and produced their individual security actions, the next task is transferring them into (their locally installed copy of) the SASaCS tool. This is handled by the Data entry and storage system. This system, shown in Figure 3, provides a set of simple, intuitive screens for users to input their security related data (e.g., risks, security actions and factors motivating them) and have it stored to a back-end tool database. To ease usability, the tool also allows the direct referencing and selection of risks from the risk catalogue, that initially factored into the company's risk management activities. Therefore, users can look-up risks from the catalogue, apply them to the current project/collaboration, and then annotate them, or otherwise use them as they see fit (e.g., input' risk priority levels, associate them with a security action, and so on).

As SASaCS is based on the ontology designed, its data entry screens benefit from the unambiguous definition of concepts (such as risk, risk level, and so on) prevalent with the ontology. The ontology diagram itself and its documentation also are useful in assisting users understanding of concepts, and linking data entry fields to output from their risk management methodologies. In addition to having data fields mirroring the basic concepts from the ontology, the Data entry interface defines a number of other fields to allow companies to add more detail on relevant aspects such as company-specific risk descriptions, justifications of risk levels, annotations regarding treatments of risks, treatment coverage levels, and security requirements. Figure 4 shows a screenshot of the security action (or in other terms, risk treatment action) data entry screen in SASaCS.

After each enterprise has saved their security- and risk-related data to the tool, the following step is encoding that data in preparation for inter-company negotiations. The Encoding system (also installed locally) facilitates this by pulling data from the tool database, marking it up in the XML-based language discussed previously, and outputting a document with the encoded data. When companies meet for negotiations therefore, (i) they use the same format to express security actions/requirements, which is also machine-processable; (ii) there is a shared understanding of the security- and risk-related concepts, promoted by the common ontology and highly supportive tool data entry screens; (iii) information is more complete as factors motivating security actions should initially have been supplied; and (iv) because encoded data (particularly security actions) includes references to risks in the risk catalogue, there are commonalities across companies' documents. The Comparison system uses these commonalities to automatically match security actions/requirements that treat the same shared risks.

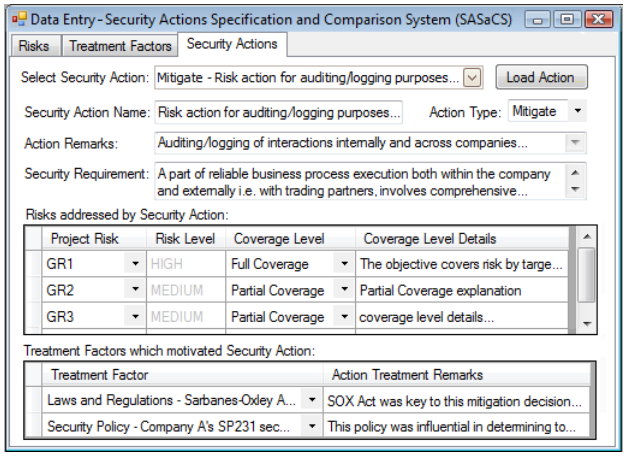

Figure 4. Security action data entry screenshot

As an example of the process mentioned above, let us assume two companies, `Supplier` and `Buyer`. Furthermore assume Figure 4 is a screenshot taken of SASaCS running at `Supplier`. There therefore exists a mitigation action formulated by `Supplier` to handle three risks, *GR1*, *GR2* and *GR3*. Reasons for their decision are listed in the treatment factors subscreen. At `Buyer`, assume that personnel only consider risk *GR1* and *GR3*; *GR1* they opt to mitigate, and *GR3* they choose to accept due to limited a security budget. By having all this information supplied in the system initially, when parties meet for negotiations, SASaCS can be used to quickly assist in various important tasks. One such task is automatically matching the disparate security actions of `Supplier` and `Buyer` based on underlying risks. Figure 5, which displays output from the Comparison system based on data above, exemplifies this. Here, companies are immediately notified of conflicting security actions (for example, in the treatment *GR3*), and situations where some entities do not address risks at all (in the case of *GR2*, by company `Buyer`). Additionally, businesses are instantly shown key reasons which motivated each company's particular security action decision (by way of treatment factors).

Streamlining these, at times simple tasks, can significantly reduce the time and effort needed by companies during the

Figure 5. Security action report output screenshot

initial stages of BOF4WSS negotiations. In the next section, we examine the encoding aspect more by presenting the XML-based language defined. For ease of reference, this language is called SADML, or Security Actions Definition Markup Language.

2) The Language: The structure of SADML was conceived to mirror the knowledge captured in the ontology (largely defined in [12]). As such, various ontology's concepts are represented as XML elements/tags. To comply with XML's hierarchical nature, it was necessary to define a sensible hierarchy of elements. Furthermore, this structure would need to accommodate one-to-many relationships across elements (for example, if a single law motivates/supports multiple security actions, this should be appreciated). Considering these and a few other salient aspects, SADML's syntax was defined. A snippet of the SADML format representing the information in Figure 4 is presented below; the + sign indicates additional data which is not displayed here for space reasons. The core language is described in the schema, indicated by `urn:risksx-schema` in the snippet.

```
<needsBase xmlns="urn:risksx-schema" ... >
  <mitigationActions>
   <mitigationAction>
    <name>Risk action for auditing/logging...</name>
    <details>Auditing/logging of interactions...</details>
    <risks>
+     <risk id="GR1">
+     <risk id="GR2">
+     <risk id="GR3">
    </risks>
    <lawAndRegRefs><lawAndRegRef idref="LR22">
      <relationToRiskAction>SOX Act was key to this miti-
       gation decision based on...</relationToRiskAction>
    </lawAndRegRef></lawAndRegRefs>
+   <securityPolicyRefs>
+   <securityRequirementRefs>
   </mitigationAction>
  </mitigationActions>
+ <acceptanceActions>
  <transferenceActions /> <!-- No actions defined -->
  <avoidanceActions /> <!-- No actions defined -->
+ <lawsAndRegs>
+ <securityPolicies>
+ <securityRequirements>
 </needsBase>
```

As can be seen above, `needsBase` is the root element and its sub-elements encompass the four general types of security action, and the main factors identified which motivate them. In practice, SADML groups risks by the *type* of security action (e.g., mitigation, or `<mitigationActions>`) which addresses them, and then the exact written action (e.g., `<mitigationAction>`) defined by a company. Because one security action can address many risks, each action has a `<risks>` element that lists the risks addressed. The elements suffixed with 'Refs' are used to indicate that existing motivational factors, for example laws and regulations (`<lawsAndRegs>`), influenced the treatment of a risk. `<securityRequirementRefs>` is the exception, in that it references security requirements (`<securityRequirements>`) that detail security actions. SADML's structure proposes one way to define security actions, risks and motivational factors, and does not intend to be a panacea in itself.

The novelty of SADML is rooted in the unique business perspective it takes on risks and security actions, which aims to (i) maintain a strong practical foundation (by mirroring the ontology designed) and (ii) place security, at least initially, at a level that understandable to security professionals and business-based decision makers (often the budget holders) alike. Next we cover existing work related to the Model and tool.

