Inter-Organisational Information Sharing – Between a Rock and a Hard Place

F. Karlsson, E. Kolkowska, K. Hedström, and M. Frostenson

Örebro University School of Business, SE-701 82 Örebro, Sweden
e-mail: {fredrik.karlsson; ella.kolkowska; karin.hedstrom;
magnus.frostenson}@oru.se

Abstract

Although inter-organisational collaboration is common, most information security (IS) research has focused on IS issues within organisations. Confidentiality, integrity of data and availability (CIA) and responsibility, integrity of role, trust, and ethicality (RITE) are two sets of principles for managing IS that have been developed from an intra-organisational, rather static, perspective. The aim of this paper is thus to investigate the relation between the CIA and RITE principles in the context of an inter-organisational collaboration, i.e., collaboration between organisations. To this end we investigated inter-organisational collaboration and information sharing concerning Swedish cooper corrosion research in the field a long-term nuclear waste disposal. We found that in an inter-organisational context, responsibility, integrity of role and ethicality affected the CIA-principles, which in turn affected the collaborating actors' trust in each other over time.

Keywords

Information security, inter-organisational, CIA, RITE

1. Introduction

Although in today's global world, collaboration between different organisations is common and necessary, most of the research within the information security (IS) field focuses on IS issues within an organisation. A missing focus is thus IS in an inter-organisational setting (McLaughlin and Gogan, 2014). An inter-organisational collaboration entails integrated business processes and sharing of information that in an intra-organisational setting is considered an organisation's own property. Such changes raise new IS challenges related to the common technical infrastructure (technical aspects), common policies and procedures (formal aspects), as well as to goals, beliefs and values about how things should be done in relation to IS (informal aspects) (Dhillon et al., 2014).

While the international standard ISO 27002 (ISO, 2013) provides some practical guidelines how to maintain confidentiality, integrity and availability (CIA) of information by establishing technical and formal security safeguards in inter-organisational collaborations, the informal aspects are not considered. In response to CIA, Dhillon and Backhouse (2000) offered RITE (Responsibility, Integrity, Trust, and Ethicality), which can be seen as alternative, or complementing, principles. Both CIA and RITE are developed from an intra-organisational, rather static, perspective,

and while CIA focuses the objectives of IS, RITE offers a way of managing IS. The aim of this paper is thus to investigate the relation between the CIA and RITE principles in the context of an inter-organisational collaboration. To this end we investigated inter-organisational collaboration and information sharing concerning Swedish cooper corrosion research in the field a long-term nuclear waste disposal.

The paper is structured as follows. Section 2 contains a discussion about existing research. First we address inter-organisational IS research, and second we look into the CIA and RITE principles. In section 3, we present our research design. Section 4 reports on our analysis of the case study. Finally, the paper ends with a discussion in Section 5 and a short conclusion in Section 6.

2. Related research

2.1. Inter-organisational research

Research focusing IS in the context of inter-organisational collaboration is scant (McLaughlin and Gogan, 2014). Most of the existing papers seem to target technical and formal aspects of IS, and we have only come across a few papers that deal with informal aspects. Technical aspects of IS in the context of inter-organisational collaboration are mostly studied in relation to access controls (e.g. Chen et al., 2007, Kayem et al., 2011) and architectural framework (e.g. Djordjevic et al., 2007, Yuan et al., 2009, Mao et al., 2008). When it comes to formal aspects a lot of effort has been put into researching the area of outsourcing (e.g. Pemble, 2004, Dommun, 2008, Berghmans and van Roy, 2011).

The few studies focusing informal aspects of IS in the context of inter-organisational collaboration are related to outsourcing (Tsohou et al., 2007, Robertson et al., 2010, Bahl et al., 2011). Bahl et al. (2011) identified cultural challenges in outsourcing to India and Tsohou et al. (2007) presented a conceptual framework in order to track down and manage cultural differences between organisations in outsourcing ventures. In the third study, Robertsson et al. (2010) investigated moral reasoning related to outsourcing decisions and concluded that from this perspective IS issues are more important than quality issues for the stakeholders. Against this backdrop we can conclude that to the best of our knowledge, principles of IS with regard to inter-organisational collaboration has not been researched at all and thus there is a need for more studies within this area. Our study contributes to this research by investigating the relation between the CIA and RITE principles in the context of an inter-organisational collaboration.

