Genre-Based Assessment of Information and Knowledge Security Risks

Ali Mohammad Padyab
Luleå University of Technology
ali.mohammad.padyab@ltu.se

Tero Päivärinta
Luleå University of Technology
tero.paivarinta@ltu.se

Dan Harnesk
Luleå University of Technology
dan.harnesk@ltu.se

Abstract

Contemporary methods for assessing information security risks have adopted mainly technical views on the information and technology assets. Organizational dynamics of information management and knowledge sharing have gained less attention. This article outlines how an information security risk assessment method can be elaborated using knowledge-centric analysis of information assets. For this purpose, we suggest the use of a genre-based analysis method for identifying organizational communication patterns, through which organizational knowledge is shared. Initial experiences of the method try-outs by three experienced information security professionals are discussed. The article concludes with a look at the implications of a genre-based analysis of knowledge assets for future research and practice.

1. Introduction

More than a decade ago, Dhillon and Backhouse [1] highlighted the importance of understanding and protecting information assets instead of having a plain focus on physical and technical assets in the field of information security. Indeed, many if not most of the current risk assessment methods base their analysis upon the concept of "information assets" [2]. However, a few researchers have criticized current risk assessment methods by illustrating some deficiencies in identifying information assets. The methods may define what an information asset is but they seem to assume that the risk analyst will then simply know the organization's information assets without further facilitation of their identification [3]. Moreover, most risk analysis methods are regarded as providing a plain technical view on information (data) and technological assets, ignoring the dynamic environment of knowledge work and people as knowledgeable entities of the organization [4, 5]. For example a recent case study [6] suggests that a relatively well-known risk analysis methodology (OCTAVE-S) fails to address knowledge security issues related to informal and non-technical organizational processes.

We started to address this knowledge gap with the assumption that knowledge security may be at risk in situations where knowledge is **shared** between people and organizations. Knowledge sharing may concern both tacit and explicit knowledge and it involves the knowledge creation modes of externalization, socialization, combination and internalization [7]. Anyhow, all of these modes of knowledge creation and sharing require **communication** between people, either directly in human-to-human knowledge networks or through externalized information repositories [7, 8].

Hence, we looked at theories and concepts which would help us to conceptualize organizational communication patterns as a basis for mapping knowledge security risks. Among such theories, the genre theory of organizational communication [9] provided us with a well-established conceptual basis as well as established analytical means, both with regard to human-to-human communication, such as meetings [10, 11] and documented information [12]. Hence, we employed an already established Genre Based Method (GBM) [13] to identify and analyze knowledge assets. We then combined GBM with a lightweight risk assessment method, OCTAVE Allegro (OA) [14], to relate risk assessment to the genre-based model of organizational knowledge. With the objective of evaluating the resulting hybrid method (GBM-OA), we then introduced it as part of an online Master's course on knowledge security. Three experienced information security professionals, who were asked to try out the method and make a security risk analysis in their own organizations, attended the course. Their feedback on the method use provided us with insight and ideas for improvement. In this paper, we report on the hybrid method of GBM-OA and its initial evaluation in the aforementioned setting.

The remainder of this paper is organized as follows. We present the theoretical background in section 2. Section 3 introduces the GBM-OA method. The method and the reflections of three professionals who have tested it are presented in section 4. Section

978-1-4799-2504-9/14 $31.00 © 2014 IEEE
DOI 10.1109/HICSS.2014.428

5 discusses our findings. We conclude by indicating limitations and ideas for further research in section 6.

2. Background

2.1. Security Risk Assessment

Risk Assessment is defined as to "identify, measure, quantify and evaluate risks and their consequences and impacts" [15, p. 22]. The output from risk assessment will help the organization to conduct a cost-benefit analysis based on current controls and countermeasures to whether mitigate, transfer, avoid or accept the risks [16-18]. Today there are more than 200 practitioner-oriented risk assessment methods and other academic security models available [19]. Even though they employ different approaches to measure risks, the objective is to identify and value assets, identify vulnerabilities to those assets, assess risk and create mitigation strategies [20-22].

Assets are defined as anything that has value to the organization [23, 24] in terms of both tangible (computer systems, people) and intangible assets (company reputation etc.) [25]. Asset identification plays a critical role in any risk assessment method because without assets there would be nothing to protect [26]. Information as a key asset in organizations has been given especial attention in the literature. Dhillon and Backhouse [1] distinguish the information assets from the physical, tangible assets, which have traditionally been the focus of security risk analyses. Some information assets form the core of any information systems and warrant careful analysis as they play a vital role in the business [27]. This has led the risk assessment methods to consider information assets as a core object of analysis [2]. Grimaila and Fortson [28] argue, "The lack of information asset based risk management process results in significant uncertainty and delay when assessing the impact of an information incident." (p. 266).

Shedden et al. [4] studied how to enhance existing risk assessment methods in favour of a better information asset identification approach. Their proposals are based on the argument that information and knowledge assets are at risk from people inside the organization and through channels of informal communication. So, it is important to include these knowledge assets in the risk analysis methods. The following issues are important to be included in risk analysis: 1. Identification of knowledge asset leakage 2. Identification of critical knowledge 3. Deeper level of information asset identification. Organizations using current risk assessment methods tend to identify assets at an overly general level due to "ease of use" [29] or more tangible assets like technological resources [28]. However, Shedden et al. [4] have not yet proposed any method or tool to fulfill their propositions. Our search of the literature did not find good candidates, either.

