Towards A Model to Support the Reconciliation of Security Actions across Enterprises

Jason R. C. Nurse[†] and Jane E. Sinclair[§]
[†] Cyber Security Centre, Department of Computer Science, University of Oxford, UK
[§] Department of Computer Science, University of Warwick, UK
jason.nurse@cs.ox.ac.uk, jane.sinclair@dcs.warwick.ac.uk

***Abstract*—As an increasing amount of businesses look towards collaborations to gain a strategic advantage in the marketplace, the importance of systems to support these collaborative activities significantly increases. Within this area, arguably one of the most important issues is supporting interaction security. This is both at the initial, higher level of humans from businesses agreeing on joint security needs and the lower level of security technologies (communication protocols, VPNs, and so on). As there has been a substantial amount of work on the latter level, this work-in-progress paper tries to restore some of the balance by considering the problem of supporting companies at the business (and more social/human) level of interactions. We focus particularly on the initial tasks of negotiating and reconciling their high-level security needs. Our specific aim is therefore to explore the design of a model which replicates the human decision-making process with regards to the reconciliation of conflicting security needs at this higher level. The modelling of such a process is a prime area for research in the socio-technical field because it seeks to formalise several social aspects not typically modelled in a technical sense.**

***Index Terms*—Security actions and requirements; security risks; human negotiations; decision-making model; social aspects; interdependent security**

I. Introduction

The automation of security functionality at the lower level of systems and technologies has been commonplace for many years now. Security professionals and users alike can choose from various suites of security systems to automate everything from protecting themselves and their organisations from malicious attacks, to setting up secure communications with internal and external entities, and even negotiating and resolving potentially conflicting system security requirements and goals. Although there has been significant progress within this technical layer, it is fair to say that this has not been replicated when interacting at the business and more human level, and dealing with security there. In this context, security actions (i.e., ways in which a company responds to a set of one or more risks that it faces) are specified in natural language and are relatively high-level, rather than being formally structured and defined in a system-specific context.

One specific example of the disparity in technical and business layers is the difficulty in finding tools to automate (or at least, assist in) the, at times complex and arduous task, of comparing, negotiating and reconciling business-level security actions. At the technical level however, there have been numerous discussions and system proposals (e.g., [1–3]) on similar security interaction topics. These three activities are important particularly because they are central to progress in the initial stages of companies entering cross-enterprise collaborations such as joint ventures and extended enterprises [4]. The rationale for this disparity in levels is somewhat understandable and undoubtedly links to two aspects. The first one is the difficulty in specifying these actions (and the social factors supporting them) in a formal and highly structured way such that systems can process and reason on them. And secondly, there is the subjective and variable nature of each company's security needs. Nonetheless, given the benefits of supporting any automation of such negotiation tasks, we do believe it warrants consideration. These benefits relate to the time saved by businesses in negotiations, avoiding the mayhem [5] prevalent with such activities and the overall increased productivity likely to result.

In this paper therefore, we take the opportunity to build on favourable results from previous work [6, 7] on the similar problem of supporting security negotiations, and explore the development of a simple model to assist in the reconciliation of conflicting security action types. The classic example of conflicts is where one company wants to *mitigate* a particular shared risk (for instance, the risk that results from highly skilled attacks on Web services-based communications between parties), while its partners want to *accept* or simply *insure* against it. This could be because they do not view the risk as impactful or likely. We identify four action types (accept, mitigate, transfer and avoid [8,9]) as the focus of our work and define conflicts as areas where these types fail to correspond, thus highlighting differences in risk treatment.

As can be expected, there are numerous concerns and considerations in creating such an approach. Of these, probably the most intriguing is the question—how can a representative tool-based reconciliation be undertaken that would lead to credible decision support for conflicting security actions. As this is a key foundational part of the approach, this research question has been selected as the focus for this paper. The novelty of this work is twofold. First, is the attempt itself to allow some level of automation support in the reconciling of conflicting business-level security actions/decisions — complete automation is not the goal as we appreciate there are various aspects best handled by humans. Second, is the process that guides this task and the actual model. This process is different in that it aims to include several social decision

factors not traditionally incorporated in a mathematical sense and build a representative decision model.

To aid in answering the aforementioned question, Section II begins this paper with an analysis of how decisions – and particularly the security action reconciliation decision – could be formally modelled. Formal modelling is necessary as it allows for straightforward software processing. With a prospective decision model defined, a simple example is presented in Section III to demonstrate its application in supporting a reconciliation decision between three interacting companies' personnel. Following the example, there is a detailed discussion of some of the main issues which arose in modelling and overall limitations of the decision model to date in Section IV. As this is primarily a work-in-progress paper, it is these issues and limitations which are of greatest interest as they highlight directions for future work. In Section V, some first impressions on the decision model itself and its aims are presented and assessed. These impressions were gathered from security professionals in a round of semi-structured interviews. We then reflect briefly on the importance of trust to our research and the model in Section VI. Section VII highlights some related research while conclusions and avenues for future work are presented in Section VIII.