2.2. Principles of information security

Previous research and practice has identified a number of principles for managing IS in an organisation (Dhillon, 2007). Although it is important to understand the meaning and origin of these principles, such a discussion is beyond the scope of this paper. The principles of CIA are the most known and most frequently used within IS (Dhillon, 2007). According to ISO 27 001 (ISO, 2005) confidentiality states that

information is not made available or disclosed to unauthorised individuals, entities or processes. Integrity of data means the of safeguarding the accuracy and completeness of assets. Availability is defined as information that is accessible and usable upon demand by an authorised entity (ISO, 2005). Dhillon and Backhouse (2000) argued that the CIA-principles are useful and important primarily in relation to formal and technical parts of IS management in an organisation, while they are insufficient when dealing with informal aspects of IS management. Therefore they offered additional principles, known as Responsibility, Integrity of role, Trust, and Ethicality (RITE). Responsibility means that members of an organisation, or in our case members of an inter-organisational collaboration, know and understand the existing rules and responsibilities. Based on that knowledge, these members are able to develop their own security practices in unexpected situations; practices that are in line with organisational rules and responsibilities. Integrity means having feelings of integrity as a member of an organisation and feeling loyalty to that organisation. Trust means that members in an organisation are not controlled but instead are trusted to act according to the organisation's norms and accepted patterns of behaviour. Ethicality means that members of an organisation should act according to ethical principles.

3. Research method

3.1. Case description

The relation between CIA and RITE was studied in the context of a reference group on copper corrosion research with regard to long-term nuclear waste disposal in Sweden. The reference group was established 2010, after researchers at the Royal Institute of Technology (KTH) in Stockholm found that copper can corrode in oxygen-free water indicating that the method for nuclear waste disposal advocated by the Swedish Nuclear Fuel and Waste Management Company (SKB) may be flawed. SKB was sceptical to the results and wanted to investigate them further. Two research projects were planned. The first at SP Technical Research Institute of Sweden on copper wires that had been in a test tube for 20 years and the other research project was planned at Uppsala University with the aim to repeat the experiments of the KTH researchers. The reference group, which was established on an initiative of SKB, was supposed to have full insight in the design and accomplishments of these experiments and also a possibility to review SKB's reports regarding these experiments before being published. SKB promised full transparency and openness regarding the experiments. The reference group consisted of researchers (KTH), SKB representatives, environmental groups, and representatives of public interests, such as politicians and civil servants of the local municipalities and regions affected by the nuclear waste deposit. In October 2012, an environmental group, the Swedish NGO Office for Nuclear Waste Review (MKG) officially left the group motivating this with SKB's unwillingness to improve public transparency into SKB's entire work with copper corrosion. MKG claimed that the transparency that SKB offered was far from what they promised when the reference group was established. In 2013, the KTH researchers decided to leave the group because of a conflict regarding the process of reviewing a preliminary report from the experiments. The KTH researchers claimed that they had been instructed by SKB to

neglect some research findings that would influence the review of the report. They argued that such a review was unacceptable within established scientific practice. We can see that the different views on how the information should be handled and who should be trusted with sensitive information prevented the reference group from achieving its aim. Therefore, we found this case suitable for studying the relation between CIA and RITE in the context of inter-organisational collaboration. A detailed description of the case background can be found in Andersson (2014).

3.2. Data collection and data analysis

Given that several different views on the collaboration and its outcome exist, our study focused on perceived IS (Oscarson, 2007). The empirical data consists of interviews with key members of the reference group on copper corrosion and protocols from this group. The interviews took about one hour each, and were conducted by phone, tape-recorded, and subsequently transcribed. We chose interviews as data collection method as we were "interested in gaining a rich and inclusive account of the participant's experience" (Polkinghorne, 2005). In our case, reference group members' experiences about information sharing about copper corrosion differ. In order to deepen our understanding, as well as allow for multiple perspectives, we chose to include members with different and contrasting views on their role in the reference group. In order to validate the interviews, we also analysed 17 protocols from reference group meetings between 2010 and 2014.

