WHEN MORE, SMALLER ONES ARE BETTER THAN FEWER, LARGER ONES

A theory driven study on whether large collaborations are actually desirable to improve the cyber security related awareness of individual organisations by means of pragmatic information sharing

Bart Spijkervet
Faculty of Technology, Policy and Management
Delft University of Technology

Abstract – Many organisations are affected by cyber-attacks themselves or via other organisations. To improve the awareness of organisations on cyber security related matters various information sharing collaborations were implemented. However, it is uncertain what the design should be like to be able to share pragmatic information productively. To determine whether large collaborations, possibly even spanning across sectors, are actually preferable a theory driven research project was performed. This article presents the main finding following from that research project. The main finding is that smaller collaborations are to be preferred if organisations want to share pragmatic information. With smaller collaborations the differences between organisations will be limited. Such limitations of differences are essential for the participants to be able to develop a shared view of what has to be done to- and on how to- improve the cyber security. Finally, the resulting limitations of differences between organisations in collaborations are also essential for the development of trust. Trust is of importance for organisations to actually be willing to share the required, sensitive information that other organisations need. Future research should focus on empirical validation that smaller collaborations are indeed more productive in sharing sensitive information.

Keywords:
Situation awareness, information sharing, cyber security, trust, collaboration

I. INTRODUCTION

Cyber security used to primarily be about the protection of information stored on digital systems. It was a concern to the owner of that information. But cyber security is now about notably more than just information security. Reason is the (increasing) awareness of the vulnerability of systems of critical infrastructures, such as power plants. But also the denial of service attacks on financial sectors had its impact. Although the vast amounts of cyber-attacks resulting in cases of espionage, copied or stolen information, and destruction of data is still a concern, there now is more attention to the potential disruptive consequences to society of cyber-attacks. With that it is touched upon that cyber security is, as described by [1], about the larger whole of securing the interests of individuals, organisations and nation states that function in (or are affected by) the digital environment.

This increased attention to cyber security is for good reason. By nature attackers already have an advantage, but this is reinforced with cyber-attacks in general and the current state specifically. On the offensive side of attacks, an increasing number of (successful) attacks were witnessed. These attacks are becoming more insidious [2, p. 14], targeted [2, p. 10] and possibly becoming more devastating overall by reverse engineering of the most devastating ones [2, p. 54]. Furthermore, allegedly smaller and less defensible organisations are increasingly targeted [2, p. 4]. The defensive side on the other hand is already behind in terms of capabilities[3], is underinvesting in security [4], lacks the required full overview of cyber threats [5] even resulting in cases in which parties did not notice they had been successfully attacked [6], and there is a lack of timely sharing of successful attacks to allow others to take precautionary measures or to allow minimization of potential damages [4] (such as by revoking access to their systems or changing credentials).

This combination of strong attackers and weak defenders is considered to necessitate organisations to collaborate by sharing information on how to avoid incidents, to help each other at times of attacks and to inform in case of attacks [4][5]. Setting up such an information sharing collaboration is challenging if the required information changes and the flow of information is amongst different parties in different directions at different moments in time. Different parties get attacked and with that making sense of why this was possible might necessitate involvement of these different parties. With all that there is a natural tendency to focus on large collaborations, hoping the required information will be in the collaboration. In the United Kingdom there is a large scale collaboration in development, involving collaborating organisations from a variety of sectors [7]. In contrast, in the United States, the collaborations are oriented per sector[8]. It was suggested by NSS Labs that inter industry partnerships are important too as threats also cross

industries. But as also mentioned by NSS Labs, opting for a limitation of collaboration to intra sectorial collaborations helps build trust. [9] With that, the question is, if something has to be changed, whether collaborations have to increase or decrease their scope in terms of participant sectors.

