Information Security Practices in Inter-organizational Collaboration

Early-stage paper

Hanna Paananen
University of Jyvaskyla
hanna.k.paananen@jyu.fi

ABSTRACT

This early-stage paper considers information security practices within networks of partner organizations. This topic is currently emerging in the information security management literature as in the past, the focus has been on organizations, and partners were discussed as "external stakeholders." This paper identifies issues that arise when there is a need to manage information security issues beyond the organization's boundaries. Then it moves to examine practices of inter-organizational collaboration and their relevance to information security management. The paper concludes that this topic should be further explored, and better support should be provided for creating practices for inter-organizational information security management.

Keywords

Information security management, security practices, inter-organizational collaboration.

INTRODUCTION

The business world is transforming through information technology and data networks (Von Solms, 1996). They enable each industry, at its own pace, to change from clear-cut structures and boundaries towards organizations that operate in ever-changing networks of partnerships and

outsourcing relationships (Ashenden, 2008). They engage in an inter-organizational collaboration that is not controlled through simple hierarchical or market mechanisms (Majchrzak et al., 2015). These novel ways of operating challenge many traditional information security management (ISM) practices.

Traditionally ISM between organizations has been seen as a contractual issue where relationships can be clearly defined through competition and supply chains (Sindhuja, 2014). For example, the ISO27002:2013 standard uses the words “agree” and “mandate” in its recommendations (The International Organization for Standardization, 2013), which can be construed as expectations for contracts and a position of authority of one partner over another. However, the landscape is changing, and organizations operate in increasingly complex partner networks that require new approaches for inter-organizational ISM (Sindhuja, 2014). External themes beyond organizational boundaries have been scarce in cyber security research literature but have recently gained more attention (Yeoh et al., 2022).

Cyber security attacks are on the rise, and as a recent development, they are increasingly carried out as new types of supply chain attacks (Lella et al., 2021). This development forces security management to change from focusing on predetermined threats towards giving more weight to having a response towards unknown threats (Baskerville et al., 2014; Sutcliffe, 2011). Organizations no longer operate in such a stable market that they can manage information security solely with predetermined rules; instead, they must trust their employees to make information security decisions (Baskerville et al., 2014; Paananen et al., 2020; Siponen & Iivari, 2006). A key component of a resilient organization is its members, who are constantly alert and on the look for anything suspicious (Sutcliffe, 2011). This puts the focus on people and their competencies in identifying security issues. The people working with information security issues

must be capable of continuous learning to stay on top of things. However, sharing information security knowledge is often seen more as a marketing effort to transmit messages to a passive audience rather than a collaborative effort with the aim of changing behavior or practices (Alshaikh et al., 2021; Anderson et al., 2022).

In this research-in-progress paper, we will first examine how information security management across partnership networks is addressed in the research literature. Next, we focus on understanding how creating, transferring, and learning knowledge occurs in the practices of inter-organizational cooperation. Lastly, we discuss future research directions and offer conclusions.

INFORMATION SECURITY IN NETWORKS OF ORGANIZATIONS

ISM literature is generally focused on the organization as the scope of the examination. For example, in the information security policy literature, the external stakeholders (such as partners and customers) are often mentioned but rarely discussed in depth (Cram et al., 2017; Paananen et al., 2020). However, for many organizations, there may be a significant need to exchange business-critical information within a network of partner organizations. Here we consider some information security concerns that are specific to inter-organizational collaboration.

Partner networks may combine complex collaboration structures where each organization has its specific role in adding value. The organizations may be very different in type and size and not form a clearly identifiable value chain. The danger of having "weak links" in the network motivates more security-aware organizations to try to manage information security beyond the organizational boundaries (Russell & Saldanha, 2003; Sindhuja, 2014; Von Solms, 1996). Then

again, a good posture on information security may be seen as part of the corporate image, and being the weak link in the eyes of the partners is not desirable (Sindhuja, 2014).

Like an organization's internal ISM, the inter-organizational ISM requires managing people, processes, and technology (Ashenden, 2008; Sindhuja, 2014). However, the management practices that might work within a single organization may not be applicable to a network of organizations (Niemimaa, 2016). When dealing with the inter-organizational aspects of cybersecurity, it is strongly affected by aspects of the inner and outer context. Elements of the outer context become especially important, including economic, political, social, and sectoral aspects, in addition to competitors, customers, and partners (Karyda et al., 2005; McFadzean et al., 2007; Sindhuja, 2014). As the power structures in collaboration efforts may be exceedingly complex, the adoption of joint management practices may be difficult.

