Life is a collaborative problem which cannot be resolved: the case of cybersecurity

Understanding the quality of collaboration for cybersecurity incident- and risk management

Jerry E.B. Andriessen

Wise & Munro Learning Research, jerry@wisemunro.eu

Mirjam Pardijs

Wise & Munro Learning Research, mirjam@wisemunro.eu

In this position paper, we briefly present CS-AWARE, a socio-technical solution for cybersecurity problems in the context of municipalities and organizations. We our scenario-based approach to designing collaboration, and end with four issues that we think are worth more attention in the collaboration research community: capturing collaborative agency, collaborative awareness developing over multiple experiences, the role of theory and the role of participants in defining quality.

CCS CONCEPTS • Interaction design • Collaborative and Social computing • Network security

Additional Keywords and Phrases: design of collaboration, scenario-based design, cybersecurity

1 INTRODUCTION: THE CASE OF CYBERSECURITY

Cybersecurity is one of today's most challenging problems, for commercial companies, NGOs, governmental institutions as well as for individuals. In addition to technology focused boundaries of classical information technology (IT) security, cybersecurity is a multidisciplinary issue: it includes organizational and behavioural aspects of IT systems, and also needs to comply to legal and regulatory frameworks [1].

CS-AWARE-NEXT is designed to be a follow-up project to CS-AWARE [2, 3], a H2020 project completed in August 2020. CS-AWARE provides an advanced real-time cybersecurity awareness and management framework and platform implementation for local public administrations and NIS sector organisations. The main features of CS-AWARE are a socio-technical and organizational focus, collaboration and skill building within the organization (e.g., between different departments), multi-lingual semantics support, real-time AI supported awareness and visualization utilizing threat intelligence, system self-healing and cybersecurity information sharing. A demo of the CS-AWARE platform is available on their web page. CS-AWARE-NEXT adds the dimension of collaborative between organizations, focuses on how advanced and dynamic cybersecurity management needs can be better integrated in the organizational context (including better collaboration on complex cybersecurity tasks within the organisation, and with other actors in the supply chain. This requires organizations to reflect on information sharing of cybersecurity information with different stakeholders.

There are several challenges to overcome in order to make information sharing in the context of cybersecurity risk and incident management widely supported, accepted, efficient and effective. Information sharing for organisational and local/regional cybersecurity and risk management beyond legal compliance tasks is the exception rather than the norm. In

order to address this problem, the requirements for this context need to be specified, and appropriate support mechanisms for all relevant stakeholders on the cybersecurity environment need to be provided. The incentives for organizations to share cybersecurity information beyond legal/regulatory requirements are not yet well understood. The automation of the cybersecurity information exchange process in the context of incident and risk management for organisations is still in its infancy, and an integration with modern and dynamic incident and risk management platforms like CS-AWARE has great potential for increasing the efficiency of information sharing through automation.

In this contribution we focus on the issue of collaboration, especially concerning the various forms under which collaboration appears during the project and at the pilot settings.

2 DESIGNING COLLABORATION

Our approach to designing cybersecurity collaboration is by building scenario templates. Scenario-based design [4] has evolved in the context of designing human-computer interaction. Scenarios are general patterns for how people work with information, starting from descriptions of activities, gradually moving towards more abstraction. Scenarios highlight goals suggested by the appearance of the technology; what people try to do with the technology; what procedures are adopted, not adopted, carried out successfully or erroneously and interpretations people make of what happens to them. Scenarios can be seen as stories about people and their activities. Stories have characteristic elements [5]. They mention or presuppose a setting and include agents or actors. Goals are transformations that the agent wishes to achieve in the circumstances of the setting. Stories have a plot, they include sequences of actions and events: things that actors do, things that happen to them, changes in the circumstances of the setting, and so forth. Particular actions and events can facilitate, obstruct, or be irrelevant to given goals.

For the purpose of facilitating collaboration, we are building CS-CONNECT, a tool that interfaces with the CS-AWARE platform that allows users to communicate and act in the case of incidents, but can also be used for various collaborative support activities between professionals at the regional level, for example for sharing and discussing problems, policies and knowledge management, and for education and training purposes.