Sandia National Laboratories published a classification scheme for risk assessment methods in 2004 [3]. The report found that "… none of the methods we have seen fully describe how to identify an asset or a vulnerability or a threat or a risk or a control, nor do we expect ever to see one that does. Many of the methods give definitions and provide examples but they presume you will know an asset, say, when you see one." (ibid) (p. 11). This calls for improved approaches in asset identification as the initial step within every risk assessment method. More recently, risk analysis methods have been criticized for being slow, unstructured, inflexible, involving ad hoc diagrams and analyses and providing incomplete documentation [19, 30].

Hence, we started with an observation that there is a gap in the risk analysis literature and methods with regard to the approaches for mapping organizational information and knowledge. On the other hand, employees preserve and reflect the core intellectual assets of any organization. They can cause leakage of knowledge through channels of organizational communication [31]. The current focus in risk assessment methods is largely targeted at information assets instead of the actual channels of communication and knowledge sharing. Work environment and business processes are a considerable source of asset leakage [32] and traditional information security risk assessment approaches are incomplete [4, 5]. These observations guided us to look at concepts, theories and methods for modeling organizational communication as a basis for identifying knowledge sharing situations (cf. [7]). We chose to have a closer look at the theory of genres of organizational communication [9] as the basis of an enhanced approach, as it has been already used with some success in several areas of communication analysis and systems development in organizational contexts [10, 12, 33, 34, 35].

2.2. Genre Based Method

The Merriam-Webster dictionary describes the concept of genre with the words "type", "sort", "category" and "kind". The concept of genre has also been defined numerous times in the literature (e.g. [36-38]). This research follows the definition of genres of organizational communication by Yates &

Orlikowski [9]: "A genre of organizational communication (e.g. a recommendation letter or a proposal) is a typified communicative action invoked in response to a recurrent situation." (p. 301). The genre lens has been regarded as an effective means for analyzing organizational communicative practices and information systems; involving human-to-human communication, meetings [10, 11] and documented information [12].

Päivärinta et al. [13] introduced a genre-based method for information systems planning, starting with identifying stakeholders who are involved in the planning process. The method describes how to use the concept of PUI (Producer/User of Information) entities to capture a variety of critical organizational information. The process continues to identify genres with the help of PUI representatives in a collaborative environment and supporting tools like the "diagonal matrix" (first developed by Saaren-Seppälä [39], it is used in GBM as a collaboration technique to identify genres). The genres are entered in a spreadsheet with columns of the sheet as properties of genres. The properties of this genre list are defined by the stakeholders and can vary depending on the context (Appendix).

In the current literature, we could not find traces of organizational genres utilized in any information security area. Hence, we chose a commercial, light-weight method, OA, to try out to which extent the information security risk analysis could fit into the genre based model of knowledge resources.

2.3. OCTAVE Allegro

The OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) method was created by Software Engineering Institute at Carnegie Mellon University in 1999 [40]. The method aims at facilitating the information security risk assessment in relation to the organizational mission and objectives. The OCTAVE method provides guidelines for developing qualitative risk evaluation, identifying assets critical to the livelihood of the organization, recognizing vulnerability associated with those assets and evaluating the impact of those risks if launched successfully [14]. There are three versions of OCTAVE methodology, of which we used OA for this paper. OA provides steps for identifying and assessing risk in an organization specifically targeted at information assets. It is considered as a light version of former methods to be used in small organizations without considerable organizational commitment, expertise or input. The guidelines for identifying associated information security risks consist of four general baselines and eight steps overall. OA has 10 premade worksheets but, due to page limitations, we can't explain them here. We would therefore like to urge the audience to read more about them in the OA handbook [14].

We choose OA mainly because it bases its analysis on information assets. We could rather easily replace OA's ambiguous concept of information asset with the genre-based approach provided by GBM. Another reason for selecting the OA method was based on its ease of use for students who had no experience of risk assessment methods before. We regarded it as a pedagogically good method due to its relative simplicity and easily available and well-documented guidelines. Whilst most of the students can't easily access medium to larger based organizations (especially for one single course), it is more suitable to trialling in a company which students can access for a short time (2 months) of their course.

3. Hybrid GBM-OA Method

According to OA, "[a]n information asset can be described as information or data that is of value to the organization, including such information as patient records, intellectual property, or customer information" [42, p. 34]. OA also suggests brainstorming with four simple questions to identify information assets. Apart from the definition and four questions, OA does not give us a clear definition on what might constitute an information asset. For example, according to OA, customer data and patient records are both information assets but customer data is a more general information asset in some cases; therefore it might lead to repetition of the same information asset during risk analysis. We would criticize OA in the sense that it poorly recognizes the granularity and categorization of the information assets. On the other hand, OA does not facilitate grounds for user participation. This lack of focus may ignore users as the knowledgeable entities and result in a lower chance of detecting some areas of concern. Although, according to OA, people can be containers of information, the emphasis is on information assets that some people may hold in physical and electronic format. The way OA emphasizes people essentially is to define information assets and then find people who hold those assets in their mind. Therefore OA depicts people not as producers of information/knowledge, but only as transporters of information assets.