D. Related Work

In [13], authors assessed similar disparity problems to the Solution Model, particularly in communicating security requirements. They proposed a framework for formally specifying requirements and detecting conflicts amongst collaborating parties. The difference between that research and our work is in the layers which are targeted; the Solution Model supports high-level security negotiations for businesses, whereas Yau and Chen [13] consider low-level security requirements (and by extension, only risk mitigation), and formal rules and algorithms for requirements refinement. Their approach therefore is not actually concentrated on the problem which our work emphasises.

Apart from the related literature on the ontology previously presented in [12], the only other area with similar work is the XML-based language defined. In research and industry there have been a plethora of security languages covering from access control (e.g., XACML), to identity management (e.g., SAML). The most relevant to our work is the Enterprise Security Requirement Markup Language (ESRML) [14]. This language is comparable to SADML because it emphasizes the higher layers of security, and the sharing and exchanging the enterprise security information across companies for business purposes. The shortcomings of ESRML in terms of this work however are its lack of emphasis on factors which significantly influence or drive security actions (e.g., regulations, constraints), and its concentration on risk mitigation as opposed to explicitly appreciating other ways to treat risks.

Having now covered the framework and the Solution Model and tool, Section IV reports on the interview-based evaluation conducted on these proposals. This evaluation and its findings form the key novel contributions of this paper.

IV. Evaluation and Findings

A. Evaluation Method

To evaluate BOF4WSS and the Solution Model and tool, a standard structure of research was followed. This included the definition of areas of interest and then the collection and analysis of relevant data to assess these areas. Rigid hypotheses were not preferred because this evaluation does not seek to thoroughly prove or disprove formal theory. Instead, the aim is to establish whether the information gathered supports the areas and proposals assessed, and if so, the degrees of support arising from the data gathered.

There were two core *areas* to be investigated for support in this evaluation. First was to investigate whether the framework proposed is an applicable, practical proposal which would aid businesses in reaching requisite levels of enhanced inter-organizational security and trust. And secondly, to examine if the Solution Model and tool provide a viable process to greatly support transition between the Requirements Elicitation and Negotiation phases of the proposed framework.

To study these areas, a qualitative research strategy was chosen in which digitally-recorded, semi-structured interviews were employed. The interview data gathering technique was preferred as it allowed for a detailed study into the field and the gathering of descriptive, insightful data for analysis [15]. Semi-structured interviews enhanced this process because they allowed for a mixture of structure and flexibility in questions asked. Therefore, in addition to asking planned questions which directly related to the areas above, other interesting and associated observations could be explored.

To ensure the interview questions were clear and appropriate, pilots were used to refine them initially. Also, in the interest of gaining the highest quality feedback, interviewees were sent general documentation on the models at least a week before the interview. This allowed them time to review the proposals and gather their thoughts before the meeting.

As was mentioned, the target group for interviewees consisted of industry-based security professionals. To narrow this further, purposive sampling [16] (which is the use of special knowledge to select appropriate subjects) was applied. Within this general group therefore, individuals were selected that showed a good experience (demonstrated by job roles, certifications, qualifications, and past project involvements) in the following pertinent fields: Web services technology, e-business and online business paradigms, security risk management, information assurance, security architectures, and cross-enterprise interactions.

Specifically, the interviewee selection process consisted of directly contacting persons with demonstrated experience (identified from company Web sites and/or articles published), and also using the author's contacts within companies to help identify other relevant professionals. It should be noted that no special incentives for participation were offered and interviewees participated based on their own free will. This targeted selection technique was adopted as opposed to more statistically random or quasi-random techniques, to ensure that persons selected had a good degree of requisite experience and specialized knowledge.

Additionally, because the emphasis was on gathering in-depth information rather than surface-level data from as many persons possible, only five professionals were interviewed. These professionals however had a total of 48 years experience in the security field. This small sample size allowed for a manageable, yet very detailed amount of expert feedback to be gathered in the, on average, two-hour long interviews. Small sample sizes, greater depth of information, and a focus on narrative data all are key characteristics of purposive sampling [17]. Known limitations of this sampling technique however include possible bias in interviewee selection, and lack of wide generalizability of findings [16]. As there was no relation between subjects and the interviewer and as subjects were selected based only on demonstrated experience and no knowledge of their personal opinions, bias was not viewed as a serious limitation here. Furthermore, wide and conclusive generalizations are not the goals of this evaluation but rather to gain some insight into the use of research proposals. This wisdom might also then be applied in the next stage of evaluation, i.e., the case study.

Therefore, although there are noteworthy limitations of purposive sampling, the benefits possible with the technique were seen to outweigh the drawbacks in this case. This is especially considering the resource and time constraints on this project, and great amount of time taken even to set up interviews with the five subjects chosen. (Common

issues faced were the busyness and hectic schedules of professionals, coupled with the need for companies' legal departments to be involved to consider and approve the interviewee's participation.) Finally, to encourage honest and detailed feedback, the interviewees were told that their identities would be kept anonymous. This also avoided any more possible legal complications with their companies.

The overall goal of the interview process therefore, was to present BOF4WSS and the Solution Model (particularly, core characteristics, possible areas/scenarios of contention, novel aspects of them), and attain a real-life, expert opinion and in-depth insights. This feedback would delve into the applicability (how suitable are the models for the situations and problems they target, what might the response from companies be) and strength (how well, if at all, are the problems addressed by models, what are their benefits and shortcomings) of the proposals based on security professionals' real-world experiences.

Having conducted the interviews, recordings were then transcribed. To analyze the data collected, the content analysis [16] data analysis technique was then applied. This provided a standard method to code, organize, and index the transcribed interviews. Furthermore, it allowed for easy data retrieval, pattern identification and review, and basic counting to note any relevant quantitative observations [16]. A blend of deductive and inductive approaches to identifying themes in the data was favoured. This enabled themes to be identified which focused on the investigating of the areas for support (deductive) but also common themes that arose from data that were not conceived prior (inductive).

With the research process outlined, the next section concentrates on the presentation and analysis of the research findings. This research interweaves the findings and analysis stages because it was felt that this would allow for a rich but also concise discussion. Berg [16] supports the viability of this combined option especially when compiling reports based on qualitative data.

B. BOF4WSS

The first *area* to be investigated centres around whether the framework proposed is an applicable, practical proposal which would aid collaborating businesses in achieving desired levels of enhanced inter-organizational security and trust. To examine this, questions to interviewees concentrated on core principles and novel aspects of the framework which specifically aimed at addressing the outstanding research problems. Four *themes* have been identified in which to present and analyze the data gathered.

The themes consider: (i) the framework's emphasis on a highly collaborative approach to inter-organizational security, particularly where WS is concerned; (ii) the reality that BOF4WSS is detailed and at times prescriptive; (iii) the merit of the framework's focus on higher layers (business-level for example) of security in WS-based cross-enterprise interactions; and (iv) the use of the Interaction Security Strategy (ISS) as a comprehensive security management structure, that could also foster trust across partners.

