Problems in information classification: insights from practice

Simon Andersson
Department of Computer Science, Electrical and Space Engineering, Luleå University of Technology, Luleå, Sweden

Received 18 October 2022
Revised 19 January 2023
28 February 2023
2 March 2023
Accepted 3 March 2023

Abstract

Purpose – This study aims to identify problems connected to information classification in theory and to put those problems into the context of experiences from practice.

Design/methodology/approach – Five themes describing problems are discussed in an empirical study, having informants represented from both a public and a private sector organization.

Findings – The reasons for problems to occur in information classification are exemplified by the informants' experiences. The study concludes with directions for future research.

Originality/value – Information classification sustains the basics of security measures. The human–organizational challenges are evident in the activities but have received little attention in research.

Keywords Information classification, Risk assessment, Information security

Paper type Research paper

1. Introduction

Organizations need to know what information assets they own and how valuable they are for their business to apply protection against threats (Bergström *et al.*, 2019). It allows the organization to prioritize which assets to protect first and decide how to protect them. Such protection is important, as a compromise of information in terms of confidentiality, integrity or availability can cause financial, brand and reputational damage (Tankard, 2015). For organizations to work with the management of information security, they can use an information security management system (ISMS), such as the ISO/IEC 27000 Series (ISO Central Secretary, 2018), a family of standards recommending best practices for managing information security risks. A key part of an ISMS is asset management which includes the identification and valuation of information, with a core activity being information classification (Bergström and Anteryd, 2018).

The activity of information classification builds the base for protecting valuable assets and is the foundation of risk management. The classification results in a list of ranked assets, indicating their importance and value in terms of their criticality to the organization (Agrawal, 2017). ISO 27002:2017 (ISO Central Secretary, 2017) describes its objective as an activity that is necessary to *ensure that information receives an appropriate level of protection in accordance with its importance to the organization*. Once the classification of assets is set, the result act as input into the risk assessment where classified information is required to

The support from Interreg Aurora to the ISSUES project is gratefully acknowledged.

Information & Computer Security
Vol. 31 No. 4, 2023
pp. 449-462
Emerald Publishing Limited
2056-4961
DOI 10.1108/ICS-10-2022-0163

analyze, prioritize and manage risks and apply protection (Bergström and Åhlfeldt, 2014; Everett, 2011; Webb *et al.*, 2014). Thus, it is an essential piece of risk analysis and management within organizations (Bergquist *et al.*, 2021; Everett, 2011; Gerber and Von Solms, 2005). According to Veritas (2015), 54% of data in organizations are unclassified and unlabeled; the result is difficulties in effectively spending and using organizational resources as there is no possibility of applying protection to assets you do not know exist. Statistics from Kaspersky (2021) show that 10% of computers were subject to an attack during the year 2020, further showing the need for security measures.

Identifying and classifying information is not straightforward, and problems occur (Bergström and Åhlfeldt, 2014), leading to failures of the risk assessment and risk management activities if not accomplished (Shedden *et al.*, 2016; Webb *et al.*, 2014). Guidelines and standards, e.g. ISO 27002:2:2017 (ISO Central Secretary, 2017) and NIST 800–60 (Stine *et al.*, 2008), provide best-practice recommendations for information classification. Organizations often use and follow such standards; however, as they are necessarily adaptable and written with a general scope in mind, it leads to struggles in interpreting them as they are intentionally generic and provide little guidance on how to adopt them (Bayuk, 2010; Siponen, 2006). Further, organizations find it challenging to translate the standards into an organizational context and to turn them into concrete actions (Niemimaa and Niemimaa, 2017).

The occurrence of human-organizational problems in information classification has previously been identified (Bergström and Åhlfeldt, 2014), and further investigation has been suggested (Bergquist *et al.*, 2021). This paper presents an analysis of problems to shed light on them from a practice point of view. Thus, the study aims to identify and suggest future research activities connected to information classification in organizations.

2. Research design

This study is based upon qualitative data (Fossey *et al.*, 2002) in two forms, i.e. secondary (previous research) and primary (empirical data). The search for secondary data in articles was done using Google scholar and Scopus. See Table 1 for keywords and synonyms used. The first screening was applied to identify relevant articles, i.e. those describing problems and/or challenges in information classification. After that, the secondary data, i.e. the text in the articles, were analyzed using an open-coding approach (Burnard, 1991). Such analysis can, as such, follow a non–cross-sectional format (Mason, 2017), i.e. the categories emerged from the texts rather than were formulated beforehand.