II. Decision Modelling

A. Scope

When businesses entering into an extended enterprise or partnership come together for initial negotiations, they are likely to have a number of security actions that conflict with each other. The questions that arise therefore are—how should companies proceed? And, whose security actions, if any, should be adopted? In previous research [6], we have studied a related problem in detail and defined a support model (Solution Model) and tool to assist security professionals from different organisations in initial collaboration tasks. The aims at that earlier stage were centred around collecting all the required security information and influential factors in decision-making before companies met, structuring that information appropriately, and consequently using the tool to produce informative reports to assist partnering companies in quickly identifying key discussion areas and making decisions on their joint security posture.

The objective now is to explore the extension of those aims to determine whether enhancements to the Solution Model and tool might be able to support some level of automated (system-based) decision-making. To allow for this, we aim to investigate the formalization of the manual decision-making process which companies' personnel engage in. Formalization here refers to defining the process using a mathematical model in which decision aspects, particularly the social factors which influenced decisions, are explicitly defined and quantified. Based on our prior research and discussions with security professionals, this decision-making activity consists of three core steps. Firstly, companies' personnel outline the factors supporting their security actions (i.e., aspects, social and otherwise, that dictate how they treat a specific set of one or more risks). Next, parties implicitly weigh and generally combine the importance and influence of those factors as they relate to the security decision (this is analogous to building an argument in support of their decision). Finally, analysts and security professionals compare security actions and their justifications (typically the strength of supporting factors and generally 'the argument') with other companies' respective decisions to ratify similar actions but more importantly, to reconcile any conflicting ones. Reconciliation may mean selecting one action (e.g., the one with the strongest argument) or defining an entirely new action which is satisfactory to all partners.

B. Building the Model

To assist in formalizing the security action decision process, the research field of decision making and specifically Multi-Criteria Decision Making (MCDM) is referenced. Apart from the obvious correlation, this field is seen to be appropriate for this work from numerous perspectives. These include the provision of structured methods to design mathematical decision models, a well-established literature base and finally, a process that appreciates decisions with multiple inclusive factors/criteria. Furthermore, MCDM models are recognized techniques to support decision making and guide decision makers towards identifying a preferred course of action [10, 11], a central goal of our work.

As it relates to decision modelling and the application of decision-making techniques involving numerical analysis, Triantaphyllou [11] identifies three essential steps. These are (i) determining relevant *criteria* (these are defined as the means used to judge an alternative) and *alternatives* (that is, final decision choices), (ii) attaching numeric values to the *relative importance* of criteria and to the *impacts of the alternatives* (also known as *performance*) on these criteria, and (iii) processing the numerical values to determine the ranking (preferences) of alternatives. Belton and Stewart [10] substantiate these steps but also supplement them by emphasizing the additional advantage of using numerical analysis to complement and challenge intuition. This thereby increases understanding of the problem and the final decisions made. This is also an interesting avenue for our work. Next, the three steps listed are used to define a proposed security-action decision model.

To complete the first step, we draw on the findings from [**?**, 8, 12, 13]. Based on these research articles, when making a decision on what type of security action a company should take to treat to a risk, salient motivational factors include Laws and Regulations of the host country, Contractual Obligations to other parties, Business Policies, Security Policies, Security Budgets (particularly, very limited ones) and the related Risk's Severity Level (typically classified as high, medium or low). Several of these (with the exception of risk level) we regard as social concepts that have not often been transposed to the technical world. In terms of the decision model therefore, these six factors can be seen to constitute the decision criteria; we accept that there are likely other factors but these were felt to be most generally appropriate. Using a similar process

and with appreciation of our higher level focus on action types, the alternatives identified were Mitigation, Acceptance, Transference and Avoidance security action decisions.

Having defined model aspects, the next step (according to [11]) is attaching numerical measurements. These are used for calculations and final ranking of security action alternatives. In MCDM, criteria values are typically used to represent relative weights of importance. For each criterion therefore, a value between 0 and 1 is to be stated that symbolizes the *relative* importance of the criterion to the decision maker. Relative means that values also relate to other criteria values stated such that their total sums to 1. The determination of criteria weights can be done in a few ways, but one of the most commonly used techniques is based on pairwise comparison. This technique was proposed by Saaty [14] and extensive discussions on it are available in [11, 14, 15]. At a very basic level, this approach focuses on getting decision makers to compare pairs of criteria according to importance and rank them on a defined scale. Normalization methods are then applied to derive relative weight values for each criterion. Standard questions in the technique are therefore, comparing criterion X with criterion Y, whether X is absolutely more important than Y, whether X is moderately more important than Y, whether X is equally important to Y, whether X is moderately less important than Y, and so on.