Using interviewees' feedback, the themes are assessed in terms of their use and/or strength, and application. After theme analysis, an additional section is presented including interviewees general comments on the framework, before briefly summarizing the assessment thus far. In the presentation below, fictitious names are used for interviewees. This respects their anonymity while also allowing for a more vivid presentation of findings.

1) BOF4WSS and its highly collaborative approach: BOF4WSS emphasizes a highly collaborative approach to cross-enterprise security. This high degree of collaboration (manifested in dedication to working together, a good degree of information sharing, various meetings, and other time and investment commitments) was conceived specifically to address the shortcomings stemming from the isolated and individualistic approaches to securing e-businesses which use WS. Noting the amount of stress the framework places on this topic, it was chosen as one of the areas to evaluate within the interviews. The aim being to determine whether highly collaborative approaches such as the framework, might provide more adequate solutions for WS-based e-business interactions, as opposed to more individualistic approaches. The subsequent aim would be to then identify how applicable and practical such approaches are.

In response to questions posed regarding high degrees of collaboration as opposed to individual approaches to security, all professionals expressed that these types of approaches were preferred and yielded better security solutions. Interviewees indicated that solutions were likely to be more appropriate, skills and knowledge could be pooled, and finally systems could be designed and integrated more securely. This favourable opinion was upheld by professionals when questioned about BOF4WSS and its collaborative efforts towards security as well. An interesting point put forward by one professional was that collaboration (especially initial meetings and willingness to work together) enabled him to be able to determine whether or not other companies were really committed to interactions and security or not. Collaboration was therefore being used as a tool to learn about potential partners and even their security postures *before* entering fully into business interactions with them.

Considering collaboration in the context of WS and BOF4WSS, John, a security professional of 10 years working for a leading international IT and consultancy services company, noted that collaboration is essential and needed at all levels (business, legal, and technical agreements). Continuing the Security Architect said, "... particularly with Web services, it has great promise but it's only going to work with that sort of collaboration". This view hints to an importance of an increased amount of collaboration, even within the technology-driven WS world. Detailed feedback

from other interviewees supported the importance of collaboration between companies in achieving inter-organizational security. Existing case study data (see Todd et al. [18]) can also be referenced to see a glimpse of benefits of collaboration.

Even though supporters of collaboration, two professionals warned that it was important for businesses to maintain some degree of individuality (in terms of self-defense capabilities), or at least some safety net features (contract- or technical-based) within collaborations. These would protect individual companies if their partners inadvertently or intentionally became rogue. This point acts as a reminder that collaborative security approaches should not only focus on protecting the group of entities, but also protecting individual enterprises from risks of being in the collaboration (for example, see those raised by Baker et al. [19]).

Having looked at the use of highly collaborative approaches in building cross-enterprise security solutions, the next step was to assess the application and practicality of such approaches, and the framework in particular. From the feedback received, two opposing views were apparent. Three professionals regarded high degrees of collaboration across companies as difficult to attain, whereas the others saw it as "quite practical", and not "too big a barrier". The main proponent for the former perspective was Mark, an Information Assurance manager in a global telecommunications and consultancy firm.

Drawing upon his 20 years in the security field, Mark stressed that collaboration was beneficial to have, but very difficult to attain. Additionally, making persons communicate, work together, and readily share information (which are key activities in a collaborative process such as BOF4WSS) were not easy tasks. Prime reasons cited centred around stakeholder-related issues, particularly the likely problems incurred when meshing teams from different companies with possibly different perspectives, processes, systems, and organizational cultures. These issues are supported by literature in [20], [21].

Interestingly, John also showed an appreciation for the collaboration difficulties mentioned above but did not view them as too much of a barrier. Instead he noted, "yes it is intensive and costly to some extent and I think that's the only way to be really successful". In spite of these difficulties therefore, in his opinion, these approaches were not only practical but a necessity for success with security. Literature could be seen to support this 'security success via collaboration' perspective but primarily in closely knit business partnerships such as the extended enterprise (see Dynes et al. [11]).

Considering BOF4WSS in more detail, additional notable difficulties were identified by subjects relating to complexities in stakeholder arrangement and management (getting the right people together at the right time from across companies) and cross-border collaboration issues (in essence, normal collaboration issues exacerbated by ranges of cultures and perspectives) if/when the framework was applied internationally.

Speaking objectively, the aspects mentioned were somewhat overlooked in our creation of BOF4WSS due to the assumption that shared business aims, and goals for security would drive and support collaboration. When this assumption was put to subjects, some respondents agreed that shared aims would help. However, they also expressed that there would need to be strong, mutually understood benefits for all companies, degrees of fairness ("Nobody wants to be the weak partner", Mark stated), and executive sponsorship from businesses. High-value projects and situations where there was positive history (and existing trust) between companies were also cited as scenarios in which high degrees of collaboration would be more practical. All of these driving factors would have implications for BOF4WSS and indicate situations in which it might be best used.

As a brief summary to the information above, there was some consensus that the high degree of collaboration advocated by BOF4WSS would lead to a more adequate security solution for cross-enterprise interactions. According to the data however, its applicability may be limited (or at least, best suited) to business scenarios where either there is a strong commitment to businesses goals (and security is seen as an enabler to those), a substantial degree of executive sponsorship, they are high-value projects (amount stood to be gained or loss, motivated need to do whatever necessary to get job done), or there is existing trust between companies. The first two of these were previously mentioned in [2], [3] as criteria for businesses adopting BOF4WSS. Conversely, the need for positive history and some degree of existing trust between companies was not envisaged before as a prerequisite to adoption. This was a significant finding as it suggested that even though the framework was aimed at building trust across partners, some history or trust should already exist.

2) Detailed and at times prescriptive framework: In seeking to create a comprehensive security-focused methodology (which supported companies from the planning to maintenance of cross-enterprise interactions using WS), a central objective of BOF4WSS was to provide detailed, and occasionally prescriptive guidance. This guidance included the activities that might and should be conducted, possible ways in which they could be conducted, and their pertinence to attaining desired levels of layered security within the foreseen cross-enterprise interactions. With appreciation of the detailed level of guidance and the possibility that it might not be well received by companies, it was chosen for assessment in the interviews. The objective was to ascertain its usefulness and applicability in aiding the creation of a security solution.

From an analysis of the data, it was seen that a majority of professionals found the detail in BOF4WSS (exemplified

through the presentation of the framework's phases) of benefit to companies, and felt that enterprises would and should be open to it. Some of the benefits they quoted included the fact that detail would force people to consider all the factors, and give structured ways—especially for inexperienced persons—to solve security problems. Another benefit seen in the framework was the visibility and ability to audit, it would bring to all aspects of the cross-enterprise scenario. According to Matthew, head of Information Security and Risk Management at a higher educational institution, "An audit department would absolutely love this". This was stated because the framework would define a structure that audit departments, even though not security specialist, could follow and use to track and compare projects and other company interactions. It should be noted that Matthew has worked in other businesses in IT security roles previously. He also expressed that issues in core business and education (at his institution's level) were very similar.