Organizations that operate in partnership networks face the challenge of not being completely in control of their information assets. In close partnerships, the inter-organizational information flows may include some of the most business-critical information of these organizations (Sindhuja, 2014). This again creates a challenge to define the organizational policies in a way that allows sharing of sensitive information. When partner organizations have different policies for their employees about sharing information, it may lead to tensions in the collaboration. (Jarvenpaa & Majchrzak, 2016.)

Organizations have the need to share information with their partners, but this poses a challenge for information security. The need for fast and flexible information exchange necessitates putting more information security responsibility on the people who work in these processes (Ashenden, 2008). Sharing security information as well would benefit the information security posture of the partnership but may only happen if there are financial incentives such as gaining customers or

better competitiveness (Gal-Or & Ghose, 2005). Cyber threat information sharing is a complex task that requires competencies not only in knowing what to share and how but also why and to whom (Brilingaite et al., 2022).

Learning and adjusting is a central part of maintaining information security. The collaboration between organizations changes when people and organizations join and leave the network, and new needs and goals arise (Majchrzak et al., 2015). Threats and regulations change as well, and it may be challenging to make sure the organization's security investments are up to date (Saleh, 2011). These exceptional situations can create business opportunities that require readjusting security procedures (Siponen & Iivari, 2006). Possibly due to this need to adapt, inter-organizational policies or contracts may have vague expressions such as 'regulations must be adhered to' but lack instructions on how this should be done (Karlsson et al., 2017). This requires good adjusting capabilities from the collaborators, who must be able to change their course of action to meet the requirements of the partner network and their own organization (Jarvenpaa & Majchrzak, 2016).

The ISM efforts within a partner network must be dynamic and respond to changes in the operating environment of the entire network. Information security may not be reached with prevention measures alone, but effective response strategies are also needed (Baskerville et al., 2014). There is a need to coordinate joint plans to communicate and recover from disasters (Russell & Saldanha, 2003), which may be challenging due to the lack of a central authority.

KNOWING AND LEARNING IN PRACTICE

We often like to talk about organizational matters in terms of business units, processes, roles, policies, and strategies. These concepts are used to consider and communicate complex issues in

a more simplified way through categorizing and generalizing (Vergne & Wry, 2014). However, the complexity behind these concepts, the practices, is what affects the outcomes of operations. The information security-related processes increase security when the people executing them engage in practices where they learn and use knowledge to make good decisions (Majchrzak & Jarvenpaa, 2010; Niemimaa, 2016; Siponen, 2006).

When we look beyond roles and processes into the groups of individuals performing practices, we can begin to understand knowledge in cybersecurity collaboration at the grassroots level. The practice perspective implies that meaning-making and knowing happen when we experience the world and participate in interconnected practices (Marabelli & Newell, 2012; Wenger, 1998, p. 62). Inter-organizational cybersecurity management entails a complex social setting where information is shared and learned.

Cybersecurity management is often described through the tasks that must be performed rather than the people engaged in the activity(Anderson et al., 2022). Cybersecurity professionals' competencies, i.e., the knowledge, skills, and attitudes (Anderson et al., 2022, p. 2), affect how these tasks are performed. The knowledge requirement is often described quite vaguely, involving understanding the threat environment, operations of controls, and how they perform (Anderson et al., 2022; Pöyhönen et al., 2021). Skills like analyzing, identifying, managing, and overseeing are typical tasks for cybersecurity managers (Anderson et al., 2022). Attitudes like desires and values can manifest in the way the person perceives risk and the importance of information technology which may lead to very different strategies for cybersecurity even in seemingly similar organizations (Anderson et al., 2022; McFadzean et al., 2007).

Practices are not so much connected to security management roles as they are to individuals enacting them. People have different competencies which are needed when solving information

security issues (Anderson et al., 2022). When an individual participates in information security collaboration, this shapes their own experience but at the same time provides the possibility to shape the practices of the community (Wenger, 1998, p. 55). If there is a lack of certain competencies in the group, they may not be able to work efficiently together to counter threats (Bartnes & Moe, 2017).

Social practice is what people develop in an organization in order to complete their work, for example, when complying with information security rules. The structure and meaning of these practices are both explicit and tacit (Wenger, 1998, p. 47). The explicit part consists of things like policy documentation, privacy notices in systems, training courses, and using encrypted email. The tacit part of practices is something we take for granted and think of it as common knowledge. People and groups have tacit knowledge about business processes which is needed for adapting information security requirements for specific situations (Ashenden, 2008). However, tacit knowledge requires reinforcement in the social setting to exist (Wenger, 1998, p. 47), which means that maintaining a sound information security posture requires ongoing social activity around the subject. Within organizations, the repetition is built into the ISM but can easily be missing in inter-organizational collaboration if the operations rely on highly abstract contracts.