In terms of this research's security-action decision model, there are two options to determine criteria weights. The first option consists of each company's decision makers using the pairwise comparison technique and entering the values themselves. Saaty [15] supplies a comprehensive manual example, but such functionality could be built into any software/system we propose. This option has the benefit of directly drawing upon decision makers' perspectives and thereby possibly being a more representative model. Also, each company would have their own tailored weights. The second option also involves pairwise comparison but looks at the provision of standard or default weight values for companies' use, which are based on the security industry's knowledge (garnered using polls to professionals or security standard bodies). This bypasses the need for additional work by companies (in conducting pairwise comparisons) by relying on a generic weighting which could be held constant across collaborating parties. As these options each have their benefits, both are expected to be included in the model (and resulting software) at some stage. This would allow for flexibility in that, if businesses are more concentrated on understanding and having a representative model, they could use a pairwise comparison system feature. However, if they are primarily interested in speeding up the process and using common weights across parties, the second option's feature could be chosen.

To gather further insight into the pairwise comparison technique and generate some initial weights which could be used in our work, we applied it to determine the standard weights for the six criteria presented above. Considering the substantial detail present in this method, limited space in this paper and the fact that the final weights are of more importance and novelty to this research, we do not include the process here; readers are directed to [16] for detail on the method, process and value calculations. The respective criteria weights calculated are, Laws and Regulations (LR) at 0.409, Contractual Obligations (CO) at 0.285, Business Policies (BP) at 0.111, Security Policies (SP) at 0.116, Security Budgets (SB) at 0.053 and the related Risk's Severity Level (RL) at 0.026. The consistency ratio of 0.0982 indicates a good consistency of the comparison data entered and choices made (see [14] for more on consistency ratios).

Briefly commenting on the weights produced, one can see the great deal of importance associated with Laws and Regulations as they contribute just over 40%. Contractual Obligations are also key considerations with roughly 30%. A Risk's Severity Level or a limited Security Budget, however, only contribute relative weights of 2.6% and 5.3% respectively to a security decision. This was an interesting finding because even though Security Budget and Risk Level were crucial factors when looked at individually (if relying on *absolute* instead of *relative* weights for example), when compared to other criteria, they were often seen as notably less important. Similar to the Risk Level and Budget values, the Business Policies and Security Policies of companies only gained small relative values, 11.1% and 11.6% respectively. This was noteworthy from the perspective that even though policies dictate a business' mission and operations, legal structures such as laws, regulations or contractual obligations are always paramount. Objectively speaking however, these weights do not claim or profess to be perfect. Different decision makers may arrive at different weights and these are likely to all be valid given they are justified and maintain a good consistency ratio [14]. The reality that different weights will lead to different final decisions/outcomes is also accepted. The advantage of subjectivity in that case is that the final decision will reflect the opinions of the decision makers who defined the weights and therefore would cater more to their context.

Progressing from attaching numeric values to criteria, the next step is quantifying the impact (hereafter, *performance*) of the alternatives on the criteria. This seeks to define how companies felt about criteria as they pertained to a specific security action decision made. To allow for a more appropriate analysis and emphasis on criteria influence, there was a slight variation from the norm at this stage. Therefore, instead of the usual aim of determining how well an alternative fulfils criteria, the objective was determining how much an alternative was motivated or influenced by criteria. This change was not noted to have any negative side effects on modelling.

Unlike criteria weights, performance values are entirely supplied by businesses' decision makers near to decision time. There were two choices apparent in the literature ([11]) for entities to decide performance values. These were, pairwise comparison in terms of criteria (which leads to relative values) or allowing decision makers to specify absolute values. In the interest of not prolonging or further complicating the decision/transition phase for companies, the latter option was chosen. The Weighted Sum Model (WSM) [11] is an example

of a commonly used method that employs absolute values. For this research, absolute values in the range of 0 to 10 were allowed for entry by companies to define the extent to which an alternative was motivated by a criterion type. To ease usability for companies' personnel, a Likert scale [17] could be provided (in the model and resulting software) listing five items, each with corresponding representative absolute values. These are: 1. *Very Important* (score of 10.0), 2. *Important* (score of 7.5), 3. *Moderately Important* (score of 5.0), 4. *Of Little Importance* (score of 2.5) and 5. *Unimportant* (score of 0). In terms of a decision therefore, they would be applied, for example as follows: "The Sarbanes-Oxley Act (the criterion) was *Very Important* (the performance) in making the Security action decision to mitigate a risk (the selected alternative)". Another example of the use of this scale and the values will be shown in Section III.