The main warning placed on the framework by professionals was that it should be wary of being detailed and prescriptive to the extent that companies were not allowed to adapt parts to the nature/culture of their enterprise. This could relate to tools, specific techniques, or constituent methodologies. As is seen to some extent in Section II and largely in [3] however, the framework appreciates these issues and either provides a set of options (such as a listing of risk management methods to determine security needs), or relies on industry standards and best practices (including use of ISO/IEC 27000 for security or UML for modelling).

From the findings above therefore, it can be concluded that the detail provided by BOF4WSS should be useful to businesses and more of an advantage than a hindrance. This would not only apply to persons and businesses that lack experience in dealing with security issues in WS interactions within an e-business context, but also to entities seeking to have a framework to maintain structure, consistency and visibility in the overall process.

3) Appreciation of higher layers of security in cross-enterprise interactions: Another main aim of BOF4WSS is to emphasize holistic security solutions. Holism is used to refer to an all-encompassing approach that considers technologies, policies, processes, methodologies and best practices for security. This aim specially attempts to combat the overly reliant focus on technical mechanisms for security discussed in Section II. The purpose of this section therefore is to evaluate that aim and its merit in the context of cross-enterprise WS interactions.

Commenting on the data gathered, all interviewees displayed an appreciation of high levels of security and echoed the sentiment that technical approaches alone were insufficient. This finding therefore supported the framework's charter and literature in Singhal et al. [22] which highlighted the need for the higher layer of security with WS.

Speaking on this topic, John remarked that the challenge found in business today was achieving this higher level of engagement in projects, specially business ownership, and business and ICT alignment. Technology-level integration was not a problem but rather getting the engagement, involvement, and buy-in for projects at the higher business levels, security-related and otherwise. Lack of these higher level aspects, he noted, were the reasons many projects failed or stalled. Considering this challenge in terms of BOF4WSS, there is a focus on the higher layer, however no special mechanisms of encouragement to achieve it are provided. In the framework design it was envisaged that there would be a top-down drive for projects and therefore efforts were concentrated on supplying guidance for the necessary processes.

An additional concern lodged by two professionals was that even though the higher layer of security was important, the translation and implementation of these higher aspects to lower levels were equally important and not to be neglected. Paul, a Senior Security Researcher at another well-known global IT company, warned that various things get lost in translation and imperfect implementations. This can be to some extent supported by difficulties highlighted in [23], [24]. Furthermore, Paul stated that, "you cannot solve problems at the highest level, that's the thing, you do have to come down to the lowest level". As a result of these factors, he highlighted that it was key that security go through the entire process and the framework should maintain a balance between higher and lower layers to security, and not overly emphasis either. This was an accepted perspective in BOF4WSS as it aims for holistic security.

Continuing the assessment on the merit of higher layers of security, the next question to interviewees centred on trust, and whether this layer (and the activities therein such as jointly defining policies, agreeing on process for security, meetings and so on) in BOF4WSS might lead to increased trust across entities and their personnel. In response to this, a majority of professionals agreed on the likelihood of increased trust resulting. Common rationales presented linked to time spent together and commitment towards security that, once present, would be demonstrated to partners. Both of these could lead to relationship building, which then may lead to trust. Todd et al. [18] is one documented real-world scenario where high-level activities such as joint risk assessments, "proved to be the foundation upon which mutual trust between the security communities ... has been built" [18].

Mark was the least enthusiastic about the higher layer naturally achieving trust as he felt that trust was a very complex and difficult thing to attain—a view supported by Van Slyke and Bélanger [25]. This he attributed to human factors and the difficulty in predicting human behaviour. Aside from this however, respondents' feedback supported the possibility of increased trust across business partners.

4) Use of the Interaction Security Strategy (ISS): The Interaction Security Strategy (ISS) is one of the more novel parts of BOF4WSS, in that it seeks to create and apply a cross-enterprise management structure not found to be used in practice. The first question to interviewees therefore was to gather their opinion on this strategy in terms of security and trust. Another point of interest was how the strategy compared to existing approaches, particularly contracts, as these seemed to be the main agreements structure used today by companies.

The feedback gathered indicated that a majority of security professionals felt that the ISS was a valid and useful approach for cross-enterprise security and trust. Only Luke, a Senior Security Researcher with 4 years experience, disagreed as he was not sure about ISS positioning in the framework's process flow, or the level of security present in the ISS; he regarded it as too detailed.

One intriguing finding was that even though legal contracts formed the main agreements mechanism across companies, they were reported to cover security only very generally. For example, if in the UK or EU, they might only very briefly reference the Data Protection Act. Drawing on his 10 years experience, Matthew highlighted that contracts are not likely to cover security policies, continuity planning, or even ISO/IEC 27000 best practices. He emphasized that it was therefore important to have an extra layer of security (similar to the ISS) in place. Generally supporting this point, a 2010 survey [26] has highlighted that roughly 40% of large business respondents do not ensure that their contracts with third party providers include security provisions. This is a telling aspect in terms of contracts and their lack of focus on security.

Additional advantages of the ISS identified by some interviewees linked to the flexibility it would allow, and the pragmatic, actionable structure it provided over contracts. Contracts were seen to be very specific, hard to follow, and often expressed in legal jargon. The key stipulation made by subjects however, was that the ISS was always in line with the contracts. This, they stated, would ensure synergy in agreements. In general therefore, professionals' feedback above is seen to support the ISS as a key tool in creating and instilling a cross-enterprise security solution. This would enhance the practical security provided today and support agreements in contracts.

The second question related to the ISS concentrated on its use as a mechanism to foster trust across businesses. Trust was hoped to be achieved by making security approaches (pertaining to the scenario) more predictable and transparent (these being two key attributes of trust [27], [25], [28]). From the resulting interview data, a consensus was apparent as professionals all regarded the ISS as likely to foster trust. Reasons supplied included the clear guidance to companies, and the ownership and understanding it supplied personnel with, considering that they aided in its creation. Both of these aspects link with intended goals of ISS. John's support for the ISS in this regard was motivated by its charter towards a joint security posture, something that he felt was more conducive to trust, rather than the "us and them" mentality he saw in some businesses today. This opinion can be related to collaboration in general and the reality that some entities might not be willing to collaborate to this extent.

The other salient view on the ISS and trust was held by Mark. He expressed the view that,"[the ISS] probably fosters trust in that it takes away distrust ... What you'd certainly find is that one of the major hurdles is getting over the distrust, doesn't mean that you've actually got trust once you've got over that". This view, albeit a solitary one in the context of respondents, highlights the precarious nature of trust and possible difficulty in gaining it across persons and enterprises. In general however, the ISS is seen to positively aid in this venture and provide a structure that could enhance currently used mechanisms.

5) General thoughts on the framework: With the framework's core principles and novel aspects assessed, the next three paragraphs highlight other noteworthy feedback (based on consensus, ideas related to research literature, or simply practicality) given by interviewees.