The categorization of the secondary data resulted in the formulation of five problems; those problems then guided the empirical data collection. The identified problems were named: Deciding on a level of granularity, non-complete registry of assets, actor subjectiveness, discourse interpretation problems and difficult to adapt guidelines. An example of a quote and open coding can be seen in Table 2, paired with the relevant articles used to formulate the identified problems.

Keywords	Synonyms
Information classification	Asset classification, Data classification, Information asset classification
Challenges	Issues, Problems
Information security	Cyber security, Data security

Source: Created by author

Table 1.
Search words

Table 2. Example of coding and relevant articles used to formulate problems

Example of quote	Open coding	Articles used	Identified problem
" . . . but it is clear that many are struggling with granularity and the implications of it" (Bergström and Åhlfeldt, 2014, p. 34)	Organizations have difficulties deciding on a level of granularity	(Bergström and Åhlfeldt, 2014; Fibikova and Müller, 2011; Shedden *et al.*, 2016)	Deciding on a level of granularity
"An analysis is always just as good as the data it is based upon, and most risk management approaches are of little use without a reliable asset inventory" (Fenz *et al.*, 2014)	A complete registry is needed to achieve good risk management results	(Bergström *et al.*, 2019; Bergström and Åhlfeldt, 2014; Fenz *et al.*, 2014; Leming, 2015)	non-complete registry of assets
"Subjective Scoring Methods and Risk Matrices have been claimed to add their own sources of error in an ISRM (Hubbard, 2020; Anthony (Tony) Cox, 2008). Such as compressing ranges (Anthony (Tony) Cox, 2008), presumption of regular intervals, e.g. different people at different levels in an organization will rate scales differently (Hubbard, 2020)" (Wangen and Snekkenes, 2013, p. 5)	Depending on previous experiences, roles, framing etc. one tends to interpret and value risk and value of/to assets differently	(Bergström *et al.*, 2019; Bergström *et al.*, 2021; Bergström and Åhlfeldt, 2014; Anthony (Tony) Cox, 2008; Fenz *et al.*, 2014; Hubbard, 2020; Kaarst-Brown and Thompson, 2015; Sajko *et al.*, 2006; Wangen and Snekkenes, 2013)	Actor subjectiveness
"The need for a security ontology, a 'common language' for IS professionals to ease communication and help achieve a common understanding of IS across companies and borders." (Wangen and Snekkenes, 2013)	Not understanding each other properly will lead to problems in discussions and interpretations of discourse	(Ahmad *et al.*, 2015; Arhin and Wiredu, 2018; Richmond *et al.*, 2005; Shedden, 2016; Wangen and Snekkenes, 2013)	Discourse interpretation
"As collections of canonical practices, they 'inevitably and intentionally omit the details' (Brown and Duguid, 1991, p. 40), making them too abstract to be directly applicable to a specific organizational context." (Niemimaa and Niemimaa, 2017, p. 12)	Guidelines are difficult to interpret and adapt as they often omit details	(Bayuk, 2010; Bergström, 2020; Bergström *et al.*, 2021; Brown and Duguid, 1991; Niemimaa and Niemimaa, 2017; Fibikova and Müller, 2011; Ghernaouti-Helie *et al.*, 2011; Park *et al.*, 2010)	Difficult to adapt guidelines

Source: Created by author

The five categorized problems then guided the data collection which was conducted within a private sector organization that provides information security consultancy services and within a public authority organization with its main task positioned in IT. Using private and public-sector organizations allowed different actors to provide insight from varying viewpoints. The respondents were found in collaboration with a representative from the organizations' information security department.