These deficiencies strengthened our motivation to employ GBM within OA. Through GBM, we can conceptualize information/knowledge assets and use those genres as the information asset fields in OA. GBM gives us a clear definition of communication

channels (mediums) and exchanged substances that exist both physically and electronically (information assets) or within people's minds (knowledge assets). User participation is at the heart of GBM, thus the targeted organization can benefit from better understanding of the areas that might need immediate attention. Moreover genres can, to some extent, capture informal business practices that are not documented and exist within people's minds. These motivations guided us to interlock GBM within OA. The resulting method steps are (see Figure 1):

GBM 1 Define stakeholders of security risk analysis: The method starts with the first phase of GBM by defining who should participate in the analysis. A representative from management or CISO is an ideal choice for a leader. (S)He will identify basic group of stakeholders who are perceived to be important according to the organizational strategic goals and objectives. The list of participants can be expanded accordingly.

OA 1 Define risk measurement criteria: The method continues with the first phase of OA by defining "Risk measurement Criteria". The participants identified in the previous step will define risk scopes and prioritize risk areas that are connected to strategic areas. The output, "Prioritized risk areas and scopes", is used in the last step to analyze risk and mitigation strategies.

GBM 2 PUI entities: This step identifies internal and external PUI entities that can vary from people, processes, units, objects and etc. A list of PUI entities can lead identification of more stakeholders; therefore it is important to update the list as the process proceeds.

GBM 3 Identify genres of communication: Representatives from PUI entities "transfer knowledge" in collaborative sessions to identify genres. We can facilitate this collaboration with the help of diagonal matrix technique [39]. The idea is to list PUI entities so that participants can identify genres (see figure 3). The risk analyst collects the genres in different sessions for later analysis. At this stage, there is a high probability of identifying unrevealed areas of concern that might be connected to the organizational information security strategy. Therefore we might reshape security stakeholders, PUI entities or risk measurement criteria.

OA 2 (GBM 4-5): Develop an information asset profile with genre properties: Here we aim to gather metadata for the genres. Properties are defined by the leader and risk analyst who has knowledge about security risks. Defined properties form an excel datasheet. We have tailored an excel spreadsheet according to the requirements of OA (see appendix figure 4) which is ready to use. Further properties can be added based on the context. Once properties have been defined, it is of paramount importance for the representatives of the PUI entities to participate. As producer/user of the information, they are the best option for filling out some of the properties (i.e. the owner of genre). Once the genre list has been completed, the risk analyst will have two options. 1. To use the genre list itself as the asset profile or 2. To transfer the genres identified to the OA worksheet (information asset profile). The choice is up to the analyst but we recommend the first option as the number of worksheets is greatly decreased and the genre list will give an overview of the overall assets.

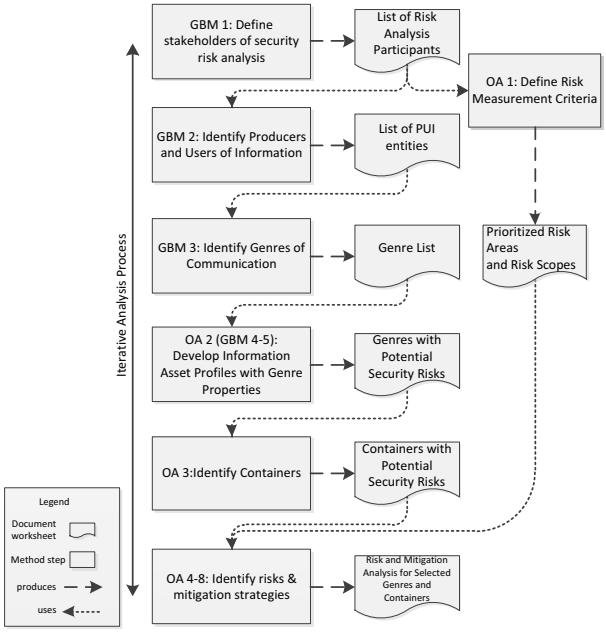

Figure 1 GBM-OA Steps and Resulting Documents

OA 3 Identify containers: This step aims to identify containers where information assets exist. From a genre point of view, this is where (what medium) the genre takes place (see example in appendix figure 5). This step can also emerge in the genre list but it might cause repetition of the same container across a number of genres, therefore the choice of integration can depend on the number of genres identified.

OA 4-8 Identify risks & mitigation strategies: This step involves OA steps 4 to 8 without a change in the original OA method. Now that we have prepared the information assets (genres), it's time to analyze the risks according to "prioritized risk areas and risk scopes" produced in the second step. The greatest advantage of having GBM on side is the possibility of collecting more threat scenarios from

informal networks of people. Representatives of PUI entities can participate in this stage to reflect their past experiences from past threats and to give ideas regarding future mitigation strategies (figure 6 in appendix). The whole process is iterative, meaning that the analysts can go back to the previous steps and make adjustments to the outputs in each phase and continue downwards.

Overall, we can perceive that we have replaced information assets with genres and ambiguous OA information asset mapping with a structured stepwise method (GBM).