One view that arose with respect to security frameworks and methodologies generally, was the inherent difficulty they faced in balancing complexity and being comprehensive, with making them useful and consumable by businesses. John aptly summarizes this opinion in his remark, "getting the balance right is so important where it's rigorous enough to add value and to make sense, make the process more structured, and at the right level but not so verbose that it's not useful". He further stated that even though the real proof would be in the adoption of the BOF4WSS, to him, it looked okay and seemed "light enough ... to be useful".

Another intriguing point which surfaced was that BOF4WSS did not appear to be specially suited to medium-to-high security or trust industries or business scenarios. Instead interviewees felt that it was generic and according to Matthew, "would be good across the board". This perspective was of interest because the framework was originally targeted at businesses and scenarios that emphasize trust and medium-to-high levels of security (see [2], [3]). These cases were chosen as they were seen to justify the significant effort and resources needed to adopt and use BOF4WSS. Based on the data collected however, the framework might have wider scenario applications, subject to limitations from other findings.

The final significant point relates to framework applicability again, but more from a higher perspective. In considering the application of BOF4WSS to scenarios, Paul expressed that asymmetries (whether due to size or bargaining power) in the market might limit the framework's use. This was because asymmetries lead to some enterprises looking to

develop solutions (usually individually) to service as many generic customers as possible. This was as opposed to focusing on one-to-one collaborations and individual partner requirements (such as purported by the framework). Albeit a notion only mentioned by one professional, the collaborative nature of BOF4WSS might suggest that it is better suited for symmetric-type interactions. These are interactions where each party has an influence, and party-to-party negotiations, design, and development is expected.

6) Summarizing framework analysis: Having presented and analyzed the main findings related to the framework, below these are briefly summarized and used to investigate the degree of support for the *area* highlighted at the beginning of Section IV-B.

The first area was the most debatable and investigated the high degree of collaboration desired by the framework. Based on the analysis in that section, collaboration was likely to lead to more adequate and thereby enhanced solutions than those possible with individual or isolated approaches to security. Additionally, it was also concluded that BOF4WSS (and to some extent, highly collaborative approaches in general) may be better suited to certain business situations and scenarios because of their nature (see the collaboration theme discussion for details). These findings strongly support the area being investigated, but limit the target scenarios of the framework.

Considering the level of detail provided by BOF4WSS, a majority of interviewers saw this as a benefit to companies which would, and should be welcomed. This was assuming that it allowed some degree of flexibility, which it can be said that BOF4WSS does (through the provision of various tool/technique options). Cited benefits of the framework included forcing companies to consider all the factors, aiding inexperienced persons (in what is arguably still a relatively immature field in terms of WS use for supporting complex business processes), and creating a level of visibility and ability to audit, for cross-enterprise development and subsequent interactions. These aspects can all be seen to enhance current security approaches and therefore provide good support for the area studied.

Reflecting on the appreciation for higher layers of security in the context of WS in e-business, data showed a consensus in their merit and value within the overall security approach and solution. The main concern identified at this stage related to getting the necessary level of engagement, at what is essentially the business layer within companies. This is a problem not covered by the framework as it was assumed the necessary top-down drive for projects already existed. This top-down drive would be present in the applicable scenarios suited for BOF4WSS, highlighted in the sections above.

On the topic of trust, a majority of positive interviewee feedback acted to further support the framework's appreciation of, and concentration on this higher layer. To recap, this layer involved getting companies together to interact, collaborate, and discuss and plan interactions security. Generally, these findings are therefore considered to provide a noteworthy degree of support for the area being investigated, both in terms of security and trust.

The ISS is in many ways a specialization of the higher layer security approach covered above, and interviewees also saw it as a useful approach in terms of cross-enterprise security. Its importance was accentuated particularly because there seemed to be no standard overarching management or guidance structure for businesses which pertained to security. Contracts were referenced, but it is known that these documents do not contain detail on security nor do they place it in an actionable language and context. Furthermore, findings indicated that trust between companies was likely to be fostered by the ISS. Interviewees linked this to the transparency and clear guidance for companies, and ownership and understanding implied as companies would have aided in the creation of the ISS. In terms of the area for support, the novelty in the ISS was seen to add to current approaches both in terms of security, and possibly also regarding trust.

Based on the preceding paragraphs and sections, it can be concluded that in the context of this evaluation, there is significant support for the framework. This support is with respect to providing an applicable and practical approach to enable businesses to reach requisite levels of enhanced cross-enterprise security and trust. Critically speaking, the majority of support for the use and viability of the framework, relates to business scenarios where there is either: a strong commitment to businesses goals; a great degree of executive sponsorship; they are high-value projects (and this value drives the need to do whatever necessary to complete the task properly); there is history and existing trust between companies; and there is symmetry in business interactions. Based on these characteristics and predefined target areas for the framework as defined in [2], [3], specific candidate companies that should benefit most from BOF4WSS adoption are:

- Large companies with smaller units (or subsidiaries) seeking to streamline online interactions using WS between these smaller units — As part of the same company, executive sponsorship and strong commitment from parent units would be a strong driver for smaller units to collaborate and bring interactions to fruition. These units would be focused towards symmetric collaboration therefore there would be the need for both parties to engage in context-specific negotiations, design, customization, and development. Also, assuming history between these units (given that it is the same company) there will already be a foundation of trust that can be exploited and built on.
- Partners in an extended enterprise setting, for example e-supply chains — Research in extended enterprises aided in the construction of this framework and a number of the criteria listed above meshes with needs

in these types of business networks. As trust is already a key prerequisite in extended enterprises [27], if a group of businesses in such a network desired to switch from proprietary integration formats to WS for cross-enterprise interactions, BOF4WSS would be very useful. The long-term nature of these networks and strong commitment towards a shared goal and mutual benefits also support the framework's use. Furthermore, because these businesses tend to already be collaborators at the strategic and business level, collaborations in security using BOF4WSS would be a natural next step to protect inter-organizational interactions and individual enterprises. Symmetric interaction would also apply.

– Small and medium-sized enterprises (SMEs) seeking to build long-term partnerships — This relates in particular to small and medium-sized companies with past history, a strong commitment to partnerships, sustained symmetric interactions, and the desire to achieve shared business goals realized using WS. BOF4WSS would be of great applicability to these type of companies for two reasons. First, because there might be a lack of expertise and experience, the framework's detailed guidance would be very useful. Second, as there are less stakeholders, stakeholder arrangement and management should be less of a problem. To justify the time and resources necessary by BOF4WSS, long-term alliances are likely to be the most practical scenarios. In such situations companies can see their investment yielding returns in the long-term.

The next section presents the findings and analysis conducted regarding the Solution Model and tool.

C. The Solution Model and Tool

In this section, the second core *area* is examined to determine whether the findings support it, and if so, to what extent. Specifically, this involves an investigation into whether the Solution Model and resulting tool provide a viable process to support transition between the Requirements Elicitation and Negotiation phases of the framework. Similar to the evaluation of BOF4WSS above, questions to interviewees assessed novel characteristics and core precepts of the Model and tool.