The last step in Triantaphyllou [11] focuses on processing the numerical values to determine the ranking of each alternative. For this task, the WSM method of processing numerical data was used. Other methods were considered but proved either to be too complicated or to require too much information from decision makers for this research's context. The Analytic Hierarchy Process (AHP) [14,15] is a good example of a popular technique that was debated but later overlooked because of its heavy emphasis on pairwise comparisons to determine all input values (both criteria weights and performance values). That emphasis would require a level of user input that would most certainly not aid the initial negotiation on security actions across partnering companies. The formula for WSM (sourced from [11]) is presented below. This pulls together all of the aspects and values defined previously.

$$A^*_{WSM-score} = \max_i \sum_{j=1}^{n} a_{ij} w_j, \ for\ i = 1, 2, 3, ..., m. \quad (1)$$

Here, $A^*_{WSM-score}$ is the WSM score of the theoretically best supported alternative, n is the number of decision criteria (social and otherwise), a_{ij} is the actual performance value of the *i-th* alternative in terms of the *j-th* criterion, and w_j is the weight of importance of the *j-th* criterion. This formula can stand as the formal model to define the security action decision process, the $A^*_{WSM-score}$ score capturing which company's security action is best supported (has maximum value) and thus might be preferred. Below is a simple example using the proposals thus far.

III. A Situation Example

Assume a situation where there are three companies about to enter a partnership and they have conflicting business-level security actions for a particular shared risk related to maintaining the integrity and confidentiality of inter-organisational Web services-based communications. That is, `Buyer` is vying to mitigate it, `Supplier` prefers to accept it and `Distributor` wants to insure against the risk and thereby transfer it to an insurance company. Below, we list the factors behind each company's decision and also suppose that the performance values provided have been chosen by the businesses' personnel.

Factors supporting `Buyer`'s mitigation-based security action:

- If the related risk were to materialise, there would be a significant impact on the business and interactions with external partners. This leads to our rating of risk severity as High, and subsequent mitigation action. — Therefore, **Important** was selected to indicate that the Risk Severity Level criterion was Important in making the decision to mitigate the risk.
- Sarbanes-Oxley Act (SOX) of 2002 requires that companies should be able to confirm that only authorized users have access to sensitive information and systems. — Therefore, **Very Important** was selected.
- Our security policy strongly advocates the protection of the integrity and confidentiality of all potentially sensitive communications. — Therefore, **Important** was selected.

Factors supporting `Supplier`'s acceptance-based security action:

- There is very limited security funding and therefore we are unable to implement more comprehensive security measures at this point. — Therefore, **Very Important** was selected.
- From our risk analysis, it has been deemed unlikely that this risk would materialize as existing basic authentication measures are thought to provide adequate security. — Therefore, **Very Important** was selected.

Factors supporting `Distributor`'s transference-based security action:

- Our security policy states that security risks to confidentiality of company data classified as Private, must be handled. — Therefore, **Important** was selected.
- Cutbacks in the company have led to an extremely limited security budget for this year. — Therefore, **Very Important** was selected.
- A law exists that emphasizes that risk should be handled. The law permits that handling via insurance is an allowable alternative. — Therefore, **Important** was selected.

The following decision matrix puts the data above, criteria weights and respective performance values into context.

	Criteria					
Alternatives	LR (0.409	CO 0.285	BP 0.111	SP 0.116	SB 0.053	RL 0.026)
Mitigation	10	0	0	7.5	0	7.5
Acceptance	0	0	0	0	10	10
Transference	7.5	0	0	7.5	10	0

To apply the WSM formula, the scores for the three alternatives are:

$$\begin{aligned} Mitigation = &\quad 10 \times 0.409 + 7.5 \times 0.116 + 7.5 \times 0.026 = 5.155 \\ Acceptance = &\quad 10 \times 0.053 + 10 \times 0.026 = 0.79 \\ Transference = &\quad 7.5 \times 0.409 + 7.5 \times 0.116 + 10 \times 0.053 = 4.4675 \end{aligned}$$

Therefore the best supported alternative (in the maximization case) is Mitigation, `Buyer`'s choice. The SOX Act (a law) supporting their decision being a key reason due to the large weight assigned to the Laws and Regulations social factor.

This example presents a simple application of the decision model defined. From that illustration, it is apparent that the model works on the basis that the action with the 'strongest' support is preferred. This seeks to be similar to the manual negotiations process where the best justified or supported action is chosen. The next section continues discussion of the proposed model and presents its most notable limitations and thus, areas for analysis in future work.