The analysis was conducted in four steps. First, we searched for respondents' statements about information sharing in the collected empirical data (interviews and protocols). Second, these statements were subsequently classified according to the principles of CIA or RITE. Third, we sorted these statements with regard to time. Fourth, we searched for differences in the respondents' views on the collaboration and in relation to CIA or RITE. The statements reported in the paper were chosen for illustrative purposes. In order to capture multiple perspectives, we have chosen statements from different respondents.

4. Analysis

In this section we take a closer look at how the three actors perceived the collaboration with regard to IS. We do so by structuring the analysis according to the RITE and CIA-principles, and provide illustrative empirical examples related to these principles. An overview of the analysis is shown in Table 1. The table is structured into four columns. The leftmost column contains the principles we address, the second to fourth columns contain the different actors' views on each of the principles. Starting from the left we find SKB, in the middle column MKG, and finally KTH. In addition, we analyse the case based on two snapshots in time to capture the dynamics of the case; (T_1) when the reference group was initiated and (T_2) when the reference group was dissolved.

Responsibility: The three actors had different responsibilities in the collaboration. Throughout the reference group (T_1-T_2) SKB was the process owner. They had

responsibility to investigate whether or not copper corroded in oxygen-free environments, and to "assess that the process did not affect safety of the long-term disposal of nuclear waste" (Protocol May 19, 2010). MKG joined the reference group (T_1) with the intention to safeguard quality of the process of selecting a technical solution for disposal of nuclear waste. Hence, they viewed themselves as process reviewers. KTH played the role as scientific reviewer and advisor to the projects that were to be executed. "We realised that we were the only ones who could comment on them [the results] scientifically" (KTH-researcher). These responsibilities were reinforced further as we approach T_2 where MKG and KTH opted-out as a result of how the work in the reference group unfolded.

Principle	**SKB**	**MKG**	**KTH**
Responsibility	Process owner	Process reviewer	Scientific reviewer and advisor
Integrity of role	Reference group concerning specific topics	The general public concerning all topics	Reference group
Trust	T_1: Moderate for KTH and MKG T_2: Moderate for KTH, low for MKG	T_1: High for KTH, low for SKB T_2: High for KTH, low for SKB	T_1: Moderate for SKB, and MKG T_2: Low for SKB, moderate for MKG
Ethicality	Only publish information that SKB has reviewed	No information may be withheld	No information relevant for scientific review may be withheld
Confidentia-lity	T_1: No project information is held confidential to the reference group T_2: Intermediate results are made confidential	T_1: No information about SKB's research should be confidential to the general public T_2: No information about SKB's research should be confidential to the general public	T_1: No project information should be held confidential to the reference group T_2: No project information should be held confidential to the reference group
Integrity of data	T_1: Integrity of data exists T_2: Integrity of data exists	T_1: Integrity of data exists T_2: Integrity of data does not exists	T_1: Integrity of data exists T_2: Integrity of data does not exists
Availability	T_1: All project information is available to the reference group T_2: Intermediate results are not made available	T_1: All information about SKB's research should be available to the general public T_2: All information about SKB's research should be available to the general public	T_1: All project information should be available to the reference group T_2: All project information should be available to the reference group

Table 1: Overview of analysis

Integrity of role: SKB used the reference group to discuss "corrosion of copper in an oxygen-free environment" (Protocol March 24, 2011). It meant that they did not view the reference group as a legitimate area to discuss all the research that they

conducted. As process owner they felt able to choose projects, project results or parts thereof that were to be discussed in the reference group. In addition, they clearly stated that information to the public should only be provided when information where conclusive. MKG on the other hand demanded that information about all SKB's research activities should be available to the public. Hence, they saw no restriction in whom to include in the dissemination of research results. They based this view on the self-imposed role as process reviewer. KTH saw the members of the reference group as the group that should be trusted with disseminated research results. However, they experienced (T_1-T_2) that SKB viewed them "in the same way as the general public instead of having some kind of exclusive position because we were part of the reference group" (KTH-researcher).