For the presentation and analysis of data, four *themes* have been chosen. These include: (i) opinions on transition problems highlighted; (ii) the premise that risks drive security actions and requirements; (iii) the likelihood of business partners sharing detailed information on common risks and their intended treatments; and (iv) the ultimate use of the Model and tool. Data within these themes is analyzed with respect to its application and scope. As with Section IV-B, there is a final section that summarizes the conclusions from the analysis completed.

1) Opinions on transition problems highlighted: The charter of the Solution Model was to address the transition problems that companies were likely to encounter in moving from the Requirements Elicitation to Negotiation phases in the framework. These problems were identified based on an informed case scenario and relevant research literature. Considering their importance as a driving factor for the Model however, this theme assesses the issues again with the goal of determining exactly how serious they might be from professionals' perspectives.

Commenting on the feedback received, all but one security professional—i.e., Luke—agreed with the transition issues highlighted. In response, Luke said he was unsure whether security would be considered at what he considered, an early stage in negotiations. In cases where there was agreement, professionals concurred with all of the transitional problems (such as semantics issues, difficulties understanding motivation for actions, and the arduous task of comparing and negotiating actions), and substantiated their opinions by drawing on past experiences.

In terms of semantics issues during phase transition, John stressed the importance of spending time initially agreeing on terminology in projects, as words in the security domain are often misused. Paul and Matthew were two of the main proponents supporting the reality of disparity in formats of security actions and requirements. Relating to this, Matthew stated, "there are companies that might have a basic statement, they might have a graphical representation, they might have a few bits and pieces and in my experience actually getting those to marry together initially, is one of the hurdles you do have to get over". These aspects can be compared to the security mayhem discussed by Tiller [7].

One of the most interesting findings in the data related to the motivation behind security actions and requirements. On this topic, John noted that in addition to partners not supplying (or supplying little) motivational information initially, if they were asked to justify actions at a subsequent stage, they did not always have good reasons to support their security actions. He explained that in some situations where standard security actions (such as reused action lists, or generic security checklists) were provided by companies, the original meaning might have be lost, or the security landscape might have changed. Therefore in addition to the problems associated with businesses not communicating the motivation behind security actions, the reality exists that companies themselves might not be clear about reasons for their actions. This adds an extra level of complexity and discussions as companies meet in the Negotiations phase.

Another noteworthy observation from the data was that personnel involved in cross-enterprise negotiations may not always have a security background—they may be business-oriented persons for example. Matthew felt that some personnel have basic knowledge of security aspects but because they lacked core knowledge and experience in security, this tended to prolong the negotiations process. This is important because it highlights that even though it may be desirable

for security experts to be involved in negotiation, that might not always be the case. This lack of involvement however can affect the negotiations process negatively.

The findings presented and analyzed in the previous paragraphs all help to support the reality of the problems faced as companies transition between BOF4WSS phases (or any general cross-enterprise negotiations task really). Mark's statement in response to the question about transition problems sums it up aptly as he expressed, "Oh, I've seen that, and you're exactly right, that is the way it happens, it takes months, possibly years in some circumstances". This quote captures the seriousness of the transition problems highlighted in this research.

2) Risks drive security actions and requirements: To ease difficulties in the initial matching and comparison of security actions and requirements across enterprises, the Solution Model proposed the use of a shared risks catalogue. A common risks base would be key to allowing for automated matching using a tool. Central to this proposal was the idea that risks are the core drivers for security actions. This notion was supported by literature surveyed in [12] and thus embodied in the resulting ontology. With appreciation of the importance of this notion to the Model and resulting software tool (that is, SASaCS), it was chosen for assessment in the interviews.

Reporting on the data gathered, a majority of professionals supported the 'risk-driven' notion. Feedback ranged from, "it always stems from risks and understanding risks, risk management, risk evaluation, it really drives everything to be honest", to "driving security, a risk-based approach something I firmly believe in". Cost factors were also mentioned by one interviewee but these still related to underlying risks and their mitigation cost/benefit savings. Interviewee feedback therefore can be seen to give support to findings in our previous work in [12].

While accepting the role of risks as a driver for security, one interviewee expressed that a number of companies do not actually operate on a risk basis. Unfortunately, no examples were given as to what companies might do instead to define their actions. This reality is nonetheless a thought-provoking one in terms of the Solution Model because even though it is not ideal (interviewees and research from [12] point to a risk-based approach being best), if it is widespread, it might limit the adoption of the Model and tool.

The last important finding related to the communications benefit likely to result in using risks as a base for security-related discussions. Interviewee feedback highlighted that in using a risks base, security professionals and business persons (involved in negotiations) alike could understand what was at stake (impact to organization and so on). From this research's perspective, this is beneficial for two reasons. Firstly, if business-level personnel do engage in security negotiations (as alluded to in the theme above), using a language they will understand would give them the necessary insight into the process. And secondly, business persons are typically the budget holders (John and Mark emphasize this) therefore again, they have to understand the need for security for funds to be released to implement security actions.

3) Likelihood of sharing detailed information on risks and risks' treatments: The Solution Model and BOF4WSS requires that business partners share a great amount of information on common risks faced, factors (including, laws, organizational policies, and so on) that influence/motivate security actions, and security actions themselves (whether they are geared towards risk mitigation or otherwise). With appreciation of the possible inherent difficulties accompanying this task (such as companies not wanting to share such information), this evaluation theme focuses on how realistic is it an expectation.

The conclusions from the data analysis in this segment were less clear, and even in cases where professionals felt that information sharing was realistic, they still placed a number of conditions on sharing. For example, some stated that once the data requested was at a relatively high level and did not go into specific vulnerabilities or impacts to the organization, it would be feasible. This was an intriguing finding because the structure of the risks catalogue and data in SASaCS does to some extent ask companies to define specific vulnerabilities that constitute a risk. This might therefore require the catalogue structure to be modified slightly to show less detail, or finding scenarios where parties were likely to be open and the structure could be accepted as is.

Supporting the opposite view, the feedback did observe that in some situations, companies might refuse to give much information to partners and cite confidentiality reasons. Overall however they were two prerequisites identified that would increase likelihood of information sharing. These were, trust and an existing relationship between companies. Mark states, "a lot of companies, particularly in private sector are unlikely to do that unless you've got that trust". This shows a significance of existing relationships and trust to the Solution Model, similar to that necessary for the framework.

4) The ultimate use of the Model and tool: The SASaCS tool is a software implementation of the Solution Model. As such, it aims to streamline a number of tedious, repetitive and long-winded tasks, and thus, significantly ease transition between framework phases. The evaluation of the Model, largely by way of the tool, was therefore imperative in these interviews. To conduct this evaluation, the tool prototype was demonstrated to interviewees and then questions were asked. Below the feedback and analysis results are presented.