A semi-structured approach was applied in the collection of empirical data (Fontana *et al.*, 2000). The five identified problems were thus representing the themes for data collection, which contained open-ended questions investigating the categorized problems of information classification. The open-ended questions allowed the informants to formulate their answers freely (Adams, 2015; Pedersen *et al.*, 2016) while making it possible for them to focus on the topics. The interviews lasted between 28 and 72 min and were recorded and later verbatim transcribed, i.e. word for word (Halcomb and Davidson, 2006). The analysis of the transcribed empirical data can be described as a thematical text analysis (Clarke *et al.*, 2015). The analysis of the empirical data identified, interpreted and searched for patterns which explained experiences in relation to the categories of problems (Clarke *et al.*, 2015). Expressions from the respondents have been used to add additional insights and understanding from practice to problems (Alhojailan, 2012). Table 3 shows an overview of the respondents, their position in the organization, the length of the interview, the abbreviation used in the analysis and which sector they belong to.

3. Asset management and information classification

For organizations to work with risk management, they can use an ISMS to minimize adverse events by assessing potential risks and assigning appropriate security measures where necessary (Shameli-Sendi *et al.*, 2016). An ISMS describes methods organizations can use to secure their assets and consists of a collection of policies, procedures and guidelines based on best practices (ISO Central Secretary, 2018; Niemimaa and Niemimaa, 2017). Within such a framework, asset management is considered to be a crucial part and includes the identification and valuation of information. The intent of asset management is to know what information exists and to value that information, with a core activity being information classification. The classification is, in turn, a crucial part of risk analysis (Gerber and Von Solms, 2005). The information classification results in a valuation of information assets in terms of confidentiality, integrity and availability. This valuation indicates how information can be, e.g. handled, stored and potential consequences in the case of a compromise (Bergström and Anteryd, 2018). The classified assets act as the primary input to the risk analysis, which is needed to understand what kind of protection to apply.

Position	Length of interview	Abbreviation	Sector
Business Developer	60 min	BD	Private
Senior Information Security Consultant	1 h 12 min	SISC	Private
Senior Consultant/IT-Archivist	28 min	SC/ITA	Private
IT-Archivist	40 min	ITA	Private
Information Security Specialist	42 min	ISS	Public
Object Owner	40 min	OO	Public
Information Security Specialist 2	36 min	ISS2	Public
Information and Data-protection coordinator	35 min	IDPO	Public

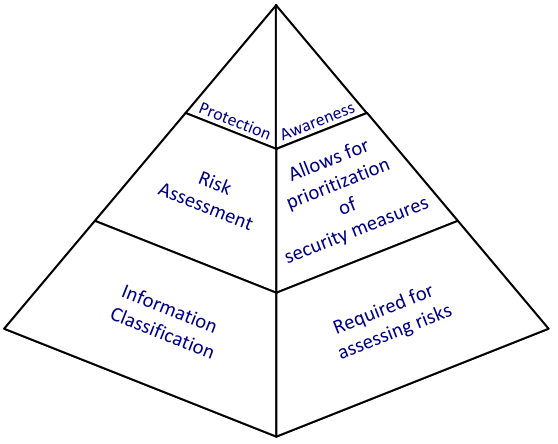
Source: Created by author

Table 3. Overview of informants

Conducting information classification is often done with the use of a classification scheme that contains a chosen number of consequence levels and definitions of each level in terms of confidentiality, integrity and availability (Bergquist *et al.*, 2021). It is necessary to define the stated levels clearly; not doing so can result in uneven classifications if there is too much room for interpretation. Each asset then receives a classification based on how valuable its confidentiality, integrity and availability are to the organization. The value is based on the potential consequence of information compromise. Typically, organizations divide consequences into sections such as financial and reputational consequences (Tankard, 2015). Doing so allows for a clearer view of how compromised assets might affect the organization to be gained. Additionally, classifying the asset from different perspectives, such as from a business continuity perspective or a reputational perspective shows the value of the asset from different viewpoints. With a classification in place, it allows the organization to gain knowledge of the identified assets' value in terms of how critical they are to business practices, how to prioritize them for the application of protection and to what extent the organization should spend resources to keep them protected (Agrawal, 2017). If the information classification is not considered a critical activity, it can lead to problems with the risk assessment. If there are shortcomings with the classification, it will reduce the possibility of adequately protecting the organizational assets as less knowledge is available, leading to less informed decisions (Shedden *et al.*, 2016; Webb *et al.*, 2014). Further, it also means that assets that should have been identified will remain unidentified. Thus, the organization is unaware of how to prioritize it for protection and what amount of resources is necessary to spend to keep it secure. Figure 1 showcases a thought-model of dependencies between information classification, risk assessment and applied protective measures, displaying the activity on the left side and its purpose on the right.