IV. Discussion and Limitations

One of the greatest novelties about the proposed model is that it tries to formally accommodate a number of previously under-represented social factors in the decision process. This advances existing literature and approaches where primarily, only risks and risk levels were scored and valued. Whilst it is understood that risks allow the easiest formal and numeric (especially monetary, in terms of loss potential) definition, the various other high-level and social factors in a security-action decision process should also be considered. This research attempts to provide a logical start towards a model that aims at the high-level inclusion of such factors. Having discussed the proposed reconciliation model in the previous section, its main limitations are now outlined. These highlight known practical limits in the decision model, but additionally areas that surround the further formalization of crucial decision factors. We focus especially on the model's internal restrictions rather than the external data-entry component where companies' personnel are required to input values for weights and performances. We do nonetheless appreciate that this also forms somewhat of an issue in terms of at what points data are input, who inputs that data, how does one arrive at the measures, and how does one ensure values are representative. Other ongoing research is considering these aspects.

The first general limitation of the decision model is that it does not account for multiple factors/criteria of the same type. For example, if a company has four laws supporting a security-action decision instead of one, the model should reflect this, potentially by a greater weighting or performance value. A greater influence or 'argument' would be the likely behaviour in real-world negotiations. Currently however, the decision model does not. Possible solution options to accommodate this include having extra parameters for each additional factor, or building such aspects into the performance Likert scale. For example, only allowing *Very Important* to be selected if three or more factors/criteria of the same type support a security action decision. This aspect therefore needs to be considered further. An additional issue in dealing with laws (and potentially one or two other external factors) specifically, is that if a law prescribes a particular treatment for a risk, that treatment has to be adopted, there is no need for further comparison or room for negotiation. Where two or more companies have laws supporting different treatments therefore, the model/tool would not be able to process this case and would therefore need to fully defer the reconciliation task for that risk to businesses' personnel.

Another potential restriction of the model is that it regards decision alternatives in an isolated manner. For example, assume there are ten companies in a scenario, nine desire to transfer a risk, but one company opts to mitigate it. Furthermore assume that the mitigation company has the maximum calculated value (that is, $A^*_{WSM-score}$). According to the model, all companies should adopt this decision. Even though this occurrence is a possibility, in the real-world it is probable that majority vote might triumph. One way to tackle the isolation issue might be to sum decision values from companies with the same security action type. Then, compare these totals and choose the action with the maximum value. Provided the nine businesses above had a summed total greater than the total of the one, their action type would be selected. Albeit accommodating, there is one caveat to even this technique however. This lies in the reality that the majority vote might always prevail even in situations where it might not be best. Future work would therefore have to investigate, monitor and balance this carefully.

The next limitation relates to the complexities of the security-action decision process and the interrelation between its components not encompassed by the model. An example of this is a situation where a company has a single action that addresses ten security risks. Arguably this action should receive an increased weighting or performance value simply because of the fact that it covers so many risks; its removal therefore would potentially lead to ten risks being untreated. The problem in the model here is that it focuses on security actions on a risk-by-risk basis and not more generally as is possible in actual interactions. There is also the argument that the specific risk or specific risk's severity level plays a part, instead of just noting the generic Risk Severity Level criterion. Thus, possibly in situations where a risk has a severity level of 'High', this should be given a slightly greater (or lower, depending on the context) weighting than where a severity level of 'Low' supports a company's security action decision.

Additionally and more from an interrelation perspective, the model does not support links across social factors, risks or treatments, nor is it retrospective. Concerning the last point, the model can suggest that companies mitigate a risk instead of accept it, but it does not look at the impact that decision might have on other risks or factors. For example, such a decision might mean that there is less budget (money) to spend on mitigating another risk, therefore that other risk may now need to be avoided or accepted by the collaboration. These are complex issues not addressed by the model as yet, but which represent actual negotiations and discussions. Further comprehensive work is needed in this area to see how these aspects can be captured and to what extent.

The last debatable aspect of the model relates to decision makers. In MCDM techniques, there is typically a single, or group of decision makers concentrating on a specific decision. If it is a group, they first need to agree on input values

(typically through consensus or voting) then enter them into the approach. The approach processes these values and selects a preferred alternative based on maximum scores. The same decision makers therefore provide all the input values. In this research's model however, each company may go through the decision-making process individually and then at the end supplies their security action summation score (formally, $\sum_{j=1}^{n} a_{ij} w_j$) to the system. This score is then compared with other companies' decision scores regarding the same risk and the maximum is chosen as the preferred or best supported alternative. Therefore, different decision makers supply input values. Although the use of separate decision makers seems like a useful and valid application of the MCDM technique, no literature could be found which also applies it. Further work therefore should encompass the evaluation of this particular application and its ultimate viability.