The main question in this article is to consider what the consequences are to focus on larger collaborations, possibly spanning different sectors, as opposed to opting for smaller collaborations, for the sake of improving situation awareness of organisations by means of pragmatic information sharing on cyber security related matters.
The scope of this article is limited to the identification of the impact of the size of the collaboration on the collaboration itself and the sharing of information. As a result thereof important topics such as the actual topic of shared information or who to invite in collaborations are not discussed. Furthermore, the focus is on the more challenging information sharing collaborations that focus on detecting exploitations of vulnerabilities.
This article is entirely based on a part of a more extensive research project on information sharing collaborations. In that project the to be considered steps in the development of collaborations were identified [10]. To assess the impact of the size of the collaboration three theories were and are used: situation awareness, trust and the configuration theory. To answer the main question of this article it is first considered what the consequence would be if the size of the collaboration would increase, followed by what would happen if it would actually decrease.

The structure of this article is as follows. The improvement of situation awareness is considered to be the main goal of the information sharing collaborations and is discussed in the second section. In the third section trust is first discussed on a theoretical level and that is followed by a discussion of the consequences of the scale on the development of trust. In the fourth section the notion of a socially agreed upon definition of reality is discussed in theory using the configuration theory and next the impact thereof is applied to the topic of cyber security. In the fifth section the impact of the size of collaborations in two real world examples is discussed using the findings from the preceding three sections. The final section presents the conclusions.

II. IMPROVING SITUATION AWARENESS

The intention of information sharing collaborations is, in this research, considered to serve the purpose of improving the situation awareness of some organisation. The concept of Situation Awareness (SA) is described by Endsley [11, p. 36] as having some level of awareness about the situation in an environment in some respect. She distinguishes three nested levels of awareness an agent can achieve. Perception, or level one awareness, is the least advanced level of awareness in which an agent is able to perceive the elements in the current situation (e.g. amount of traffic to a specific server on specific ports). The overarching level two awareness, comprehension, is about attaching meaning to the values of those elements (e.g. unusual amount of traffic from specific locations). The third level, projection, is about being able to understand the future status (e.g. understanding it will saturate the amount of resources and render the service unavailable). It is presumed that high levels of situation awareness positively influence the decision making capabilities, which presumably affects the performance. [12, p. 36] Because of this presumed relationship, information sharing is supposed to be of value to improve the performance of organisations in terms of allowing them to be able to improve their cyber security.
In the end, society has to be interested that one or multiple organisations improves its SA. Supposedly this increase in SA will increase the performance of the organisations in terms of cyber security. And that could result in less accidents, such as hacks by adversaries. It is not necessarily the case that all organisations have to improve their SA. By allowing one party, such as a central hub or knowledge centre, to improve its SA, that party might provide information to others on how to proceed instead (such as suggested by [13, p. 283] in their architecture of a Cyber Attack Information System).
In the end the underlying intention is to have the 'right' participants in the collaboration. The right participants have sufficient levels of situation awareness in some respect. A respect which is relevant to others. The troublesome bit is that, especially in advanced attacks, it is not known who has the required SA to help others out. From all this follows the urge to have more participants, as with that more SA enters, which potentially could be of use. Ultimately the main intention is to have proper coverage to complete the required SA of some party, preferably entirely up to level three. The proper coverage could be, in extremes, thought of by inviting many parties. This option is currently selected by scaling a collaboration to the level of sectorial collaborations and even to the level of that of inter-sectorial collaborations. By inviting many parties, presumably much SA is available and the challenge becomes to combine the insights of those different, yet compatible views present. With that, the main concern is to maintain a high productivity of information sharing, being the ratio of the effectiveness of the information sharing and the

required efforts therefore. It is on one side the challenge of effectiveness in terms of having the required SA present in the network and delivering it. The useful participants have to be present in the collaboration. (Assuming that the required SA can be used to provide the required information.) On the other hand it is about being able to find the participant with the required SA in an efficient way. Especially with larger collaborations and more challenging conditions efficiency is a concern. The key is to have participants not waste much time finding out where to find the required information. Herein Meta SA is of importance, the awareness of knowing who knows what and who needs what [14, p. 1291].