Knowing and sharing knowledge is materially entangled, which means it is connected with objects or artifacts (Orlikowski, 2006). When organizations write contracts or agree on procedures for information security collaboration, it is a process of giving form to the experience of collaboration (Wenger, 1998, p. 58). They provide common ground for the participants to create and negotiate the meaning of shared practices (Wenger, 1998, p. 65). Documented policies and contracts also give form to conflicts between practices. The people participating in the

collaboration must mediate between sometimes opposing requirements from organization policies and network needs (Jarvenpaa & Majchrzak, 2016). In these situations, the practices relating to organizational policies may override collaboration practices if they are more explicitly expressed and materially shared.

Organizations' information security practices differ, as do their abilities to utilize shared threat information. As the meaning of threat information is produced in the security practices of each company, negotiation between organizations is needed to share information in a way that is relevant to the partners (Wenger-Trayner & Wenger-Trayner, 2015, p. 17). In addition to a need for sharing knowledge within a partner network, there is also the need to reinforce the competencies of all participants so that the practices in information-sharing become mutually beneficial.

Inter-organizational collaboration requires crossing many boundaries. In partner networks, the organizations represent different industries with different bodies of knowledge and organizational cultures. When people cross organizational boundaries, it may lead to confusion and misunderstanding (Wenger-Trayner & Wenger-Trayner, 2015, p. 17). Responsive information security, on the other hand, requires enough familiarity with the normal mode of operating that it is possible to sense even the slightest of abnormalities (Sutcliffe, 2011). Creating familiarity with the security situation outside the boundaries of one's own organization requires engaging with the partners, forming an image of the network, and aligning competencies in coordination (Wenger-Trayner & Wenger-Trayner, 2015, pp. 20–21).

DISCUSSION

This paper goes beyond the view of an organization as the unit of study in information security management. We look at the operational environment and partner network as the broader context, where organizations must try to control the balance between sharing and protecting information. Then we move closer to inspect the collaboration and discover individuals engaged in practices where a common understanding of the situation is created, and different ways of working are reconciled.

Inter-organizational cybersecurity challenge	***Practice point-of-view***
Weak links	*Lack of required competencies*
Inter-organizational ISM	*Need for repeated practices*
Obstructing organizational policies	*Materia anchoring practices*
Disclosing information	*Negotiating mutually beneficial practices*
Adjusting to changes	*Learning beyond boundaries*

Table 1: The alignment of inter-organizational information security challenges and practice point of view

The asymmetry of information security capabilities within a partner network may cause additional risks to other organizations. This raises the need to coordinate the capabilities within the networks. This does not only mean ensuring that certain roles are issued in every organization but that the people in these roles have the knowledge, skills, and attitudes required to manage information security beyond organizational boundaries (Brilingaite et al., 2022).

Information security activities between organizations are usually described as a contractual issue rather than an ongoing joint ISM program. Having a mutual understanding of the importance of repeated practices could, however, support the constant improvement of capabilities. Adapting well-established practices in case of strategy changes or new people is easier than starting afresh when the network changes.

Vague partnership contracts combined with strict organizational policies may create difficult situations for the people operating with the partners. The creation of mutually beneficial practices between collaborators could be enabled by considering the materiality of the practices beyond contracts. There is a need for shared (virtual or concrete) spaces, stories, documents, and rituals. They create a common ground that helps translate meanings beyond organizational boundaries. For example, Majchrzak and Jarvenpaa (2010) suggested an information system that could support people in creating a safe context for ad hoc information sharing across organizational boundaries.

Information security talk often gravitates towards confidentiality, while integrity and availability are just as important. The sharing of information is vital to collaborating organizations, but when information security is concerned, it often creates barriers to progress. Sharing threat information may be even more problematic to organizations due to the fear of damage to the corporate image. A continuous effort to build trust is needed to ensure that the collaboration remains beneficial to all parties. Further, the act of sharing threat information may not be enough to increase security; instead, there is a need to support translating the security knowledge from one organization to another (Marabelli & Newell, 2012).