Trust: When the reference group started (T_1) we saw that SKB trusted both KTH and MKG. However, there was a difference in the amount of trust for these organisations. SKB had high confidence in KTH as scientific reviewers in the reference group; at the same time SKB's confidence in MKG was a bit lower, mostly for historical reasons that MKG belongs to the environmental community. MKG on the other hand expressed a low confidence in SKB when they entered the reference group, much for the same reasons. MKG welcomed KTH's presence in the reference group because they would act as scientific reviewers; hence MKG had high confidence in them. Finally, KTH trusted both SKB and MKG when the reference group started.

The actors' trust in each other changed as the work in the reference group proceeded towards T_2. MKG and KTH started to distrust SKB. MKG expressed that "we are not impressed with how they [SKB] handled knowledge within the company" (MKG representative). This was mainly a result of how SKB made information available to the members of the reference group, and how they dealt with integrity of data which is discussed further below. KTH's loss of trust is evident in following statement: "it [transparency] was nice words in the beginning, but as time went by we understood that we did not get the transparency to the experiments. What we saw and commented on was what they [SKB] had decided from the start" (KTH-researcher).

SKB's trust in MKG was at the same time reduced because MKG disseminated information before official versions of the minutes were made available from the reference group. SKB claimed that MKG "was the one that each time after a meeting wrote on MKG's website … we still had agreed that in order to get decent reports all minutes should be public and that all members of the reference group should be given the opportunity to give their opinion on the content before the minutes were made public" (SKB-representative). SKB's confidence in KTH partly remained intact during and after the reference group's lifetime, even though they left the reference group. It is shown by the following statement: "after the opt-out SKB wanted to associate KTH yet again to another group, where [person name] would be included" (KTH-researcher).

Ethicality: The three actors anchored their actions in different ethical principles that aligned with their responsibilities. SKB viewed it as ethical to review all research results before publishing them in order to only publish information that had their

quality approval. MKG argued that "it [information] should be transparent" (MKG-representative) and made available as soon as possible. They meant it is the only way to guarantee well-informed choices with regard to nuclear waste disposal. KTH argued that information should be provided according to well-recognised scientific principles where all raw data from the research is made available to the reference group. Consequently, "to remove [research] results is a serious matter" (KTH-researcher).

Confidentiality: SKB claimed that when the reference group started (T_1) they had an IS policy not to keep any information concerning copper corrosion confidential. The SKB-representative claimed that "every actor in this context [the reference group] would have access to the results as they were produced". As the work proceeded, MKG, as process reviewer, requested that "SKB creates a reference group to follow the entire company's research on the KBS-method's barrier system, not only experiments on cooper corrosion in in deoxygenated water" (Protocol, March 23, 2011), and they requested to see unpublished reports. Consequently, they argued in line with the ethical principle of transparency. SKB "tried to oblige as much as possible. In the end, however, we had only agreed that the experiments in Uppsala were to be dealt with in the reference group" (SKB-representative).

As a consequence, SKB decided to change their IS policy (before T_2). "This reference group had great impact on SKB's policy for reporting" (SKB-representative). They started to divided research material into work-in-progress documents and final reports: "if we have the materials, which of course we have, which is work-in-progress material, it is never classified as a report or finished product. Instead it is a document" (SKB-representative). Work-in-progress documents were treated as confidential information and not released outside SKB. "It [the new policy] included the whole organisation, just not only research" (SKB-representative).

Integrity of data: As process owner SKB argued that they had to guarantee the quality of published research information. In one of the protocols we found: "SKB's policy is to only report data that we understand and trust" (Protocol November 15, 2010). This statement was anchored in SKB's ethical principle. They viewed it as their duty to remove research information that was uncertain, and that action did not affect the data integrity. MKG and KTH were of a different opinion. Both these actors argued that this process meant violating data integrity, that important data from the research projects were not included in the published information. For example, one disagreement concerned one of the reports. KTH described how "they [SKB] told us at a reference group meeting that all of the results were inaccurate because deficiencies in [test] equipment. Though they did not tell it in that report, where attempts were made to adapt the results to their own reality" (KTH-researcher). This view was also provided by MKG: "I think this is remarkable, scientifically, that these SKB-reports do not completely address the deficiency analysis of what is reported" (MKG representative).