Importantly, information sharing collaborations for the purpose improving SA take time to develop. Both on the side of the participants themselves (such as articulating what has to be known) and of the organisational structure itself [15, p. 217]. It takes time to find the most productive organizational structure. Opting for an all-connected structure (in which everybody can contact everybody) might overload the participants. On the other extreme, opting for a rigid structure, including checks and balances, might be too sluggish and load individual parties disproportionately. [16] With all that, redesign and changes are to be expected to optimize efficiency and effectiveness of the structure.

III. TRUST

The presupposition of the collaboration is that the participants are willing to share information with each other. In absence of a proven system capable of producing trustworthy information sharing collaborations, allowing for system based trust, parties have to trust the individual participants of the collaborations in some way. Participants have to trust each other with information, expecting the other organisation not to behave opportunistically.

Breakdown of the concept of trust in parties

The type of trust thus far referred to in this article is called 'reliance' by Nooteboom. It is the expectation that 'things will not go wrong', regardless of the basis of that expectation. [17, p. 49] There are two extreme bases of the expectation, 'assurance' and 'trust in the strong sense'. [17, p. 11] Assurance is about forms of control by minimizing the opportunities to behave opportunistically. To say it is about assuring that things will not go wrong. At the other extreme is trust in the strong sense, with the expectation that the trusted party (trustee) can be trusted even if there are opportunities and incentives to behave opportunistically. The troublesome bit is that trust in the strong sense does not scale well and takes time to develop. Being extremes, there will actually be some mix of trust and assurance. Even with extensive levels of trust in the strong sense, contracts are used, albeit that their purpose is different, they serve as an aid to memory, not to assure trustworthiness. [17, p. 49]

Trust in the strong sense is considered to be the preferred mode of interaction over assurance in the long run given its intrinsic and extrinsic values [17, p. 2]. Although trust is relatively expensive, because of the required investments in building such a relationship are specific hereby posing high sunk costs [17, p. 131], such costs can be outweighed in the long run. First of all, the intrinsic value is that people prefer to work on the basis of trust in the strong sense, as opposed to working in distrust, which necessitates checking the behaviour of others [17, pp. 2–3]. The extrinsic value of trust is that it has lower transaction costs due the reducing effect of trust on the relational risk [17, p. 2]. Furthermore, compared to contracts, trust does not presuppose knowing or foreseeing all possible situations and protecting against undesired situations. It is better equipped to cope with uncertainties. Trust works on the basis of limits of trustworthiness for specific conditions. Within those limits there is trust. Beyond those limits the trusting party (trustor) has to be aware [17, p. 46], yet trustworthy behaviour of the trustee in those cases can deepen trust [17, p. 197]. Uncertainties might be result of the sharing of new types of information. Such changes would probably require updating contracts. Other extrinsic values of trust are that it influences the quality and the fluency of communication [18, p. 2].

Development along two extreme systems of trust

In newly developed collaborations, organisations cannot fall back on trusting the system producing and auditing collaborations, or at least trust the present collaboration as a whole. Because of that they have to trust the organisations participating in the collaboration and their representatives in the collaborations. With that, the scale, development and scope of the information sharing collaboration can be considered as factors of importance. Decisions with regard to those factors results in development in either a (more) contractual based system (type A) or a (more) relational based system (type B) [17, p. 131].

The first extreme system of trust is based on contracts amongst multiple parties system. Assurance in that system is the dominant factor. Large scale collaborations and collaborations with early on high stakes (as in sharing confidential information early on in the lifecycle of a collaboration) tend to stimulate the use of forms of assurance. Parties will opt for forms such as extensive contracts minimizing room for opportunistic behaviour and protecting against uncertain events. The motivation therefore is that with larger collaborations the organisations in the

collaboration will differ more, the 'cognitive distance' between organisations is larger. With larger distances organisations have more difficulty in assessing what the other organisation might do with the information. Furthermore, with large collaborations it is also harder to see who has access to the information. In such a case the willingness to share data for the purpose of sense making will be challenged, unless extensive contracts can limit the room for opportunism. Alternatively, the organisation might refrain from sharing the detailed information in the first place.