To briefly summarize this reflection section, there is still a great deal of work to be done in creating a highly representative, formal decision model. This paper has provided a well-grounded start to that process by identifying a basic model which included a number of previously under-represented decision factors particularly from within the social context. Even though these factors are difficult to value and accommodate, they form key parts of the decision process and should be duly represented. In looking towards any level of automated reconciliation support therefore, the biggest challenge will be in identifying the minimum level of data input and time commitments necessary, which leads to the greatest, most useful security-action reconciliation assistance. After all, the focus is easing phase transition and not complicating or prolonging it further. There must also be an appreciation however that on occasion, even small levels of automation will simply not be possible or feasible. For example, take the situation where two or three companies have mandatory laws that support conflicting security actions. Or, consider the case where companies have very high scores or very close total scores. Boundaries will be needed in the system to flag these situations and for further discussion by personnel.

Finally, as identified previously, there is additional scope beyond reconciliation for aiding understanding of security-action decisions. Weighting and performance data provides a rich source of information which explicitly defines companies' perspectives. This information could be used to support complex or detailed negotiations processes, as opposed to streamlining security negotiations.

V. First Impressions on the Decision Model

The creation of a decision model that replicates the human decision-making process with regards to the reconciliation of conflicting security needs was explored for several reasons. Firstly, the novelty of such a model itself that especially aims to include a number of social decision factors not usually incorporated in a formal or mathematical sense. Secondly, the favourable feedback on current research [6, 7] which forms an ideal basis for the model. Finally, there is the additional time likely to be saved by businesses in negotiations and the overall increased productivity that could possibly result if any level of automation in the decision-making process could be achieved. The last of these points was especially relevant noting the importance placed on time and productivity by security professionals in [6]. This is an interesting proposal from a research perspective, but because this tool is ultimately aimed at industry use, gaining some real-world feedback even at this early stage would be very useful. This would help to put the proposals into a practical context and give a first impression regarding feasibility. To attain real-world feedback on the decision model therefore, questions on the model and its aims were posed to five security professionals in separate interviews. The interviews were of a semi-structured nature and lasted for around 15 minutes. Professionals possessed a total of 48 years experience in the security field and had all previously engaged in cross-enterprise security negotiations. Below a brief analysis is conducted on the feedback gathered. Fictitious names are used to preserve the identities of the participants and any link to their employers.

At a general level, security professionals regarded the notion and process of a model for reconciliation as 'interesting', but expressed that a great deal of analysis and proofing would be required. John, a security professional of 10 years working for a leading international IT and consultancy services company, summed up interviewees' views in his statement, "it's an interesting idea, but the exact nature of the formula or the risk factors, how that would work, I think I'd want to see more examples, to prove to me that it works and makes sense". Finally he added, "but I think it's an interesting idea worth exploring". This and similar views from most professionals are taken to support the feasibility of future investigations towards modelling and potential levels of further automation.

There was a single view not in support of fully automated reconciliation. This came from Mark, the most experienced security professional amongst interviewees. He strongly felt that the goal should be towards modelling to aid in decision making and complementing understanding—not therefore, in providing definitive answers for security. Mark stated, "I'm not a firm believer in, you press the button for risk assessments and you get the answer out". This opinion was likely due to Mark's view that risk assessments and some aspects of security were an art and not a science, therefore human aspects still need to be present. This is a salient point as it provides a reminder of the continued need for some human presence even in this level of the negotiation process. Furthermore, it alludes to the possibility that the real use of our model may be more towards assisting understanding of the decision process. This is rather than any attempts, although not foreseen, towards full automation.

Lastly, professionals agreed with the general set of social factors included in the model and were unable to identify any other core ones. They also concurred with the notion of *degrees of importance* of social factors/criteria (such as Laws or Policies) in terms of a security-action decision. For example, a relevant law may influence the treatment of a risk more than a related security policy. Interviewees' agreement

therefore acted to directly support the reasoning behind the performance or impact values (i.e., the Likert scale) discussed prior.

In summary, a majority of interviewees viewed the proposal as interesting, but noted that it required a great deal of analysis and validation. The main opposing perspective referenced the need for humans to actually make the reconciliation decisions (instead of a tool). This opinion was linked to the perception that risk assessments and aspects of security are more of an art (therefore somewhat subjective and mutable) than a science (strictly defined). This is a very valid and salient perspective and therefore future work is expected to concentrate slightly more on modelling for decision support and not towards expert or fully automated systems. Even if tool-based reconciliation is not used for definitive solutions to security conflicts, a model and tool that could present an initial solution that would then need to be ratified by a human, would support negotiations more than the existing research [6] currently allows. In the next section, we consider the notion of trust and how it relates to and influences the success of the model.