Essentially, scenarios are codesigned together with participants during the following activities: (a) A three days SSD workshop [6], in which stakeholders from an organisation collaboratively build rich pictures of their system network, the business processes, and the interdependencies; (b) A storytelling workshop, where these stakeholders collaboratively build stories on their experiences with cybersecurity issues, in their professional context; (c) A CHAT analysis [7] of the stories, revealing activity systems, including norms and rules about cybersecurity, and potential tensions within those systems [8].

3 ON COLLABORATION

Generally, the process of collaboration involves participants in a dynamic process, during which issues arise and choices have to be made. The opportunistic nature of collaboration renders both process and outcomes unpredictable. The element of surprise and creativity provides many opportunities for learning, about the process, about the domain, about each other. The question what ‘good’ collaboration for incident- and risk management looks like, concerns relating dynamic processes (of collaboration) to an intrinsically dynamic domain (of cybersecurity). In the first place, it is about how to get people involved into such collaboration, in professional settings, individuals who work at different locations, often in different organisations. Such a question could be addressed in a CSCW framework, where CSCW is about designing systems meeting support requirements for cooperative work arrangements. More specifically, this is a question about articulation of distributed activities [9, 10].

How can technology support these cooperative work arrangements, and what would be indicators of good quality collaboration in this domain? These are the actual questions we are working on at the current stage of the project. We will propose a few suggestions, and end with some general comments.

3.1 Examples of collaborative scenarios

In our interpretation, collaboration be stakeholders can be described as three general types. CS-CONNECT will be designed to support the main activities in these scenarios.

1. Cybersecurity issue in the Ecosystem: This scenario addresses an issue in the regional network of organizations. A cybersecurity issue is found in this ecosystem, which requires the collaboration and the coordinated actions of the organizations (some of them, who depend on the problem component) involved. In this scenario, the CS-CONNECT collaboration environment is meant to be designed to fully support the jointly addressing such problems, with respect to incident-handling and risk management. CS-CONNECT is expected to provide smooth coordination of activities, effective communication and information sharing, for improved situational awareness at the ecosystem level.
2. Cybersecurity issue in an Organization: The scenario addresses an issue that is occurring to an organization within the ecosystem. It is a cybersecurity-related question or problem that the organization cannot resolve and wants to discuss with the others. In this scenario, CS-CONNECT is meant to facilitate sharing relevant information from one organization to the other participants (which is no trivial matter, for reasons of privacy and competition), and other organizations can react by sharing common relevant experiences. The CS-CONNECT environment is expected to provide smooth coordination, effective communication and guided information sharing, improving the collective ability of the ecosystem to react to issues, be them incident-handling or risk management.
3. Knowledge Management: The scenario addresses the ability to jointly build shared organizational memories (repositories) from relevant experiences within the ecosystem. This could start with reports (stories) of experiences that may later grow and evolve with relevant comments, metadata, links to incidents/issues or policies in some organization, and is also meant to support the collaboration around real experiences. The CS-CONNECT environment is meant to support the evolution of the experiences into possible issues like incident-handling or risk management, or into development and design of new improved security policies by organizations and by the ecosystem. The environment is expected to allow the reporting of experiences from the organizations, supporting joint story construction where semi-structured collaborative editing, tagging, linking, adding metadata, etc.

3.2 Comments on analyzing the quality of collaboration

1. In this particular project, we are faced with the possibility of many collaborations, with many potential differences in urgency, experience, motivation, goal types, heterogeneous participants, etc. This raises the general concern that we should also address awareness of collaboration, or improving collaboration, in the sense of knowing how to collaborate in different contexts of objectives and participants. There is no single type of good collaboration, and perhaps there is no recipe. Do analytics make any sense in such cases? Shouldn't we look for what constitutes the required collaborative agency?
2. Andriessen & Baker [11] propose and elaborate conditions for collaboration, which is not the same as indicators of quality. In the domain of cybersecurity, the ultimate challenge for all appears to be the realisation that cybersecurity is a community problem, only to be solved at the community level. This realisation only comes slowly, i.e., requiring various assignments and collaborations. We call this cybersecurity awareness: understanding cybersecurity in a broader sense (i.e., nature, cause, and management), including the ability to

link it to issues in different contexts. What happens at the level of a single task may not matter, as long as it leads to greater awareness in the broader sense of the term. What would be 'long-term indicators' for this?