The other extreme is that of a relational system of interaction with a more exclusive set of participants, with trust in the strong sense as the dominant factor. It will therefore typically be more suitable to smaller collaborations, because the cognitive distances in such collaborations are limited. This distance is important to trust because trust is often a rational evaluation of trustworthiness of the trustee in a situation [17, p. 188]. For such an evaluation it is important that the trustor understands the trustee and preferably is even able to empathize with the trustee. Trust comes down to a (i) trustor, who trusts a (ii) trustee, in (iii) some respect, (iv) depending on the conditions. This is what Nooteboom refers to as the four place predicate of trust. [17, p. 38] If the trustor can empathize with the trustee, the trustor can understand whether the trustee can actually be trusted in the current conditions. This results in some sort of implicit demarcation of the boundaries of trust. Within those boundaries there is no continuous evaluation of trustworthiness. But for such an initial assessment of trustworthiness of a trustee, the trustor has to have some way to assess the trustworthiness. In extremes this could be based on knowledge or cognition [17, pp. 12–13]. Knowledge based trust can be akin to assurance, knowing the trustee does not have room for opportunistic behaviour in some situations. Cognition based trust is about being able to emphasize with the trustee whether the trustee is confronted with tempting opportunities and incentives to behave opportunistically. It is this cognition based trust that is challenged in case the collaboration spans different sectors, as it is harder to empathize with an organisation that is in a different sector. Although the topic of concern, cyber security, might be the same, the entire background and possibly stakes of cyber security differ.

Development of the information sharing collaboration

Despite the two systems being extremes and there being intermediate forms, the initial balance of the two can be of importance. As posed by Deutsch with the 'crude law of social relations', there might be a circular causation of initial mode of interaction. Parties starting off in distrust and settling this by means of contracting presumably will continue to rely on contracts. [17, p. 96] Should this hypothesis be the case, and following from the preceding, it is important to consider how to start the collaboration as it will affect the possibilities and development of the collaboration. Both in terms of the shared information and the collaboration as a whole. In the remainder of this section first the development of the collaboration is discussed, next its impact on the content.

Development of the collaboration

The assurance oriented type of collaboration is intended for interactions with larger numbers of parties for a shorter period of time, such as a collaboration with a short turnaround. For a short period of time setting up contracts is relatively simple as there are fewer conditions to anticipate. Additionally, the preferred alternative of trust in the strong sense is not an option if the collaboration has to be short and sweet. However, in the long run the challenging conditions might necessitate redesigns of the contracts and the relatively high transaction costs might make assurance based collaborations counterproductive.

The collaboration based on a form of trust in the strong sense is oriented on the long term. It takes time to build the required trust and it requires frequent interaction (in some way) to be able to assess the trustworthiness. But over time the collaboration might evolve into one with more systemic levels of trust. Instead of exclusively trusting the participants, more subtle ways covering assurance could emerge. For example by having some reputation system, safety nets or some oversight body. Some examples thereof were discussed by Bruce Schneier [19]. An encompassing example along his train of thought is public transportation. Transportation by busses for example has evolved into a situation in which travellers trust the public system, including the options to complain or be protected against bad behaviour. They (no longer) have to exclusively trust the organisation and its motivations, let alone the employee responsible for driving the bus. The traveller trusts the undefined system of public transportation, in some way, to offer trustworthy public transportation.

Impact of the system of trust on the content of discussion

The collaboration that focusses on assuring trustworthy behaviour has all the intention to minimize the amount of uncertainty. Assurance forms such as contracts will be carefully drafted to minimize the opportunities and incentives for opportunistic

behaviour. With that, a change or increase of scope in terms of shared information is detrimental, it raises the costs and the uncertainty.
On the other hand, with trust, especially if the number of participants is relatively high, trust has to deepen. Relatively harmless information would have to be exchanged at first and slowly the boundaries of trust would have to be stretched by seeking different conditions and different 'respects'. Herein trust has the advantage over assurance based forms in that trust is better equipped to deal with uncertainty. In a sense, trust is always a wager, there is no constant checking upon the other, especially if the conditions suggest trustworthiness of the trustee.