4. Initial experiences from method use

The choice of methodology in this research was dependent on the type of data available for the analysis. In this research, we used a set of reflections and risk analysis reports from three IT and security professionals taking part in a Master's course. They have tried out the proposed method in real settings and documented their experiments. The preliminary data was gathered by the abovementioned course instructor which formed the basis for analysis.

4.1. Data collection and analysis

Preliminary data gathering for our initial evaluation of the suggested method was performed through course assignments. The course was part of a Master's program in Information Security. The students were asked to reflect upon the proposed method (GBM-OA) after each session of the class, while the instructor gradually nurtured the different components of the genre-based method in conjunction with OA. Three participants on the course had a strong professional background and experience in the field of information security management and our preliminary evaluation is based on their work using the suggested method in the companies they are affiliated with and the in-depth reflections they produced from their experiment. Two of them were Chief Information Security Officers (CISO) and one was an IT professional. The first participant was a CISO (hereafter CISO1) in a company located in Sweden with 10 years of Information Security experience. The second CISO (hereafter CISO2) worked in financial intermediary for quote services in the UK. He had more than 10 years of IT security experience. The third participant was an IT professional (hereafter ITPRO) in a private equity firm in USA with more than 20 years of experience. Further interviews with these three managers were conducted afterwards to capture their ideas with respect to the practical issues of the hybrid method in the hands-on project.

Diaries have been collected as part of a closed group wiki page with each student having a dedicated reflection page. The usefulness of this type of communication is that students can read other students' thoughts and comment and discuss about the issues in an interactive manner. The students were granted flexibility to use the method and document their assumptions and reasoning with logical justification. A total of 179 pages of risk assessment documents, 37 pages of reflection diaries in addition to 3 pages of follow up interviews were analyzed in this paper. The first round of data including reflection diaries and risk assessment reports was collected during November 2011 to January 2012 and follow-up interviews carried out in August 2012. This was led by Charmaz [41] to ensure that reflections were coded correctly.

Goulding [42] argues that researchers choose Grounded Theory when there is no reference in the literature on the topic of interest or it has been mentioned superficially, so they will decide to build their theory on the data. Grounded Theory is widely accepted as an effective tool for building the practice within the evaluation and education discipline in particular [43-45]. The theory was further developed by Strauss and Corbin [46] with the introduction of multiple coding procedures such as open, axial and selective coding.

4.2. Experiences

The result emerged from the reflections of three professionals who were able to try out the method in reality, along with their risk assessment reports. The results have been extracted based on the usability of GBM within the context of the risk assessment and interaction of GBM and OA when it comes to the integration of the two.

Line by line coding resulted in the development of concepts as a textual representation of the reflecting idea. The concepts with related meanings are then grouped together to form a category. The categories were then compared to each other during axial coding to find the connection between the categories that helped to reorganize the categories and find the final core categories (selective coding). The results from our coding revealed three stories based around the core categories (illustrated in different colors within figure 2).

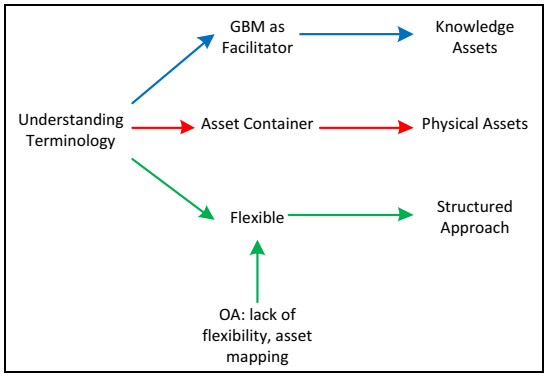

Figure 2 Result

4.2.1 Knowledge assets. The participants reported that they were able to map knowledge assets that exist in their work rather easily by using GBM. For instance, one participant was able to identify that IT operations have some sort of reoccurring face-to-face meetings in which some important information about "authentication credentials" is discussed in a special location. Those communication situations can then be exposed to variety of threats:

"I find that the process of documenting the key KM genres for a company helps one to identify those key business processes which are most essential for commercial success … in my organization most of the really critical KM genres are on individuals' own laptops and in email and excel sheets - there clearly needs to be a wider dialogue in the organization on how to handle high-value information and knowledge."(ITPRO)

GBM's collaborative environment and involvement of employees during genre gathering helped participants to map knowledge assets:

"The classification (with some explanation) is really easy to understand, since everyone is "kind of using the method already". What I mean is that people know why they create a document, know when they need to release it and who the intended audience is."(CISO1)

One of our findings showed that the more the participants stick to the method's core concepts, the more they would be able to extract knowledge assets. For example, one professional decided to gain assistance from a Data Flow Diagram to gather genres due to time constraints, therefore he kept the employee participation at a lower level:

"Like any concept they [GBM] require some thoughts on how they can be implemented in the context of an individual risk management framework, but once they have been used a couple of times the concept becomes clearer. In some businesses the term "data flows" might cover a similar process, however that is very data-centric whereas genres are very producer/user-centric."(CISO2)