Due to the dynamic nature of partner networks and threat environment, there is a continuous need to be able to adjust to changes. This is not possible if the collaborating people do not have

enough opportunities to familiarize themselves with this area beyond their organizational boundaries. The organizations and the collaborating community must be aware that people must learn about information security collaboration practices. This requires creating opportunities for learning and ensuring continuity when people in different roles change. The collaboration should also include a wider coverage of different roles since, in the case of an emergency, there is a need for smooth cooperation between experts across business areas and technologies (Bartnes & Moe, 2017).

Future directions

This examination of the need for ISM in partnership networks raises the question if traditional policies and contracts are enough to respond to the challenges of forming information security practices in inter-organizational collaboration. Materiality and boundary objects are an integral part of practices and the knowledge transfer within them, which could warrant exploring novel types of facilitating artifacts. These artifacts could include principles that help understand and improve collaboration efforts (Marabelli & Newell, 2012).

Action design research is a good fit for this research agenda since it focuses on the creation of artifacts that emerge from the context of the organization. The method allows for the artifact to emerge from the interactions between individuals within the action of forming practices for inter-organizational ISM. The goal is to create an artifact with a network of organizations and it should have the functions to solve some of the issues identified before, such as the repetition of practices and social learning. The artifact will be developed in iterations, including workshops with the organization network. (Sein et al., 2011.)

CONCLUSION

This research-in-progress paper discussed the issues relating to ISM in inter-organizational collaboration. The focus of the analysis was set on understanding the tensions that arise in the practices of information security beyond organizational boundaries. Five themes of issues in inter-organizational information security collaboration were identified and matched with the practice point of view. This area is not heavily researched before from this perspective and warrants further study both in analyzing existing literature and creating new approaches to support inter-organizational ISM. To this end, an action design research study is proposed in order to create an artifact to solve the identified issues.

REFERENCES

Alshaikh, M., Maynard, S. B., & Ahmad, A. (2021). "Applying social marketing to evaluate current security education training and awareness programs in organisations," *Computers and Security*, *100*. https://doi.org/10.1016/J.COSE.2020.102090

Anderson, A. B., Ahmad, A., & Chang, S. (2022). "Competencies of Cybersecurity Leaders: A Review and Research Agenda," *ICIS 2022 Proceedings*, 1–17. https://aisel.aisnet.org/icis2022/security/security/9

Ashenden, D. (2008). "Information Security management: A human challenge?" *Information Security Technical Report*, *13*(4), 195–201. https://doi.org/10.1016/j.istr.2008.10.006

Bartnes, M., & Moe, N. B. (2017). "Challenges in IT security preparedness exercises: A case study," *Computers and Security*, *67*, 280–290. https://doi.org/10.1016/J.COSE.2016.11.017

Baskerville, R., Spagnoletti, P., & Kim, J. (2014). "Incident-centered information security: Managing a strategic balance between prevention and response," *Information & Management*, *51*(1), 138–151. https://doi.org/10.1016/j.im.2013.11.004

Brilingaite, A., Bukauskas, L., Juozapavičius, A., & Kutka, E. (2022). "Overcoming information-sharing challenges in cyber defence exercises," *Journal of Cybersecurity*, *8*(1), 1–9. https://doi.org/10.1093/CYBSEC/TYAC001

Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2017). "Organizational information security policies: a review and research framework," *European Journal of Information Systems*, *26*(6), 605–641. https://doi.org/10.1057/s41303-017-0059-9

Gal-Or, E., & Ghose, A. (2005). "The Economic Incentives for Sharing Security Information," *Information Systems Research*, *16*(2), 186–208. https://doi.org/10.1287/isre

Jarvenpaa, S. L., & Majchrzak, A. (2016). "Interactive self-regulatory theory for sharing and protecting in interorganizational collaborations," *Academy of Management Review*, *41*(1), 9–27. https://doi.org/10.5465/amr.2012.0005

Karlsson, F., Hedström, K., & Goldkuhl, G. (2017). "Practice-based discourse analysis of information security policies," *Computers and Security*, *67*. https://doi.org/10.1016/j.cose.2016.12.012

Karyda, M., Kiountouzis, E., & Kokolakis, S. (2005). "Information systems security policies: a contextual perspective," *Computers & Security*, *24*(3), 246–260. https://doi.org/10.1016/j.cose.2004.08.011

Lella, I., Theocharidou, M., Tsekmezoglou, E., Malatras, A., Garcia, S., & Valeros, V. (2021). *ENISA Threat Landscape for Supply Chain Attacks*. https://doi.org/10.2824/168593

Majchrzak, A., & Jarvenpaa, S. (2010). "Safe Contexts for Interorganizational Collaborations Among Homeland Security Professionals," *Journal of Management Information Systems*, *27*(2), 55–86. https://doi.org/10.2753/MIS0742-1222270202