IV. Developments of different perceptions of reality

Thus far the primary focus was on the sheer amount of participants and the consequences thereof. But aside from the sheer amount, the (in part) underlying differences between the participants actually play a crucial role too. This was casually discussed with trust because larger differences amongst parties make it harder to empathize with the other organisation and with that it is harder to assess trustworthiness. But it is also relevant to situation awareness, specifically on defining what is relevant. As discussed in the first section, situation awareness is about awareness in some situation. This section is about the challenges in defining the situation that have to be considered. Such a definition of 'the situation' dictates what situation the organisations have to be aware of. To support the analysis the configuration theory is used and it is linked to current challenges in the realm of cyber security.

The socially defined reality of cyber security

The core of the configuration theory is the presumed interaction of a social and a cognitive dimension [20, p. 86][21, p. 258][22, p. 27]. The social dimension represents the parties taking part in a configuration ('who'), the cognitive dimension represents their definitions of reality ('what') [21, p. 271][22, p. 325]. Each party in a configuration has its own definition of reality, which is defined on the basis of insights of prior interactions with other parties. In a configuration the different parties together (re)define a commonly agreed upon definition of reality [22, p. 325]. Such a (re)definition reflects what a configuration, at that moment in time, defines as being the relevant situation. Definitions of reality are therefore merely a snapshot of a moment in time. [21, p. 258][22, p. 326] The two dimensions are interacting as a double helix [22, pp. 34–35], in that they affect each other, but also that one can be traced back to the other [20, pp. 86–87]. A configuration of smaller organisations might define the situation, 'the reality' of cyber security, to not really being applicable to them as they are no real target. (Which many smaller organisations actually do think [23].) On the other hand, there are definitions of reality that cyber security is a concern, yet not a technical issue, rather a managerial one. A view which might be attributable to some configuration focusing on the current vulnerabilities of SCADA systems which could technically be solved or at least be avoided, should management offer the resources for that.
Another important aspect of the configuration theory is its focus on allowing for a continuous redefinition of reality and also allowing for changes of participating organisations in a configuration [22, pp. 38–39]. Furthermore, participants are not considered to necessarily find themselves in one configuration, they might be part of multiple configurations (they are 'multiple included') [22, pp. 269–270]. It is this multiple inclusion that allows for redefinitions of reality as participants come into contact with different definitions of reality, which they can introduce in other configurations.

Targeted attacks on different victims

The notion of a socially defined definition of reality is an actual fact as seemingly attacks are becoming increasingly targeted on specific, different victims [2, p. 4]. With that organisations are actually confronted with different realities. On top of that, they might perceive these realities different, possibly due to not detecting the actual, specific reality. (The latter being a reference to the increasing amount of organisations that did not detect a successful attack by themselves, but had to be informed by others thereof [6].) And finally, organisations might think differently of what the underlying cause is and how it should be solved. The latter could be the result of why some focus on (zero day) vulnerabilities, whereas others ([5]) think that the majority of all problems can be avoided by patching systems.
With that, focusing on large scale collaborations will typically result in rather abstract definitions of reality. This can be of value in a broader discussion of how to treat the issue of cyber security, in terms of addressing responsibilities and considerations of whether some systems should be online in the first place. Smaller collaborations can define a more practical definition of reality. The result is a more concrete definition of the relevant situation on which organisations have to improve their awareness. With such a definition participants can seek parties which have the relevant SA and are willing to provide information. Crucially, knowing that parties can be multiple included, there is no specific need to maximize the scale and scope of collaborations. In the end, the main goal is to be in contact with those

organisations that are, in some way, affected by the same attacks. This could be because they are in the same sector, of the same size or have something else in common.