4. Insights from practice on information classification problems

The paper addresses five problems categorized as relevant for information classification: deciding on a level of granularity, non-complete registry of assets, actor subjectiveness, discourse interpretation and difficult to adapt guidelines. They are first explained one-by-one



Source: Created by author

Figure 1.
Dependencies between information classification, risk assessment and protection

from a theoretical perspective and then put into the context of experiences in the following section which presents and discusses empirical data.

Deciding on a level of granularity, to find an appropriate level of detail of the identified information, has been found to be a challenge (Bergström and Åhlfeldt, 2014; Shedden *et al.*, 2016). A high level of granularity means that the classification is done on every single file. Such an approach provides a detailed view of assets. A low level of granularity means that classifying assets is based on a whole system or a complete process as a cohesive unit. Naturally, the latter approach is less resource-intensive and might explain why a default approach in many organizations is to apply a low level of granularity (Shedden *et al.*, 2016). Such an approach might seem useful at the time. However, it can result in failures to identify important components of a system or a process, consequently leaving the organization with unidentified risks and assets that remain unprotected (Shedden *et al.*, 2016). Deciding on a level of granularity might be considered a simple task, but it is a critical choice for the remaining classification. The decision to use a high or low level of granularity will impact measures needed to protect the asset. A low level of granularity will thus reduce the needed resources while accepting a higher level of risk, given that assets can remain unidentified. Fibikova and Müller (2011) conclude that no straightforward suggestion can guide organizations in making the decision of granularity. Such a decision depends on the specific circumstances of each organization's business. Additionally, the asset value and risks tied to organizational assets change over time, further complicating the decision (Fibikova and Müller, 2011).

The data from informants highlight specific issues related to decisions on the level of granularity. One informant state that they start from a vast base of information that ranges from single documents to batches. The informant continues to describe that an overview and knowledge of the information base is needed:

> We cannot classify information side by side, object by object. There has to be some sort of batching made. However, it is also important to understand that sometimes we have to break the batches. This is something that you learn as you reiterate the process – SISC.

Informants also describe that involving staff close to or responsible for a system is a cause for problems. One example an informant brings up is system developers, who tend to add a high level of granularity:

> Developers for example, they bring a database-model and starts to classify each row with an extreme amount of detail with timestamps etc. It is not necessary to be at that level; you have to think about it logically. – ISS

With the problem of being too close to the information source in focus, the informant further explained that one major challenge is the dialogue between them, i.e. the information security specialists and the system developers. How can one find a satisfying level of granularity when one part focuses on bits and pieces and the other to gain a bigger picture view? The informant continued to reflect on experiences and explained that there is a benefit in bringing in another role into the decision-making, e.g. a person with a better understanding of how the information assets in the system at hand impacts the core business. Such a person can aid in the dialogue, the informant says, for example, by explaining and exemplifying how the information matters beyond the core system. Thus, understanding how and why it needs to be classified becomes clearer.

When interpreting the problem of deciding on a level of granularity in relation to the insights from practice, it can be discerned that such decisions are still problematic. It also indicates insight as to why a lower level of granularity tends to be an initial choice for organizations, e.g. allocating resources is a challenge, the starting point is troublesome and

the dialogues between the different roles are challenging. Communication between different actors is previously identified as causing problems, for example, due to information overload (too much information), low interest among actors and inappropriate language based on whom you are addressing (Cacciattolo, 2015). This study indicates a "catch-22" moment due to the mutually conflicting and simultaneous dependent elements in information assets, e.g. if you choose details, you risk losing the overview and vice-versa. Thus, improving the dialogues across and between actors are one area in need of more studies, e.g. questions to reflect on how communication about the rationale related to the core businesses could improve information classification. One approach could be to agree on basic knowledge exchange practices, for example drawing from knowledge management approaches for perspective making and perspective taking (Boland and Tenkasi, 1995). Another approach to assisting in the choice of granularity-decisions could be to investigate the issue through an information- and knowledge-centric perspective using a genre-based approach (Padyab, Päivärinta, and Harnesk, 2014; Yates and Orlikowski, 1992).