Majchrzak, A., Jarvenpaa, S. L., & Bagherzadeh, M. (2015). "A Review of Interorganizational Collaboration Dynamics," In *Journal of Management* (Vol. 41, Issue 5, pp. 1338–1360). SAGE Publications Inc. https://doi.org/10.1177/0149206314563399

Marabelli, M., & Newell, S. (2012). "Knowledge risks in organizational networks: The practice perspective," *Journal of Strategic Information Systems*, *21*(1), 18–30. https://doi.org/10.1016/j.jsis.2011.11.002

McFadzean, E., Ezingeard, J.-N., & Birchall, D. (2007). "Perception of risk and the strategic impact of existing IT on information security strategy at board level," *Online Information Review*, *31*(5), 622–660. https://doi.org/10.1108/14684520710832333

Niemimaa, E. (2016). "A practice lens for understanding the organizational and social challenges of information security management," *PACIS 2016 Proceedings*. https://aisel.aisnet.org/pacis2016/58

Orlikowski, W. J. (2006). "Material knowing: The scaffolding of human knowledgeability," *European Journal of Information Systems*, *15*(5), 460–466. https://doi.org/10.1057/PALGRAVE.EJIS.3000639

Paananen, H., Lapke, M., & Siponen, M. (2020). "State of the art in information security policy development," *Computers & Security*, *88*(1), 1–14. https://doi.org/10.1016/j.cose.2019.101608

Pöyhönen, J., Rajamäki, J., Nuojua, V., & Lehto, M. (2021). "Cyber Situational Awareness in Critical Infrastructure Organizations," In T. Tagarev, K. T. Atanassov, V. Kharchenko, & J. Kacprzyk (Eds.), *Digital Transformation, Cyber Security and Resilience of Modern Societies* (Vol. 84, pp. 161–178). Springer, Cham. https://doi.org/10.1007/978-3-030-65722-2_10

Russell, D., & Saldanha, J. (2003). "Five tenets of security-aware logistics and supply chain operation," *Transportation Journal*, *42*(4), 44–54. https://www.jstor.org/stable/20713540

Saleh, M. (2011). "Information Security Maturity Model," *International Journal of Computer Science and Security*, *5*(3), 316–337.

Sein, M., Henfridsson, O., Purao, S., Rossi, M., & Lindgren, R. (2011). "Action design research," *MIS Quarterly*, *35*(1), 37–56.

Sindhuja, P. N. (2014). "Impact of information security initiatives on supply chain performance an empirical investigation," *Information Management and Computer Security*, *22*(5), 450–473.

Siponen, M. (2006). "Information security standards focus on the existence of process, not its content," *Communications of the ACM*, *49*(8), 97–100. https://doi.org/10.1145/1145287.1145316

Siponen, M., & Iivari, J. (2006). "Six Design Theories for IS Security Policies and Guidelines," *Journal of the Association for Information Systems*, *7*(7), 445–473. https://doi.org/10.17705/1jais.00095

Sutcliffe, K. M. (2011). "High reliability organizations (HROs)," *Best Practice & Research Clinical Anaesthesiology*, *25*(2), 133–144. https://doi.org/10.1016/J.BPA.2011.03.001

The International Organization for Standardization. (2013). ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls. In *ISO.org [Online]* (Vol. 2013, p. 80).

Vergne, J. P., & Wry, T. (2014). "Categorizing Categorization Research: Review, Integration, and Future Directions," *Journal of Management Studies*, *51*(1), 56–94. https://doi.org/10.1111/JOMS.12044

Von Solms, R. (1996). "Information security management: The second generation," *Computers & Security*, *15*(4), 281–288. https://doi.org/10.1016/0167-4048(96)88939-5

Wenger, E. (1998). *Communities of Practice: Learning, meaning, and identity*. Cambridge University Press.

Wenger-Trayner, E., & Wenger-Trayner, B. (2015). "Learning in a landscape of practice," In E. Wenger-Trayner, M. Fenton-O'Creevy, S. Hutchinson, C. Kubiak, & B. Wenger-Trayner (Eds.), *Learning in landscapes of practice : boundaries, identity, and knowledgeability in practice-based learning* (pp. 13–29). Routledge.

Yeoh, W., Wang, S., Popovič, A., & Chowdhury, N. H. (2022). "A systematic synthesis of critical success factors for cybersecurity," *Computers & Security*, *118*, 102724. https://doi.org/10.1016/J.COSE.2022.102724