Consequently, in his genre list, we were able to observe that most of the genres evolve around data assets rather than knowledge assets compared to the other two participants who tried to keep themselves closer to the core GBM concepts. We found it necessary to ensure that the users of the hybrid method understood the concepts correctly and perception of genres was not confused by other methods of information system tools used for data/process mapping, such as DFD and ERD:

"I found the TERMINOLOGY [GBM] confusing, however once it seemed genres were similar to business processes/flows then it was easier to comprehend."(ITPRO)

4.2.2 Physical assets. At some point in time, students argued that physical assets are not the main focus in GBM. This doubt has been reinforced by the learning process stage through the real setting experience. One CISO commented on GBM in the learning diary that:

"I need to get clear in my head the difference (or similarity) between an Information Asset and a Communications Genre. Information Assets are typically physical or electronic (that's how I group them). You cannot completely dismiss something like a physical information asset mapping in favor of a genre-based approach as how would you identify something like 100 HP G7 Servers? Yes, genre-based approaches might be a useful complementary tool to reveal hidden communications, but I am not sure it completely replaces traditional approaches." (CISO2)

For this reason, we closely analyzed the results from the genre list and risk assessment document to evaluate the hybrid method for this matter. We came to the conclusion that those assets having physical forms are mapped as containers (either combined in the genre list or as a separate worksheet). This proved our reasoning for keeping OA step 3 (Identifying Containers) as a separate step in the hybrid method to map physical assets in addition to GBM's ability to identify knowledge and information assets. Our practitioners' technological mindsets have their roots in traditional risk assessment methods that mostly focus on technical rather than information/knowledge assets. This reflects our initial goal to shift from a very technical risk assessment approach towards a more business practice perspective that requires a balance between physical and information/knowledge assets. However from the pilot experiment, we have learned that we need to make a clearer distinction between GBM and its relationship to the

identification of containers. Our participants' perception was that with GBM, it is possible to map all of the containers, which was not our initial purpose. It should be understood that GBM gives deeper insight into identifying and securing information/knowledge assets and related containers but it does not necessarily facilitate identification of all containers within the organization.

"Although the Genre-based approach helps identify containers where the asset is stored, transported or processed, it does not identify every container that the information asset might reside in or travel through."(CISO2)

4.2.3 Structured Approach. All three participants argued that GBM provides useful procedures to facilitate information asset identification within an organization. Despite of the initial challenges related to the genre concept, the method was regarded as relatively easy and quick to adopt and supportive for the analysis work.

GBM also provides the means to identify information and knowledge assets beyond the plain technological issues related to the media-based analysis of containers. For example, in one company the genre-based analysis was quickly able to reveal the risks related to particular core document types including in particular sensitive business information (e.g. investment analyses and bids) if shared through e-mail, while e-mail as a medium was not otherwise regarded as especially risky. All three professionals came to this conclusion while comparing OA's plain container-based approach to information asset identification versus the GBM method. This positive viewpoint on GBM sometimes referred to the systematic approach to defining stakeholders, PUIs and genres with the help of a pre-made Excel spreadsheet which helps to gather the required information:

"The Excel file provided by [the instructor] is a huge life saver for everyone whose organization does not already have an asset inventory. It is much easier to identify the assets by asking the questions (who owns it, why do we have it, etc.) than to try to brainstorm without having a starting point." (CISO1)

Although the method proved to be straightforward with step by step guidelines, it was confirmed by the professionals to be flexible as well. Flexibility in this context is defined as having the ability to make changes to the method procedures without losing critical information. The genre list worksheet provided by the course instructor led to innovative attempts by the groups. They, to some extent, decided to go beyond the list and make changes which they felt were necessary to the list. This resulted in the elimination of some elements (in some cases the whole worksheet) from OA and the inclusion of those properties in the genre list.

"Extending the original Genre worksheet to include additional columns that match fields in various OCTAVE Allegro worksheets does reduce the volume of paperwork (or electronic worksheets) that need completing … OCTAVE Allegro worksheets can easily be embedded (or deconstructed and fields embedded) into a genre worksheet"(CISO2)

These changes were based on the GBM's terminology and structured guidelines by focusing on gathering the information that is required for the risk analysis. This freedom prevented the professionals from using the method slavishly and they were able to adjust the properties in such a way as to reduce the time and effort of filling out the OA worksheets (OA worksheets were acknowledged as being too rigid by our practitioners).

5. Discussion

This paper has suggested a novel approach to information and knowledge asset mapping for security risk assessment. To this end, we have analyzed whether a genre-based method (GBM) combined with the Octave Allegro (OA) have resulted in better understanding of information asset identification. The study began with a basic premise that the current risk assessment methods are mainly based upon a technical view of organizational assets and thus ignore dynamic work environments and people as knowledgeable entities of the organization [4, 5, 47].

Our study shows that, with the use of GBM–OA, information mapping of security risk assessment is no longer a mere technical activity. Together these two methods illustrate emerging properties within the mapping context. This perspective differs from mainstream research, which primarily views risk assessment as an instrumental approach largely depending on traditional top-down perspectives (e.g., [20-22]).