Non-complete registry of information assets means that there is no complete collection of identified assets. A registry of information assets is a way for organizations to keep track of what information they own and how it is valued and managed (Leming, 2015). Even though it is of value, a common problem within organizations is an incomplete or even lacking record of information assets (Bergström and Åhlfeldt, 2014). A complete registry, or at least a satisfying one, is seen as a fundamental part of good risk management (Leming, 2015). Part of the problem with maintaining an inventory is the scope, size and rate of internal and external change (Rees and Allen, 2008). Such changes can refer to the creation and removal of information. Naturally, the larger the organization, the more resource-intensive the task of keeping it up to date is. As the risk assessment aid protection of organizational assets based on what is in the registry, keeping an inventory alive is essential; without a complete risk registry, most risk management approaches will be less effective (Fenz *et al.*, 2014).

Data from informants show that keeping a registry of information assets up to date is a challenge; the study also highlights uses for a registry other than keeping up to date with the organizationally owned information. Informants reflected on the problem of incomplete registries:

> First of all, it is important to value the information, but the first step is to make an inventory! Often times the inventory is not very well done, and that complicates things. All of a sudden, there is data you had no idea existed [. . .]. – BD

The informant continues to explain the importance of understanding the organization's assets and expands on the need for a registry. The informant explains that a registry is required to conduct the information classification properly and argues further that it is difficult to classify and value something you are unaware of. Additionally, the informant describes that the information security work starts with identifying, categorizing and making an inventory of information assets:

> It all starts with the work connected to information classification. Sometimes the inventory is there, and at some organizations, it is not there at all. – SISC

One informant also explains an additional benefit of having an up-to-date inventory, namely, that it can be used as a means of communication between management and employees. Using it this way, the informant explains that everyone gets involved and can understand the value of the information they are working with. Consequently, raising security awareness in the organization. The informant says that updating the registry is a rare opportunity to discuss potential consequences of leakage of information and to share experiences of such events.

Analyzing the problem of a non-complete registry of information assets, when put into the context of practice, it can be found that keeping it up to date is resource demanding. New (unknown) information assets that appear later in the information classification put the actors into trouble. The challenge to keep the registries updated may relate to the allocation of resources but may also relate to an organization that accepts a high level of granularity. That is, such decisions may support one activity but may cause problems at a later stage. The additional benefit of updating the registry identified in this study, i.e. to use it to aid involvement and interactions between different roles, is an interesting approach that needs to be studied further.

Actor subjectiveness can be described as the idea that humans can have the same experience but different understandings of that experience (Thorburn and Stolz, 2020). Subjectiveness is often affected not only by external sources, such as culture, norms and similar factors, but also by an individual's awareness of social, economic and legal contexts (Kaarst-Brown and Thompson, 2015). Differing opinions on the correct value of a certain information asset is a common topic of competing arguments between actors. Subjective judgments in the classification activities can lead to the well-known problem of inconsistent classifications (Bergström and Åhlfeldt, 2014; Bergström *et al.*, 2021; Fenz *et al.*, 2014; Sajko *et al.*, 2006), and this problem is often overlooked in practice and is under-researched.

In the investigation for this study, it was found that subjectiveness is indeed an issue. When asked about what challenges appear when conducting information classification activities several informants mention subjectiveness. One informant elaborates on the problem and explains that when a disagreement over a classification occurs, it is often followed by a lengthy discussion resulting in over-protecting assets. The informant explains:

> [. . .] then you have to argue for your standpoint. As long as there is no documentation done that says a decision has been made there are a lot of discussions. We at IT who work with protecting this information are put into a difficult situation. This means that in most cases you put a higher level of protection than necessary just to be on the safe side. – IDPO

The informant continues to describe that the results of over-protection is higher costs, not just monetary but also in time. The informant gives examples, such as costs tied to upgrades of a system that is accepted to handle a higher level of protection will be higher, the update will be more extensive and simply more complex. Further, another informant mentions that a tool has been developed to get around the extensive discussions regarding different opinions about asset values:

> It is very good to have a tool that contains questions, there won't be a lot of discussion and time can be spent on discussing other matters, not the classification itself [. . .] If the tools are configured well, you can save quite a lot of time when it comes to the classification as many hours can be spent on discussion if the group does not agree. – ISS2

The use of the tool has, according to the informant, not only saved them a lot of time and resources but also, in a way, reduced subjective judgment when deciding on the classification levels. The informant explained that the tool's content of requirements for information assets has made the classification process more effective. However, not all assets can be classified, and not all discussions are solved using the tool. The same informant mentions that information classification activities are a great way to connect with other departments as often, they are done cooperatively with other departments. As a result of different backgrounds between departments, the risk of misunderstandings and different interpretations of asset value is high, but the tool has assisted with better communication.