V. Real world examples akin to the two systems

In their report [9], NSS Labs mentions FS-ISAC, the Financial Service-Information Sharing and Analysis Centre, as being considered to be the most mature and most successful ISAC. With 4.400 connected members organisations it is a large collaboration. But as also discussed by NSS Labs, ISACs, such as FS-ISAC, tend to focus on more strategic level discussions, with limited actionable information being exchanged. Finally, it was noted that public bodies approach the problems from a worst-case scenario, whereas the private sector uses the most likely scenario. [9] All this is to be expected following the findings as presented in this article. Based on interviews the National Infrastructure Advisory Council already came to similar conclusions [8]. Amongst their findings they found that regarding information sharing, in the Banking and Finance centre, there are conflicting missions in which some organisations focus on catching the adversary behind the attack, whereas others had the intention to avoid additional attacks. (B-10) Furthermore, it is discussed that information sharing takes place using long standing trusted relationships with clear roles and responsibilities [8, p. B–17]. Albeit a bit ambiguous, with that description it appears that the trust relationship is balanced towards assurance.

In contrast, in the chemical sector personal relationships are highly important [8, pp. C–10]. But unlike the financial sector, the chemical sector does not entirely reuse pre-existing arrangements. The cyber information-sharing is different from discussions of physical-security. The cyber-security information is shared in a small community, with the intention to minimize the spreading of knowledge of the existence of vulnerabilities at organizations. The downside of this approach is that smaller organisations typically do not have access to such communities and lack the required personal relationships to acquire the relevant information. [8, pp. C–12]

VI. Conclusions

The suggestion to scale a collaboration to span across sectors, because the attacks are also not bound to sectors, is, in this research, considered to come down to the urge of covering all possibly relevant situation awareness. Such scaling will also increase the differences between participants. Increases in difference between organisations decrease the chances to empathize with those organisations, which is necessary for a development of cognition based trust. As a result, the balance of trust will shift more towards assurance based forms of trust relationships. Such relationships can scale better, are easier to develop, but are worse at handling uncertainty and are less efficient in the long run given the relative high transaction costs. Furthermore, with increases of the amount of participants, and specifically the (resulting) increase in differences between organisations, it is harder for participants to agree upon a shared pragmatic, definition of the relevant situation of cyber security. The result is typically a more strategic definition of reality, making the productive sharing of information for the sake of improving situation awareness at best more of a challenge. In contrast, smaller configurations of parties can come to a more concrete definition of a reality. With that, they can get a more concrete picture of what situation awareness is required and act upon that by sharing actionable information. This decrease in scale and scope comes at the expense of missing relevant aspects. This could be mitigated by having organisations take part in different configurations of collaborations, each focusing on slightly different definitions of reality.

With all that, it is not to say that larger collaborations, possibly spanning across sectors, have no use, as more high level discussions could have its value. But it is important to recognize that given the presumed tendency of adversaries to attack more targeted, less parties in a collaboration would be affected. Add to this, the drawbacks of larger collaborations, and it appears that the more productive solution is to have organisations take part in multiple, yet smaller collaborations.

A suggestion for future research is to actually implement collaborations that employ the suggested design of smaller collaborations, consisting of organisations that are part of multiple of such collaborations. The intention should be to validate empirically whether such a collaboration is actually more productive to proof the importance of smaller collaborations.

VII. References

[1] R. von Solms and J. van Niekerk, “From information security to cyber security,” *Comput. Secur.*, vol. 38, pp. 97–102, Oct. 2013.

[2] Symantec, “Internet Security Threat Report 2013,” Apr-2013. [Online]. Available: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf.

[3] J. Schellevis, “‘Ict-beveiligers lopen achter op hackers,’” 01-Mar-2013. [Online]. Available: http://tweakers.net/nieuws/87585/ict-beveiligers-