Availability: As a consequence of not keeping any information concerning copper corrosion confidential to the reference group, SKB argued that they initially made all such information available (T_1). Information about some of the related projects were also made available on MKG's requests. However, MKG still argued that "the actual problem is that the transparency is not good enough" (MKG representative). Later on SKB changed their policy and work-in-progress documents were no longer available to MKG and KTH (before T_2). Both MKG and KTH argued that this made it impossible for them to fulfil their responsibilities as process reviewers and as scientific reviewers and advisors.

5. Discussion

Several principles exist for managing IS, such as CIA (ISO, 2013) and RITE (Dhillon and Backhouse, 2000). However, research on IS management has mainly had an intra-organisational focus (McLaughlin and Gogan, 2014), while inter-organisational collaboration is common today. Therefore, we have analysed the relation between the CIA and RITE principles in an inter-organisational collaboration.

Our findings show that differences in responsibility and integrity of role affected the collaborating actors' views on the implementation of confidentiality and availability. SKB, as process owner, shared information on specific topics with the reference group. Hence, they kept more information confidential than MKG and KTH expected from the start. In addition, in this case we also found a difference in the ethical principle; a difference related to the differences in responsibility and integrity of role. SKB saw it as their responsibility to only publish information that had passed their review process. This view differed from the views of their collaborating actors; they expressed a more liberate view on transparency of information and the process on how this information had been brought about. In the end this made the three actors disagree on the integrity of data that was made available to the reference group. The actors' different views on how the CIA-principles were implemented changed their trust in each other over time. In this specific case, MKG and KTH lost trust in SKB, mainly because they did not perceive that integrity of data was kept in SKB's reports to the reference group.

Hence, we have been able to show that the RITE and CIA principles are important to consider in inter-organisational collaboration. From a practitioner's point of view, it is important that collaborating actors are aware of their responsibilities and expectations, and that these are made explicit from the start. Furthermore, it is equally important that they have a shared view of the integrity of roles and ethicality because these views affect how they perceive the implementation of the CIA-principles. In the end it seems like the perceived implementation of the CIA-principles is crucial for building trust in inter-organisational collaboration. From a research point of view we contribute by showing the relation between these two sets of principles and how they affect each other over time in an inter-organisational setting. Moreover, earlier research on RITE principles (e.g. Dhillon and Backhouse, 2000) has focused on employees within organisations, i.e. on individuals in relation

to an organisation. We have shown that it is fruitful to analyse IS management on an organisational level using these principles, i.e. an organisation in relation to one or more organisations.

6. Conclusion

Inter-organisational collaboration is important in today's society, but the knowledge on how to manage information security (IS) in such settings is limited. Against this backdrop the aim of this paper was to investigate the relation between the CIA (Confidentiality, Integrity of data, Availability) and RITE (Responsibility, Integrity of role, Trust, Ethicality) principles in the context of an inter-organisational collaboration. We conclude that there is a dynamic relation between these principles, which is important for organisations to be aware of when entering collaborations. Based on our investigated case we found that responsibility, integrity of role, and ethicality affected the perceived implementation of CIA. Differences in responsibility, integrity of role, and ethicality that the organisations are unaware of can create false expectations that can undermine collaboration, because the perceived implementation of CIA affects how (dis)trust is developed between the collaborating organisations over time.

Our findings are based on one single study of inter-organisational collaboration. Consequently, it is an obvious limitation of this study. However, our findings have shown an interesting opportunity for future research; more research is needed on IS principles in inter-organisational settings.

7. References

Andersson, K. 2014. Copper Corrosion in Nuclear Waste Disposal: A Swedish Case Study on Stakeholder Insight. *Bulletin of Science, Technology & Society,* 33**,** pp. 85-95.