In response to questions regarding the tool's usefulness in supporting phase transition, interviewees felt that it was a very useful approach and system. John stated, "I think it would be really useful. Having seen it, I think the penny

has dropped for me, I think this could be very powerful, very useful. I think this would help a lot". Furthermore he expressed, "And it would accelerate the adoption of technology solutions and this framework". John made this statement because he felt that in business today, collaborations are somewhat technology-focused and what inhibits projects is the discussion and agreement difficulties arising from the business and legal sides. The tool to him, was seen to help these sides by considering security at a higher level, communicable to people at this layer (business or legal professionals for example).

Mark was another professional who strongly supported the tool's usefulness. He commented, "a tool that helps bring that [core negotiation aspects] directly onto the table, it makes that time together far more productive". Such opinions as those mentioned here and above give evidence to support the increased productivity achievable by using the tool (and the underlying Solution Model proposed). Matthew reinforces these point as he states, "I can think of projects that it probably would have shaved off months, in terms of the initial stages of that project, had they thought to do this earlier on".

When questioned about whether they (interviewees) would use the tool in such a negotiations scenario, a majority of subjects said that they would consider it—increased productivity being cited as the prime factor. Proponents also stated that the novel benefit with the Model and tool was that they laid out companies' security positions in a clear and direct format, and forced them to agree or disagree on positions/postures. Regarding the automated identification of conflicting security actions for risks, John stated, "you almost know straight away that the collaboration is not going to work unless someone changes their posture or they agree to something". The tool can therefore save time for companies in this regard (a feasibility level) also.

From a usability perspective, generally positive feedback was recorded. Perceived benefits related to good accessibility due to the use of a browser-based report format, and the ease at which security actions from companies could be compared. Shortcomings mentioned included the need for increased flexibility in tool output (such as, additional buttons and more options on screen). These are accepted as areas for improvement in moving from a prototype to construct a full version of SASaCS.

Even though interviewees affirmed the tool's usefulness in significantly supporting the phase transition, some noteworthy shortcomings were identified. Critiquing on the higher level data present in the tool, Luke states, "it seems useful with the caveat that it might hide stuff away from the decision makers". To remedy this, he suggests a drill-down functionality to allow more detail to be seen on treatments or risks. This feature would be used by security professionals involved in negotiations, whereas business-oriented decision makers might be happy with the current higher level information. Speaking objectively, this is a useful suggestion but if implemented it would have to be optional. This is because, as was identified in the previous discussion theme, all companies might not be willing to share detailed information. Trust, to some extent, again becomes a factor.

Another observation mentioned was the dependence of the tool on the quality of the input data. "It is the input data's quality that is going to impact on the influence [of the tool]", Luke stresses. Matthew also supported this fact. To reply to this point, we accept it as an issue, however little can be done beyond giving guides and on screen tooltips to companies and users. It is assumed that companies would appreciate the productivity benefits when quality data is provided, and therefore use the Model and tool as suggested. Inadequate provision of information by some partners in a collaboration might even act as an indicator to other companies as to how serious partners are regarding collaboration and collaboration security.

5) Summarizing Solution Model analysis: In the following paragraphs, the findings presented and analyzed above are summarized in a *theme-by-theme* fashion. The conclusions drawn are then used to determine the degree of support for the *area* highlighted at the beginning of Section IV-C.

The first theme of analysis related to determining the severity of the transition problems that motivated the Solution Model's design. From the data, it was clear that a majority of professionals appreciated the problems (largely drawing on their own experiences), and viewed them as quite serious issues within projects. Additional issues were even highlighted relating to companies themselves not being clear on the exact motivation for security actions, and inexperienced personnel being involved in negotiations. Considering these points in light of the area under analysis, they can therefore be seen to support the seriousness of transition problems, especially relating to the great deal of time consumed, and lack of productivity.

The Solution Model operates on the premise that security risks drive security actions and security requirements. The validity of this premise therefore directly affects the viability of the Model and resulting system/tool. Based on the data, most professionals supported this premise and viewed it as the best way forward. Furthermore, it was seen to have additional uses because the notion of a risk was viewed as a key communications tool that could give business persons the necessary insight into security. One contrary point to risks as a driver was that a number of companies actually do not operate on this basis. Without any clear indication of a standard, well-justified process to identify actions however, little could be done to address this issue. With respect to supporting the viability of the Solution Model therefore, the data was seen to strongly support a risks base to security actions.

For the Solution Model to work, companies are required to share detailed information on risks related to the scenario,

influential factors in risk treatment, and defined security actions. On assessing the likelihood of that occurring, the analysis conclusions were not clear. Some professionals regarded it as realistic, whilst others did not. Possibly the most noteworthy finding here however was that trust and an existing relationship were cited as factors that might increase the likelihood of this information being shared. This is an acceptable prerequisite as it largely fits in with the updated target scenarios of BOF4WSS outlined at the end of Section IV-B. Assuming an atmosphere with trust and an existing relationship therefore, the interview findings can be seen to support an enhanced level of information sharing, and thus to some extent, the viability of the Model.

In investigating the Solution Model by way of the tool, the most significant question would have to be centred around the ultimate strength of the process and tool itself. In response to this question, professionals gave very positive feedback and affirmed the usefulness of the tool in significantly easing cross-enterprise security negotiations. The Model and tool were especially seen to accelerate adoption of technology solutions, and increase productivity and reduce time spent in negotiations. Furthermore, one professional saw it as beneficial to the overarching framework such that it would accelerate its adoption. This formed a critical point because it highlighted that research into support systems (such as the Solution Model and tool) could impact on the adoption of BOF4WSS.

Another important advantage is the fact that by requesting information on motivational/influential factors *before* companies meet, entities will have to find clear justifications to support their security actions. This directly helps to address the issues related to incomplete information and weakly justified motivational factors identified in the transition problems theme. Reflecting on the analysis area therefore, the findings and conclusions from this theme strongly support the viability of the Model and tool in supporting phase transition. There might be some slight improvements that can be made (including, drill down functionality, modifying structure of risks data in the catalogue and SASaCS) but these were not seen to seriously affect the use of the tool or viability of the Model.

In summary, the findings gathered provided a solid degree of support for the viability of the Solution Model in greatly aiding the transition between Requirements Elicitation and Negotiation phases of BOF4WSS. Trust and existing relationships between parties also played an important role, however this is acceptable as it coincides with the updated target scenarios of the framework.

Lastly, as this section represents the second evaluation of the Solution Model and tool (the first was the compatibility assessment in [4]), the findings and conclusions of the two evaluations were compared for any points of interest. One important observation was found. This was based on the fact that constraints (laws, obligations, policies, and so on) were seen as an additional driver of security actions in [4], whereas in this evaluation security professionals only mentioned risks. Although this leads to no clear conclusion, because the Model and tool by nature should be comprehensive, they should arguably accommodate both cases. Critically speaking therefore, the viability of the Model and tool can be regarded as negatively affected because currently they only use a risks base (and thus will only automate handling of risk-based security actions). Possible ways that constraints could be included in automated handling were previously discussed in [4].

Even though the negative feedback mentioned above harms viability, the strong support for the risks base and the tool in general supplied by industry-based professionals was felt to outweigh this aspect. Future work towards automated handling of constraints will be pursued only to ensure that the Solution Model and tool are as comprehensive as possible. This would allow them to handle a greater number of situations in which they are required to support cross-enterprise negotiations.