When analyzing the problem of actor subjectiveness in light of the practice, the consequence that it leads to lengthy discussions and argumentation becomes evident. Actor subjectiveness also leads to inconsistent classification. The empirical study points toward

over-protection being a typical solution to feeling safe when opposing arguments for an asset value are suggested. In response to subjectivity leading to lengthy discussions, one organization reduced the time spent on such discussions by using a self-developed tool. Subjectivity is viewed as a negative trait; however, different opinions are expressions of different experiences, and speaking them out allows for nuanced views of the information assets and their value. This study indicates that subjectiveness can, if organized and structured, become a benefit in information classification. Yet, lengthy discussions of every asset will not be beneficial, but allowing actors to express different arguments in some cases may provide a better understanding of the information classification problems and raise organizational security awareness.

Discourse interpretation is the action of interpreting someone's speech or piece of writing about a particular, usually serious, subject (Cambridge, 2022). As such, it is part of communication as a movement of information from a source through a channel to a destination (Arhin and Wiredu, 2018; Shannon, 1948). Information security is an interdepartmental effort rather than tied to only an IT department (Ahmad *et al.*, 2015). Thus, communication between departments is essential for the interdepartmental effort to be effective. Communicating guidelines, frameworks or manuals has proved to be problematic. Telling an employee within an organization, in writing or by voice, to read a security-guideline handbook does not necessarily mean that the employee has been communicated to (Richmond *et al.*, 2005). When communicating with others on, e.g. a departmental level, issues can appear as a cause of several factors, some tied to knowledge sharing and organizational communication. Common problems are low motivation and interest, inappropriate language, information overload, technological problems and insufficient non-verbal communication, thus causing problems with the interpretation of a particular discourse (Cacciattolo, 2015; Riege, 2005).

The study shows that discourse interpretation is both common and challenging. It is by informants deemed very important to be able to communicate between stakeholders; however, it is also expressed to be difficult in a variety of ways. One informant mentions that part of the communication issues they experience is a result of several factors, like the language used, this involves jargon, e.g. department-specific terms and interpretations, a lack of understanding of the context and difficulties of understanding each other when using only digital support. It is, according to several informants, important to ask questions in a way that can be easily understood and interpreted. Further, several informants stated that the terms used are of great importance for better understanding the topics at hand:

> You write statements and guidelines with a language that can be very difficult to understand and use terms that employees simply do not use. – ISSC2

> Communication between departments is difficult, especially when you use the same terms but mean different things. There is confusion in the terms used. This information is secret, is it secret or very secret? You have to understand the differences. It can be the result of a cultural, competence or an "in a hurry" barrier. – OO

> We prefer to solve everything digitally, it is little effort and reaches a large amount of people [. . .] but [. . .] It is difficult to formulate in writing so that everyone can understand, the co-workers will understand the message in different ways. – IDPO

The above excerpts highlight problems encountered by informants in the information classification but are also challenges regarding communication in general. In essence, the problems are grounded on the use of different expressions and terms, which mean different things to different roles and departments.

According to many informants, the language used is an influencing factor for whether there would be an understanding of each other when communicating about information classification activities. Plain explanations to also understand the context is something that was perceived as supporting communication. However, there can be regulations in public sector organizations that force actors to apply a certain type of language, for examples using words that are seldom used by the public. Often, confusion and misunderstandings occur because a term is interpreted in different ways, depending on how it is established as a jargon within a certain knowledge domain.