Bahl, S., Wali, O. P. and Kumaraguru, P. Information Security Practices Followed in the Indian Software Services Industry: An Exploratory Study. *Second Worldwide Cybersecurity Summit (WCS 2011)* 2011 London, UK. IEEE, 1-2 June, 2011.

Berghmans, P. and Van Roy, K. 2011. Information Security Risks in Enabling e-Government: The Impact of IT Vendors. *Information Systems Management,* 28**,** pp. 284-293.

Chen, T.-Y., Chen, Y.-M., Wang, C.-B., Chu, H.-C. and Yang, H. 2007. Secure resource sharing on cross-organization collaboration using a novel trust method. *Robotics and Computer-Integrated Manufacturing,* 23**,** pp. 421-435.

Dhillon, G. 2007. *Principles of information systems security: text and cases,* Hoboken, NJ, Wiley Inc.

Dhillon, G. and Backhouse, J. 2000. Information security management in the new millenium. *Communication of the ACM,* 43**,** pp.

Dhillon, G., Chowdhuri, R. and Pedron, C. 2014. Organizational Transformation and Information Security Culture: A Telecom Case Study. *In:* Cuppens-Boulahia, N., Cuppens, F., Jajodia, S., Abou El Kalam, A. and Sans, T. (eds.) *ICT Systems Security and Privacy Protection - Proceedings 29th IFIP TC 11 International Conference, SEC 2014, Marrakech, Morocco, June 2-4, 2014.* Berlin: Springer

Djordjevic, I., Dimitrakos, T., Romano, N., Mac Randal, D. and Ritrovato, P. 2007. Dynamic security perimeters for inter-enterprise service integration. *Future Generation Computer Systems,* 23**,** pp. 633-657.

Dommun, M. R. 2008. Multi-level information system security in outsourcing domain. *Business Process Management Journal,* 14**,** pp. 849-857.

Iso 2005. ISO/IEC 27001:2005, Information Technology - Security Techniques - Information Security Management Systems - Requirements. International Organization for Standardization (ISO).

Iso 2013. ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls. International Organization for Standardization (ISO).

Kayem, A. V. D. M., Martin, P. and Akl, S. G. Efficient Enforcement of Dynamic Cryptographic Access Control Policies for Outsourced Data. *Information Security South Africa (ISSA), 2011*, 15-17 August, 2011 2011 Johannesburg, South Africa. IEEE Xplore, 1-8.

Mao, T., Williams, J. and Sanchez, A. Interoperable Internet Scale Security Framework for RFID Networks. *24th International Conference on Conference: Data Engineering Workshop*, 2008. IEEE Xplore, 94-99.

Mclaughlin, M.-D. and Gogan, J. INFOSEC in a Basket, 2004-2013. *The 20th Americas Conference on Information Systems (AMCIS 2014)*, 2014 Savannah, Georgia, USA. AIS Electronic Library (AISeL), ISSecutity paper 6.

Oscarson, P. 2007. *Actual and perceived information systems security.* Linköping University.

Pemble, M. 2004. Transferring business and support functions: the information security risks of outsourcing and off-shoring. *Computer Fraud & Security,* 2004**,** pp. 5-9.

Polkinghorne, D. E. 2005. Language and Meaning: Data Collection in Qualitative Research. *Journal of Counseling Psychology,* 52**,** pp. 137-145.

Robertson, C. J., Lamin, A. and Livanis, G. 2010. Stakeholder Perceptions of Offshoring and Outsourcing: The Role of Embedded Issues. *Journal of Business Ethics,* 95**,** pp. 167-189.

Tsohou, A., Theoharidou, M., Kokolakis, S. and Gritzalis, D. 2007. Addressing Cultural Dissimilarity in the Information Security Management Outsourcing Relationship. *In:* Lambrinoudakis, C., Pernul, G. and Tjoa, A. M. (eds.) *Trust, Privacy and Security in Digital Business.* Springer.

Yuan, H., Chen, G., Wu, J. and Xiong, H. 2009. Towards controlling virus propagation in information systems with point-to-group information sharing. *Decision Support Systems,* 48**,** pp. 57-68.