3. Meier et all [12, 13] proposed five aspects as central for successful collaboration: communication (sustaining mutual understanding, dialogue management), joint information processing (information pooling, reaching consensus), coordination (task division, time management, technical coordination), interpersonal relationship (reciprocal interaction), and motivation (individual task orientation). These are evidence-based dimensions, for computer-supported communication, to which no doubt some can be added, such as inclusion and shared values. Behavioral indicators of quality for each of these dimensions may overlap, or are hard to come by. The question here is: does all of this add up, or are we happy with some degree of each? Shouldn't we start with a theory instead of with symptoms?
4. The qualities of good collaboration depend on who is considering the task objectives. There can be tension between what participants in a group perceive as good collaboration and the collaboration that is needed for the best possible outcome. Should we allow (big) data telling us how good our collaboration is, or should be? How do we view the user's perception on the quality of collaboration?

4 REFERENCES

1. Furnell, S., Vasileiou, I.: Chapter 1: A Holistic View of Cybersecurity Education Requirements. In: Vasileiou, I. and Furnell, S. (eds.) Cybersecurity Education for Awareness and Compliance: pp. 1–18. IGI Global (2019). https://doi.org/10.4018/978-1-5225-7847-5.
2. Schaberreiter, T., Roning, J., Quirchmayr, G., Kupfersberger, V., Wills, C., Bregonzio, M., Koumpis, A., Sales, J.E., Vasiliu, L., Gammelgaard, K., Papanikolaou, A., Rantos, K., Spyros, A.: A Cybersecurity Situational Awareness and Information-sharing Solution for Local Public Administrations Based on Advanced Big Data Analysis: The CS-AWARE Project. In: Bernabe, J.B. and Skarmeta, A. (eds.) Challenges in Cybersecurity and Privacy – the European Research Landscape. pp. 149–180. River Publishers, Gistrup (DK) (2019).
3. Schaberreiter, T., Quirchmayr, G., Papanikolaou, A.: A Case for Cybersecurity Awareness Systems. In: Andriessen, J., Schaberreiter, T., Papanikolaou, A., and Röning, J. (eds.) Cybersecurity Awareness. pp. 1–19. Springer International Publishing, Cham (2022). https://doi.org/10.1007/978-3-031-04227-0_1.
4. Carroll, J.M.: Five Reasons for Scenario-Based Design. IEEE Proceedings of the 32nd Hawaii International Conference on System Sciences. 12 (1999).
5. Bruner, J.: The Narrative Construction of reality. Critical Inquiry. 18, 1–21 (1991).
6. Wills, C.: The Socio-Technical Approach to Cybersecurity Awareness. In: Andriessen, J., Schaberreiter, T., Papanikolaou, A., and Röning, J. (eds.) Cybersecurity Awareness. pp. 21–43. Springer International Publishing, Cham (2022). https://doi.org/10.1007/978-3-031-04227-0_2.
7. Engeström, Y.: Expansive Learning at Work: Toward an activity theoretical reconceptualization. Journal of Education and Work. 14, 133–156 (2001). https://doi.org/10.1080/13639080020028747.
8. Andriessen, J., Pardijs, M.: Story Telling. In: Andriessen, J., Schaberreiter, T., Papanikolaou, A., and Röning, J. (eds.) Cybersecurity Awareness. pp. 45–67. Springer International Publishing, Cham (2022). https://doi.org/10.1007/978-3-031-04227-0_3.
9. Schmidt, K., Bannon, L.: Constructing CSCW: The First Quarter Century. Computer Supported Cooperative Work (CSCW). 22, 345–372 (2013). https://doi.org/10.1007/s10606-013-9193-7.
10. Strauss, A.: The articulation of project work: An organizational process. The Sociological Quarterly. 29, 163–178 (1988).
11. Andriessen, J., Baker, M.: On collaboration: personal, educational and societal arenas. Brill Sense, Leiden ; Boston (2020).
12. Meier, A., Spada, H., Rummel, N.: A rating scheme for assessing the quality of computer-supported collaboration processes. Computer Supported Learning. 2, 63–86 (2007). https://doi.org/10.1007/s11412-006-9005-x.
13. Rummel, N., Deiglmayr, A., Spada, H., Kahrimanis, G., Avouris, N.: Analyzing Collaborative Interactions Across Domains and Settings: An Adaptable Rating Scheme. In: Analyzing Interactions in CSCL. pp. 367–390. Springer, Boston, MA (2011). https://doi.org/10.1007/978-1-4419-7710-6_17.