First, the GBM extension to OA results in making organizational communication genres visible to the relevant stakeholders who can then continue to identify related risks and suggest strategies for mitigation. This approach essentially involves those who are actually experiencing the issues of organizational communication, work patterns and structures [34] in their work environment. In the case of information mapping of security risk assessment, this means that by identifying genres of communication through user participation, risk assessment is improved because it provides

knowledge at deeper levels of granularity if compared to the generic concept of (often mainly technical) assets that are often identified top-down.

Second, identification of knowledge assets beyond plain technical assets were apparent in the genre lists mainly because GBM starts with identifying stakeholders to participate in finding PUI entities. The PUI entities can take different forms such as processes, departments, managers, external PUI entities, etc. People are crucial elements in these processes, so what it means for information mapping is that with GBM, the risk assessment no longer adheres to prescriptive and normative modes of risk assumptions [48].

Finally, GBM as an add-on to OA increases the capability of uncovering what is perceived in the organization against what practices are employed in reality [13]. As Karjalainen et al. [12] argue, "Knowledge from the employees producing or using information in their work" and the output would be a "list of genres including their producers and users". It is those who can contribute to identification of knowledge assets prone to exploitation who define new risk assessment capabilities.

Altogether, GBM-OA changes the foundations upon which risks assessment are based. For example, the business practice perspective that Shedden et al. [4] propose to overcome the deficiencies in current risk assessment methods seems to be alleviated by GBM. The use of GBM changes the perspective of risk assessment from an instrumental mechanism [48] towards a link between vulnerability analysis and impact evaluation of potentially successful risk breaches [14]. Current research raises the issue of how information and knowledge assets are put at risk by people inside the organization and through channels of informal communication (e.g. [4, 48]). Our analysis illustrates a richer picture: Through GBM, we can conceptualize information/knowledge assets into genres and analyze them as information assets in OA. GBM gives us a sound definition of communication channels and exchanged knowledge that exist physically and electronically or within people's minds. As this paper indicates, organizations can benefit from better understanding of those areas that might need immediate attention.

6. Conclusion and further research

Our research outlined how information security risk assessment can be elaborated towards more organization- and knowledge-centric analysis of information assets. For this purpose, we suggested use of the genre-based approach for analyzing organizational information and knowledge risks. The risk analysis approach was instantiated by means of integrating a genre-based information systems planning method, GBM, with a light-weight risk assessment method, OA. The hybrid method (GBM-OA) was tried out in three different companies by three information security and technology professionals, who gave us initial and encouraging feedback about the potential utility of the suggested approach together with ideas for its further development. Our further efforts aim at gathering more empirical experience from using the genre-based approach and elaborating the GBM-OA method and related analysis tools further.

7. References

[1] Dhillon, G., & Backhouse, J. (2000). Technical opinion: Information system security management in the new millennium. Communications of the ACM, 43(7), 125-128.

[2] Jones, A., & Ashenden, D. (2005). Risk management for computer security: Protecting your network & information assets. Butterworth-Heinemann.

[3] Campbell, P. L., & Stamp, J. E. (2004). A classification scheme for risk assessment methods. United States. Department of Energy.

[4] Shedden, P., Smith, W., & Ahmad, A. (2010). Information Security Risk Assessment: Towards a Business Practice Perspective. In 8th Australian Information Security Management Conference, 119-130.

[5] Spears, J. (2006). A Holistic Risk Analysis Method for Identifying Information Security Risks. Security Management, Integrity, and Internal Control in Information Systems. Boston, Springer Boston. 193/2006: 185-202.

[6] Shedden, P., Scheepers, R., Smith, W., & Ahmad, A. (2011). Incorporating a knowledge perspective into security risk assessments. VINE, 41(2), 152-166.

[7] Nonaka, I. (1994). A Dynamic Theory of Organizational Knowledge Creation. Organization Science, 5(1), 14-37.

[8] Alavi, M., & Leidner, D.E. (2001). Review: Knowledge Management and Knowledge Management Systems: Conceptual Foundations and Research Issues. MIS Quarterly, 25(1), 107-136.

[9] Yates, J., & Orlikowski, W. J. (1992). Genres of organizational communication: A structurational approach to studying communication and media. Academy of management review, 299-326.

[10] Antunes, P., & Costa, C. J. (2003, November). From genre analysis to the design of meetingware. In Proceedings of the 2003 international ACM SIGGROUP conference on Supporting group work (pp. 302-310). ACM.

[11] Orlikowski, W., & Yates, J. (1994). Genre Repertoire: The Structuring of Communicative Practices in Organizations. Administrative Science Quarterly, 39(4), 541-574.