VI. The Trust Factor

Similar to any other negotiation or joint decision-making process in businesses [18], trust is paramount in our work. If partners are to realise any benefits, including increases in productivity or faster negotiations, from use of the model and tool, there must be good levels of trust and information sharing across entities. Trust touches several aspects of the model and reconciliation process, but generally these fit into two categories: trust in the information that business partners provide and trust in the tool's security-decision output. General discourses on trust and information trustworthiness can be found as necessary here [18, 19].

At the level of business partnerships, trust has always been crucial. For the model to function properly, firstly there must be trust that partners will include only pertinent social factors to support their security-action decisions. Including irrelevant factors would inaccurately inflate the respective partner's security action score, to the detriment of other partners. Likewise, there must also be trust that collaborators will supply correct criteria weights and representative performance values. Rating all aspects with very high performance, or reverse engineering the system to define highest criteria weights for the business' security actions is counter-productive and can only serve to hurt the partnership. If businesses identify any suspicious input values from partners or one-sided tool output, they are encouraged to follow these up with the respective company. Any evidence of system or model coercion may be taken itself as an early indicator that the offending partners may not be trustworthy and pursuing a long term business partnership with them might be ill-advised. At the very least, there would need to be more caution exercised in future dealings.

Another level where trust is important is in what the model and tool suggest as the 'best justified' security action for collaborating companies. Although it is a trivial calculation, as with most software there are slim chances of malfunctioning and miscalculations; doctoring of results may even be an issue if the system is implemented by a malicious partner. This issue becomes an even more serious concern where the tool is used as a first-pass filtering mechanism to compare hundreds of security actions originating from several collaborators. Businesses' security analysts interested in saving time and increasing productivity may well choose to focus only on situations where there are conflicting security actions types for risks or irreconcilable differences that need to be actively discussed by personnel. The assumption is therefore that the tool's initial comparison is accurate and as such, the security actions not flagged for human follow-up need no further consideration or investment of precious business time and effort at this point. This is an assumption that may be improper if there are any errors in the system. The main way to approach this and to build trust in the system is to conduct checks on the tool and occasional human validation of all its suggestions and information output flows. Moreover, although certain levels of automation may be possible, as stated before in this paper, the tool is not to replace decision makers but only to support and quicken the process. Thus, human security analysts should be checking a majority, if not all of the action suggestions made by the tool to ensure they fit in with the security ethos and direction of the collaboration.

VII. Related Work

Interorganisational security has been researched by numerous articles in the literature. Dynes et al. [4] is one of the more relevant research works that emphasises the problem and identifies several business cases in Critical National Infrastructure, Manufacturing and Financial Services where concerted approaches to security are required. Within that article, they outline numerous building blocks to a holistic security solution across interacting enterprises. We believe that our work can fit adequately within these blocks, particularly when deciding security strategy and agreeing on treatment of risks. This would assist directly in supporting security negotiations and expediting any necessary decisions between collaborating entities.

The topic of interdependent security is also relevant to this paper's research. Interdependent security as a concept uses game theory models to investigate how security investment decisions in one company (or unit) depend on what other interacting (interdependent) businesses (or units) are doing [20,21]. For example, it has been shown that there is less incentive for a business to invest in security if collaborating businesses do not invest, because the business is still vulnerable to risks propagated from the less secure partnering systems. This research is relevant to our work generally as it reinforces the interconnection of security decisions and at the lower level in the interrelation between risk treatments. The main difference is that the model in our research holds that partners should agree on the same treatment for shared risks. Therefore, there is no divergence and hence no need for tipping or cascading behaviour as apparent in the interdependent security approach.

In [22], the authors develop a quantitative model to define interdependent security investments based on 'linear influence networks'. According to them, the agents in their model interact in a perfect information game, resulting in a unique Nash Equilibrium. Their further work [23] also considers this problem in terms of security investments in interdependent organisations. Our model is similar to theirs in its consideration of security decision models, but differs for similar reasons as with the interdependent security approach above. Moreover, we have the unique aim of formal inclusion of social factors (e.g., laws, policies, contractual obligations) into our decision model, a goal that is not shared by that or several of the other works in the security field.

VIII. Conclusions and Future Work

The aim of this paper was to explore the design of a model which replicates the human decision-making process with regards to the reconciliation of conflicting security needs across collaborating businesses. To achieve that goal, we utilised existing research and drew on interactions with security professionals on how such a decision is made. For support of the formal modelling activity, the field of MCDM was referenced. This was done both to guide modelling and with the aim of creating a more appropriate, grounded formula. Once this was completed and a model defined, a simple example was presented to illustrate the model's application.