V. Conclusion and Future Work

In this paper we reported on the results from an evaluation conducted on two of our previous research proposals; namely, BOF4WSS and the security negotiations Solution Model and Tool used to support it. Generally, findings were seen to support the framework and Model/tool as useful, viable and practical approaches in addressing the issues they target. There were however some limitations, particularly related to applicable scenarios for the framework, and contentions regarding security actions and their core driving factors. These were important but not viewed as factors that seriously undermined these research proposals.

The next step of this research is to build on the insights and favourable findings of the initial assessments, and conduct the final evaluation process. This evaluation would constitute a thorough case study analysis where real-world companies would be observed using BOF4WSS and its supporting tools. This study would complement preliminary evaluations and allow for a much more comprehensive analysis. Furthermore, it would enable for clear, well substantiated conclusions to be drawn from this research.

References

[1] J. R. Nurse and J. E. Sinclair, "A Solution Model and Tool for Supporting the Negotiation of Security Decisions in E-Business Collaborations," in *5th International Conference on Internet and Web Applications and Services (ICIW)*. IEEE Computer Society, 2010, pp. 13–18.

[2] ——, "BOF4WSS: A Business-Oriented Framework for Enhancing Web Services Security for e-Business," in *4th International Conference on Internet and Web Applications and Services (ICIW)*. IEEE Computer Society, 2009, pp. 286–291.

[3] ——, "Securing e-Businesses that use Web Services — A Guided Tour Through BOF4WSS," *International Journal On Advances in Internet Technology*, vol. 2, no. 4, pp. 253–276, 2009.

[4] ——, "Evaluating the Compatibility of a Tool to Support E-Businesses' Security Negotiations," in *The International Conference of Information Security and Internet Engineering (ICISIE), under World Congress on Engineering (WCE) 2010*, vol. 1. Newswood Limited, International Association of Engineers, 2010, pp. 438–443.

[5] B. Hartman, D. J. Flinn, K. Beznosov, and S. Kawamoto, *Mastering Web Services Security*. Indianapolis: Wiley, 2003.

[6] O. Demirörs, Ç. Gencel, and A. Tarhan, "Utilizing business process models for requirements elicitation," in *The 29th Conference on EUROMICRO*. IEEE, 2003, pp. 409–412.

[7] J. S. Tiller, *The Ethical Hack: A Framework for Business Value Penetration Testing*. Boca Raton, FL: Auerbach Publ., 2005.

[8] M. P. Papazoglou, *Web Services: Principles and Technology*. Harlow, Essex: Prentice Hall, 2007.

[9] C. Gutiérrez, E. Fernández-Medina, and M. Piattini, "PWSSec: Process for web services security," in *The IEEE International Conference on Web Services (ICWS'06)*, Chicago, IL, September 2006, pp. 213–222.

[10] W. D. Yu, D. Aravind, and P. Supthaweesuk, "Software vulnerability analysis for web services software systems," in *IEEE Symposium on Computers and Communications*. IEEE Computer Society, 2006, pp. 740–748.

[11] S. Dynes, L. M. Kolbe, and R. Schierholz, "Information security in the extended enterprise: A research agenda," in *AMCIS 2007 Proceedings*, 2007.

[12] J. R. Nurse and J. E. Sinclair, "Supporting the Comparison of Business-Level Security Requirements within Cross-Enterprise Service Development," in *Business Information Systems*, ser. Lecture Notes in Business Information Processing, W. Abramowicz, Ed. Heidelberg: Springer, 2009, vol. 21, pp. 61–72.

[13] S. S. Yau and Z. Chen, "A framework for specifying and managing security requirements in collaborative systems," in *Autonomic and Trusted Computing*, ser. Lecture Notes in Computer Science, L. T. Yang, H. Jin, J. Ma, and T. Ungerer, Eds. Heidelberg: Springer, 2006, vol. 4158, pp. 500–510.

[14] J. Roy, M. Barik, and C. Mazumdar, "ESRML: a markup language for enterprise security requirement specification," in *IEEE INDICON*, Kharagpur, 2004, pp. 509–512.

[15] M. D. Myers, *Qualitative research in business and management*. London: SAGE, 2009.

[16] B. L. Berg, *Qualitative research methods for the social sciences*, 5th ed. London: Pearson International Education, 2004.

[17] C. Teddlie and F. Yu, "Mixed methods sampling: A typology with examples," *Journal of Mixed Methods Research*, vol. 1, no. 1, pp. 77–100, 2007.

[18] M. Todd, E. Zibert, and T. Midwinter, "Security risk management in the BT HP alliance," *BT Technology Journal*, vol. 24, no. 4, pp. 47–52, 2006.

[19] W. H. Baker, G. E. Smith, and K. J. Watson, "Information security risk in the e-supply chain," in *E-Supply Chain Technologies and Management*, Q. Zhang, Ed. Hershey, PA: Idea Group Inc., 2007, pp. 142–161.

[20] A. Baldwin, Y. Beres, S. Shiu, and P. Kearney, "A model-based approach to trust, security and assurance," *BT Technology Journal*, vol. 24, no. 4, pp. 53–68, 2006.

[21] F. Goethals, J. Vandenbulcke, W. Lemahieu, and M. Snoeck, "Different types of business-to-business integration: Extended enterprise integration vs. market B2B integration," in *E-Business Innovation and Process Management*, I. Lee, Ed. Hershey, PA: CyberTech Publishing, 2007, pp. 1–17.

[22] A. Singhal, T. Winograd, and K. Scarfone, "Guide to secure web services (NIST Special Publication 800-95)," National Institute of Standards and Technology (NIST), Tech. Rep., 2007.

[23] F. Satoh, Y. Nakamura, N. K. Mukhi, M. Tatsubori, and K. Ono, "Methodology and tools for end-to-end SOA security configurations," in *IEEE Congress on Services - Part I*. IEEE Computer Society, 2008, pp. 307–314.

[24] M. Tatsubori, T. Imamura, and Y. Nakamura, "Best-practice patterns and tool support for configuring secure web services messaging," in *IEEE International Conference on Web Services*. Athens, Greece: IEEE Computer Society, 2004, pp. 244–251.

[25] C. Van Slyke and F. Bélanger, *E-Business Technologies: Supporting the Net-Enhanced Organization*. New York: Wiley, 2003.

[26] PricewaterhouseCoopers LLP and Infosecurity Europe, "Information Security Breaches Survey 2010: Executive Summary," 2010, http://www.pwc.co.uk/pdf/isbs_survey_2010_executive_summary.pdf (Accessed 7 May 2010).

[27] E. W. Davis and R. E. Spekman, *The Extended Enterprise: Gaining Competitive Advantage through Collaborative Supply Chains*. Upper Saddle River, NJ: FT Prentice Hall, 2004.

[28] B. S. Sahay, "Understanding trust in supply chain relationships," *Industrial Management & Data Systems*, vol. 103, no. 8, pp. 553–563, 2003.