[12] Karjalainen, A., Paivarinta, T., Tyrvainen, P., & Rajala, J. (2000, January). Genre-based metadata for enterprise document management. In System Sciences,

2000. Proceedings of the 33rd Annual Hawaii International Conference on System Sciences (pp. 10-pp). IEEE.
[13] Päivärinta, T., Halttunen, V., Tyrväinen, P., (2001), A genre-based method for information systems planning, In Rossi, M., Siau, K., (Eds.), Information Modeling in the New Millennium, (pp. 70-93), Idea Group Inc (IGI)
[14] Caralli, R. A., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007). Introducing octave allegro: Improving the information security risk assessment process (No. CMU/SEI-2007-TR-012). Software Engineering Institute, Carnegie Mellon University.
[15] Haimes, Y. Y. (2004). Risk modeling, assessment, and management (Vol. 30). Wiley-Interscience.
[16] Baskerville, R. (1993). Information systems security design methods: implications for information systems development. ACM Computing Surveys (CSUR), 25(4), 375-414.
[17] Haimes, Y. Y. (2001). Risk analysis, systems analysis, and Covey's seven habits. Risk Analysis, 21(2), 217-224.
[18] Peltier, T. R. (2005). Information security risk analysis. Auerbach Publications.
[19] Dubois, É., Heymans, P., Mayer, N., & Matulevičius, R. (2010). A systematic approach to define the domain of information system security risk management. In Intentional Perspectives on Information Systems Engineering (pp. 289-306). Springer Berlin Heidelberg.
[20] Halliday, S., Badenhorst, K. & von Solms, R. (1996). A business approach to effective information technology risk analysis and management. Information Management & Computer Security (4:1), pp. 19-31.
[21] Visintine, V. (2003). An Introduction to Information Risk Assessment, SANS Institute.
[22] Lichtenstein, S. (1996). Factors in the selection of a risk assessment method. Information Management & Computer Security, 4(4), 20-25.
[23] ISO, B. IEC 27005: 2008. Information Technology–Security Techniques–Information Security Risk Management.
[24] Alberts, C., Dorofee, A., Stevens, J., & Woody, C. (2003). Introduction to the OCTAVE Approach. Pittsburgh, PA, Carnegie Mellon University.
[25] Nosworthy, J. D. (2000). A practical risk analysis approach: managing BCM risk. Computers & security, 19(7), 596-614.
[26] Houmb, S. H., Den Braber, F., Lund, M. S., & Stølen, K. (2002). Towards a UML profile for model-based risk assessment. In Critical systems development with UML-Proceedings of the UML'02 workshop (pp. 79-91).
[27] Masera, M., & Fovino, I. N. (2006). Modelling information assets for security risk assessment in industrial settings. In 15th EICAR Annual Conference
[28] Grimaila, M. R., & Fortson, L. W. (2007, April). Towards an Information Asset-Based Defensive Cyber Damage Assessment Process. In Computational Intelligence in Security and Defense Applications, 2007. CISDA 2007. IEEE Symposium on (pp. 206-212). IEEE.
[29] Shedden, P., Ruighaver, T., & Ahmad, A. (2006). 'Risk Management Standards - the Perception of Ease of Use'. The 5th Security Conference, Las Vegas, USA.
[30] McEvoy, N., & Whitcombe, A. (2002). Structured risk analysis. Infrastructure Security, 88-103.
[31] Desouza, K. C. (2007). Managing knowledge security: strategies for protecting your company's intellectual assets. Kogan Page
[32] Ahmad, A., Ruighaver, A. B., & Teo, W. T. (2005). An Information-Centric Approach to Data Security in Organizations. In TENCON 2005 2005 IEEE Region 10 (pp. 1-5). IEEE.
[33] Crowston, K., & Williams, M. (2000). Reproduced and emergent genres of communication on the World-Wide Web. The Information Society, 16(3), 201-216
[34] Costa, C., Antunes, P., & Dias, J. (2002). Integrating two organizational Systems through communication genres. In Coordination Models and Languages (pp. 351-367). Springer Berlin/Heidelberg.
[35] Tyrvainen, P. (2003, January). Estimating applicability of new mobile content formats to organizational use. In System Sciences, 2003. Proceedings of the 36th Annual Hawaii International Conference on System Sciences (pp. 10-pp). IEEE.
[36] Holman, C. H. (1972). A handbook to literature (3rd ed). New York: Odyssey Press.
[37] Simons, H. W. (1978). "Genre-alizing" about rhetoric: A scientific approach. In K. K. Campbell & K. H. Jamieson (Eds.), Form and genre: Shaping rhetorical action: 33- 50. Falls Church, VA: Speech Communication Association.
[38] Miller, C. R. (1984), Genre as social action. Quarterly Journal of Speech, 70: 151-167.
[39] Saaren-Seppälä, K. (1997). Seinätekniikka prosessien kehittämisessä. (Using the wall-chart technique for process development, in Finnish). Kari Saaren-Seppälä Ltd., Finland.
[40] Alberts, C. J., Behrens, S. G., Pethia, R. D., & Wilson, W. R. (1999). Operationally critical threat, asset, and vulnerability evaluation (OCTAVE) framework, Version 1.0 (No. CMU/SEI-99-TR-017). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University.
[41] Charmaz, K., (2006). Constructing Grounded Theory: A Practical Guide through Qualitative Analysis, SAGE Publications
[42] Goulding, C., (2002). Grounded Theory: A Practical Guide for Management, Business and Market Researchers, SAGE Publications
[43] Guba, E. G., Lincoln, Y. S., (1989). Fourth generation evaluation, Newbury Park, CA; SAGE
[44] Jones, S., & Hughes, J. (2001). An exploration of the use of grounded theory as a research approach in the field of IS Evaluation. In Proceedings of the 8th European Conference on Information Technology Evaluation-2001 (p. 49). Academic Conferences Limited.
[45] Glaser, B. G., Strauss, A., (1967). The Discovery of Grounded Theory: Strategies for Qualitative Research, Chicago, IL: Aldine Publishing Co
[46] Strauss, A., Corbin, J. (1990). Basics of Qualitative Research: Grounded Theory Procedures and Techniques. London: Sage.
[47] Alberts, C., & Dorofee, A. (2004). Managing Information Security Risks, Mellon Software Engineering Institute, Pittsburgh, PA.
[48] Dhillon, G., & Backhouse, J.(2001). Current directions in IS security research: towards socio-organizational perspectives Information Systems Journal, 11(2), 127-153.