lopen-achter-op-hackers.html. [Accessed: 05-Mar-2013].
[4] N. Kroes, “Cyber-security – a shared responsibility,” 04-Nov-2012. [Online]. Available: http://europa.eu/rapid/press-release_SPEECH-12-774_en.htm. [Accessed: 05-Mar-2013].
[5] F. Maude, “Cyber Security Information Sharing Partnership,” 27-Mar-2013. [Online]. Available: https://www.gov.uk/government/speeches/cyber-security-information-sharing-programme. [Accessed: 16-Aug-2013].
[6] D. Barrett, “U.S. Outgunned in Hacker War,” *Wall Street Journal*, 28-Mar-2012.
[7] Cabinet Office, “Government launches information sharing partnership on cyber security,” 27-Mar-2013. [Online]. Available: https://www.gov.uk/government/news/government-launches-information-sharing-partnership-on-cyber-security. [Accessed: 10-Sep-2013].
[8] National Infrastructure Advisory Council, “Intelligence information sharing,” 10-Jan-2012. .
[9] F. Y. Rashid, “Report Shows ‘Uneven Progress’ in Cybersecurity Information Sharing,” *SecurityWeek*, 30-May-2013. [Online]. Available: http://www.securityweek.com/report-shows-uneven-progress-cybersecurity-information-sharing. [Accessed: 20-Oct-2013].
[10] B. Spijkervet, “Less is more,” TU Delft, Delft, Netherlands, Feb. 2014.
[11] M. R. Endsley, “Toward a Theory of Situation Awareness in Dynamic Systems,” *Hum. Factors J. Hum. Factors Ergon. Soc.*, vol. 37, no. 1, pp. 32–64, Mar. 1995.
[12] M. R. Endsley, “Direct measurement of situation awareness in dynamic systems : Situation awareness,” *Hum. Factors*, vol. 37, no. 1, pp. 65–84, 1995.
[13] F. Skopik, Z. Ma, P. Smith, and T. Bleier, “Designing a Cyber Attack Information System for National Situational Awareness,” in *Future Security*, N. Aschenbruck, P. Martini, M. Meier, and J. Tölle, Eds. Springer Berlin Heidelberg, 2012, pp. 277–288.
[14] N. A. Stanton, R. Stewart, D. Harris, R. J. Houghton, C. Baber, R. McMaster, P. Salmon, G. Hoyle, G. Walker, M. S. Young, M. Linsell, R. Dymott, and D. Green, “Distributed situation awareness in dynamic systems: theoretical development and application of an ergonomics methodology,” *Ergonomics*, vol. 49, no. 12–13, pp. 1288–1311, Oct. 2006.
[15] P. M. Salmon, N. A. Stanton, G. H. Walker, and D. P. Jenkins, *Distributed situation awareness theory, measurement and application to teamwork*. Farnham, England ; Burlington, VT: Ashgate, 2009.
[16] L. J. Sorensen and N. A. Stanton, “Y is best: How Distributed Situational Awareness is mediated by organisational structure and correlated with task success,” *Saf. Sci.*, vol. 56, pp. 72–79, Jul. 2013.
[17] B. Nooteboom, *Trust: forms, foundations, functions, failures, and figures*. Cheltenham, UK ; Northampton, MA: E. Elgar Pub, 2002.
[18] H. Seppänen, J. Mäkelä, P. Luokkala, and K. Virrantaus, “Developing shared situational awareness for emergency management,” *Saf. Sci.*, vol. 55, pp. 1–9, Jun. 2013.
[19] B. Schneier, “Trust and Society,” Feb-2013. [Online]. Available: https://www.schneier.com/essay-412.html. [Accessed: 10-Feb-2014].
[20] H. J. van Dongen, W. A. M. de Laat, and A. J. J. A. Maas, *Een kwestie van verschil: conflicthantering en onderhandeling in een configuratieve integratietheorie*. Delft: Eburon, 1996.
[21] C. J. A. M. Termeer and B. Kessener, “Revitalizing Stagnated Policy Processes Using the Configuration Approach for Research and Interventions,” *J. Appl. Behav. Sci.*, vol. 43, no. 2, pp. 256–272, Jun. 2007.
[22] C. J. A. M. Termeer, *Dynamiek en inertie rondom mestbeleid: een studie naar veranderingsprocessen in het varkenshouderijnetwerk*. VUGA, 1993.
[23] National Cyber Security Alliance and Symantec, “New Survey Shows U.S. Small Business Owners Not Concerned About Cybersecurity; Majority Have No Policies or Contingency Plans,” 15-Oct-2012. [Online]. Available: http://www.symantec.com/about/news/release/article.jsp?prid=20121015_01. [Accessed: 24-Dec-2013].