Difficult to adapt guidelines is another categorized problem (Bayuk, 2010; Bergström *et al.*, 2021; Park *et al.*, 2010). Standards such as ISO/IEC 27002 (ISO Central Secretary, 2017) are a commonly used base for organizations to create guidelines. Standards, though, describe the activities holistically, meaning it is not a blueprint for how to apply them in organizations. One example of a problem is the difficulty of creating classification schemes that follow organizational requirements while still being usable (Bergström, 2020; Fibikova and Müller, 2011; Ghernaouti-Helie *et al.*, 2011). It is also concluded that there is a gap between formal and actual processes in information security management, which information classification is part of (Bergström *et al.*, 2021). Adopting best-practice into organizations has been stated as being difficult, not necessarily in the writing of policies but in implementing it in a way that is sensitive to the context of the organization and its local ways of working (Niemimaa and Niemimaa, 2017).

The expressions from informants indicate that organizations struggle to interpret and adapt best-practice guidelines. Both internal and external guidelines regarding information classification are according to informants difficult to interpret. One informant speaks about requirements for how to write descriptions and guidelines:

> In the world of public sector, we write regulations and guidelines in a way that is difficult to interpret and we use terms and phrases that normal persons simply does not use. – ISS2

Informants having the experience writing guidelines, such as the definitions of different security levels that should later be used as a reference for other actors when conducting classification activities, express the difficulty:

> You get into discussions where you look at consequences in terms of physical, psychological and financial. Will this asset be in what our model (classification scheme) is a limited value or high value? Where do we draw the lines? That is often the main discussion [. . .] Often times the differences between levels are quite vague and it is challenging to describe the levels in a clear manner. – ISS2

Addressing the same issue, another informant states that one problem is the formulation, description and definitions of those levels and the terms used in them. Using terms such as "great effect" is very interpretable and difficult to describe. According to the informant, this often leads to classifications that are one step above necessary as there is a fear of classifying assets too low. This reflection gets confirmed by another informant that explains that internal documents to guide the classification activities exist, but they are difficult to use and vague in their descriptions. This results in guesswork to reach a classification. The informant understands that an organization cannot describe everything in documents but describes the problem of interpretations:

> You can't explain everything, but you can help by writing easy generic matrices. I sometimes see explanations of classifications to be 'results in high level of monetary loss'. What is high? And what is low? You have to help out with these things. – SISC

Giving examples are, by several informants, stated to be helpful, but, if too detailed, actors will try to replicate the examples instead of using them as guidelines for the classification. One informant concludes that while it is important to use examples for actors unfamiliar with the process, it is also important not to make examples too specific.

The problems with adapting guidelines are analyzed in this study as related to those being too complicated or general. Even though the informants are aware of the necessity to transform guidelines to the organization's requirements, they express a wish of them being more specific. The informants also describe the paradox of using examples: they cannot be too specified, but not too general either. Further studies of interest could include how to provide good and usable examples.

5. Concluding on further research

This paper presents five problems identified related to information classification and sheds light on how those problems are experienced in practice. The problems were as follows: *deciding on a level of granularity*, *non-complete registry of assets*, *actor subjectiveness*, *discourse interpretation* and *difficult to adapt guidelines*. Empirical data from two types of organizations, i.e. public and private, was collected to shed light on the practice in relation to the problems, thus addressing the purpose which was to identify future research directions. Solving the problems within information classification is no simple task. However, as the problems that have been presented here indicate, research beyond technical challenges can help organizations to classify their assets. This paper, thus suggests a number of directions for further studies, namely:

- Research addressing the problems of choosing a level of granularity could involve perspective-making and perspective-taking (Boland and Tenkasi, 1995), thereby highlighting for example communication practices. Related to the problem it would be interesting to investigate communicative genres to identify critical information (Päivärinta, 2001).
- The problem of having a non-complete registry of assets could be a base for studies of how different roles in an organization, such as managers and developers, apply different lenses of worldviews (Checkland, 2000) that guide communication.
- Research targeting if and how actor subjectiveness can be organized and structured to allow informed decision-making would benefit the classification work. Such studies could alter how experiences are perceived as a negative trait and turn it into a base of best practices.
- Investigations addressing the problem of discourse interpretation could focus the work done in groups and workshops, for example including interpersonal response behaviour in teams (Sonalkar *et al.*, 2012). Additionally, further investigation on how to define, not absolute, but operative terms in multi-departmental organizations is of interest to tackle this problem.
- The problem of difficult to adapt guidelines could be a base for user-oriented research focusing on how to formulate functional guidelines that meet realistic behaviour in the workplaces. Behaviour design or nudging (Thaler and Sunstein, 2009), for example, could add to the understanding of how guidelines could be adapted to organizational behaviour.