Following the presentation of the model, it was discussed in detail and its limitations highlighted. Even though the model itself is viewed as a novel proposal for the socio-technical field which challenges current research thinking regarding the formalization of social aspects, its limitations are slightly more important here. This is because they identify key issues for this (especially in terms of future work) and other research which attempts to formally define such a decision process. We then presented high-level feedback from industry-based security professionals on this initial decision model. Generally, professionals showed interest in the conceptualisation but noted that much more testing and analysis would need to be done. This at least provides some level of support for the feasibility of the ideas and thus the need for future research in this area. Lastly, we considered the notion of trust and highlighted why good levels of trust across collaborating entities was crucial to the success of the model and any decision-support it would provide. Trust has always been a significant component in business interactions and that importance is simply maintained here.

As it relates to further work, we aim to focus specifically on the limitations from Section IV and act on how these may be resolved. From there, the next task is to conduct a case-study to evaluate the model's use in the real-world including how well it is able to model the process and factors and to what extent it outputs usable decisions.

References

[1] S. Yau, P. Bonatti, D. Feng, and B. Thuraisingham, "Security and privacy in collaborative distributed systems," in *29th Annual International Computer Software and Applications Conference*. IEEE, 2005, p. 267.

[2] P. McDaniel and A. Prakash, "Methods and limitations of security policy reconciliation," *ACM Transactions on Information and System Security*, vol. 9, no. 3, pp. 259–291, 2006.

[3] T. Lavarack and M. Coetzee, "A framework for web services security policy negotiation," in *ISSA Conference*, 2009, pp. 153–170.

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

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

[6] J. R. C. Nurse and J. E. Sinclair, "An evaluation of BOF4WSS and the security negotiations model and tool used to support it," *International Journal On Advances in Security*, vol. 3, no. 3, 2010.

[7] ——, "A thorough evaluation of the compatibility of an e-business security negotiations support tool," *International Journal of Computer Science*, vol. 37, 2010.

[8] A. Jones and D. Ashenden, *Risk Management for Computer Security: Protecting Your Network & Information Assets*. Amsterdam: Elsevier, 2005.

[9] D. J. Landoll, *The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments*. Boca Raton, FL: Auerbach, 2006.

[10] V. Belton and T. J. Stewart, *Multiple Criteria Decision Analysis: An Integrated Approach*. Boston: Kluwer Academic Publishers, 2002.

[11] E. Triantaphyllou, *Multi-Criteria Decision Making Methods: A Comparative Study*, P. M. Parlos, Ed. Dordrecht: Kluwer Academic Publishers, 2000.

[12] G. Stoneburner, A. Goguen, and A. Feringa, "Risk management guide for information technology systems (special publication 800-30)," NIST, Tech. Rep., 2002.

[13] International Organization for Standardization (ISO), "ISO/IEC guide 73 risk management – vocabulary – guidelines for use in standards," Tech. Rep., 2002.

[14] T. L. Saaty, *The Analytic Hierarchy Process*. New York: McGraw Hill, 1980.

[15] ——, "Decision making with the analytic hierarchy process," *International Journal of Services Sciences*, vol. 1, no. 1, pp. 83–98, 2008.

[16] J. R. C. Nurse, "A business-oriented framework for enhancing web services security for e-business," Ph.D. dissertation, University of Warwick, 2010.

[17] R. M. Perloff, *The Dynamics of Persuasion: Communication and Attitudes in the 21st Century*, 2nd ed. Mahwah, NJ: Lawrence Erlbaum Associates, Inc., 2003.

[18] P. Ratnasingam, "Trust in inter-organizational exchanges: a case study in business to business electronic commerce," *Decision Support Systems*, vol. 39, no. 3, pp. 525–544, 2005.

[19] J. R. C. Nurse, S. Creese, M. Goldsmith, and K. Lamberts, "Information quality and trustworthiness: A topical state-of-the-art review," in *The International Conference on Computer Applications and Network Security (ICCANS) 2011*. IEEE, 2011.

[20] H. Kunreuther and G. Heal, "Interdependent security," *Journal of Risk and Uncertainty*, vol. 26, no. 2, pp. 231–249, 2003.

[21] G. Heal, M. Kearns, P. Kleindorfer, and H. Kunreuther, "Interdependent security in interconnected networks," in *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*, P. Auerswald, L. Branscomb, T. LaPorte, and E. Michel-Kerjan, Eds. New York: Cambridge University Press, 2006, pp. 258–275.

[22] R. Miura-Ko, B. Yolken, J. Mitchell, and N. Bambos, "Security decision-making among interdependent organizations," in *IEEE 21st Computer Security Foundations Symposium*. IEEE, 2008, pp. 66–80.

[23] R. Miura-Ko, B. Yolken, N. Bambos, and J. Mitchell, "Security investment games of interdependent organizations," in *46th Annual Allerton Conference on Communication, Control, and Computing*. IEEE, 2008, pp. 252–260.