8. Appendix

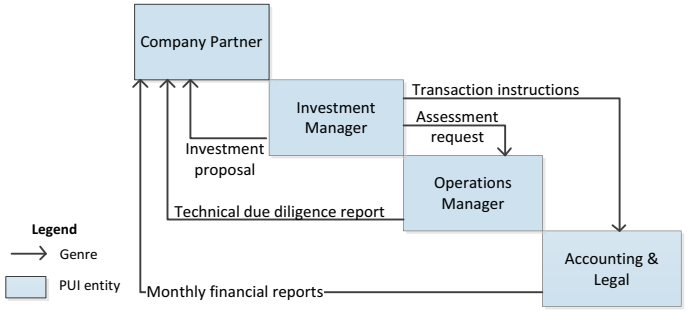

Figure 3 example of Diagonal matrix with genres and PUI entities

List of Content Types & Elements						
Source/Producer	Content & communication genres	Audience / User(s)	Owner(s)/Responsible(s)	When is communication done?	where does communication take place?	How do people communicate / share knowledge?
PUI / Producer	*Genre*	*PUI / User(s)*	*Whose?*	*When?*	*Where*	*How? (rules, application etc)*
Investment Manager	Transaction instructions	Accounting & legal	Accounting & Legal	Daily	PC (Account & legal staff)	Documents (DOC), email
Investment Manager	Assessment request	Operations Manager	Investment Manager, Operations	Monthly	mail server	email
Investment Manager	Investment proposal	Company partner	Investment Manager	Daily	PC (Investment Manager)	Documents (DOC, Paper), Presentations (PPT)
Accounting & legal	Monthly financial reports	Company partner	Accounting & Legal	Monthly	PC (Account & legal staff)	Documents (XLS, Paper), email
Operations Manager	Technical due diligence report	Company partner	Operations	Monthly	PC (Operations Staff)	Documents (DOC), Presentations (PPT)

Figure 4 example of a genre list

Monthly financial reports	Information Asset Risk Environment Map (Technical)	Monthly financial reports	Information Asset Risk Environment Map (People)
Internal		**Internal personnel**	
Container Description	**Owner(s)**	**Name of role / responsibility**	**Department or unit**
Formal files are XLS and they are saved in the internal server of the company	Accounting & Legal staff IT Operations	Accountant	Accounting & Legal
		System / network engineer	Internal IT
External		**External personnel**	
Container Description	**Owner(s)**	**Contractor / vendor, etc.**	**Organization**
Sent via email to the partners.	Partners	Partner employees who receive the reports via email and mail	Partner staff

Figure 5 example of container (technical & people) in OA worksheet 9

Monthly financial reports	INFORMATION ASSET RISK WORKSHEET		
Area of Concern	Reports are sent via email to partners		
(1) Actor Who would exploit the area of concern or threat?	Hacker		
(2) Means How would the actor do it? What would they do?	The attacker can attack the mail server to gain "financial reports" or intercept the traffic		
(3) Motive What is the actor's reason for doing it?	Financial gain		
(4) Outcome What would be the resulting effect on the information asset?	■ Disclosure ☐ Destruction ☐ Modification ☐ Interruption		
(5) Security Requirements How would the information asset's security requirements be breached?	Confidentiality security requirements will be breached if an attacker manages to acquire access to the server		
(6) Probability What is the likelihood that this threat scenario could occur?	☐ High	■ Medium	☐ Low
(7) Consequences What are the consequences to the organisation or the information asset owner as a result of the outcome and breach of security requirements?	(8) Severity How severe are these consequences to the organisation or asset owner by impact area?		
	Impact Area	**Value**	**Score**
If the attacker acquires the connection strings (username, password, internal IPs), the attacker might be able to connect to the database and execute queries outside the application's scope	Reputation & Customer Confidence	**High**	**5**
	Financial	**High**	**5**
If the attacker acquires administrative credentials to the database, the attacker will be able to disrupt the operation of the database	Productivity	**High**	**5**
	Safety & Health	**Low**	**1**
	Fines & Legal Penalties	**Medium**	**3**
	Accreditation	**Medium**	**3**
		Relative Risk Score	**22**

(9) Risk Mitigation Based on the total score for this risk, what action will you take?			
☐ Accept	☐ Defer	■ Mitigate	☐ Transfer
For the risks that you decide to mitigate, perform the following:			
On what container would you apply controls?	What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?		
Server	Following security controls needs to be deployed • Operating system hardening • Encryption • Patch Management		
Accounting & legal, partner	Arrange training awareness programs for the employees		

Figure 6 Risk analysis and mitigation strategy in OA worksheet 10