References

Adams, W.C. (2015), "Conducting semi-structured interviews", *Handbook of Practical Program Evaluation*, pp. 492-505.

Agrawal, V. (2017), "A framework for the information classification in ISO 27005 standard", *2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud)*, New York, NY, IEEE, pp. 264-269, ISBN: 978-1-5090-6644-5, doi: 10.1109/CSCloud.2017.13.

Ahmad, A., Maynard, S.B. and Shanks, G. (2015), "A case analysis of information systems and security incident responses", *International Journal of Information Management*, Vol. 35 No. 6, pp. 717-723.

Alhojailan, M.I. (2012), "Thematic analysis: a critical review of its process and evaluation", *West East Journal of Social Sciences*, Vol. 1 No. 1, pp. 39-47.

Anthony (Tony) Cox, L. Jr (2008), "What's wrong with risk matrices?", *Risk Analysis: An International Journal*, Vol. 28 No. 2, pp. 497-512.

Arhin, K. and Wiredu, G.O. (2018), "An organizational communication approach to information security", *The African Journal of Information Systems*, Vol. 10 No. 4, p. 1.

Bayuk, J.L. (2010), "The utility of security standards", *44th Annual 2010 IEEE International Carnahan Conference on Security Technology*, pp. 1-6, doi: 10.1109/CCST.2010.5678676.

Bergquist, J.-H., Tinet, S. and Gao, S. (2021), "An information classification model for public sector organizations in Sweden: a case study of a Swedish municipality", *Information and Computer Security*, pp. 2056-4961, doi: 10.1108/ICS-03-2021-0032.

Bergström, E. (2020), "Supporting information security management: developing a method for information classification", PhD thesis. University of Skövde.

Bergström, E. and Åhlfeldt, R.-M. (2014), "Information classification issues", *Secure IT Systems*, in Bernsmed, K. and Fischer-Hübner, S. (Eds), Springer International Publishing, Cham, Vol. 8788, pp. 27-41, ISBN: 978-3-319-11598-6 978-3-319-11599-3, doi: 10.1007/978-3-319-11599-3_2.

Bergström, E. and Anteryd, F. (2018), "Information classification policies: an exploratory investigation", p. 15.

Bergström, E., Karlsson, F. and Åhlfeldt, R.-M. (2021), "Developing an information classification method", *Information and Computer Security*, Vol. 29 No. 2, pp. 209-239, ISSN: 2056-4961, 2056-4961, doi: 10.1108/ICS-07-2020-0110.

Bergström, E., Lundgren, M. and Ericson, Å. (2019), "Revisiting information security risk management challenges: a practice perspective", Security Risk Management Challenges: A Practice Perspective, Information & Computer Security.

Boland, R.J., Jr. and Tenkasi, R.V. (1995), "Perspective making and perspective taking in communities of knowing", *Organization Science*, Vol. 6 No. 4, pp. 350-372.

Brown, J.S. and Duguid, P. (1991), "Organizational learning and communities-of-practice: toward a unified view of working, learning, and innovation", *Organization Science*, Vol. 2 No. 1, pp. 40-57.

Burnard, P. (1991), "A method of analysing interview transcripts in qualitative research", *Nurse Education Today*, Vol. 11 No. 6, pp. 461-466.

Cacciattolo, K. (2015), "Defining organisational communication", *European Scientific Journal*, Vol. 11 No. 20.

Cambridge, D. (2022), "Meaning of discourse in english", available at: https://dictionary.cambridge.org/dictionary/english/discourse

Checkland, P. (2000), *Soft Systems Methodology: A Thirty Year Retrospective*, Systems Research and Behavioral Science.

Clarke, V., Braun, V. and Hayfield, N. (2015), "Thematic analysis", *Qualitative Psychology: A Practical Guide to Research Methods*, pp. 222-248.

Everett, C. (2011), "Building solid foundations: the case for data classification", *Computer Fraud and Security*, Vol. 2011 No. 6, pp. 5-8.

Fenz, S., Heurix, J., Neubauer, T. and Pechstein, F. (2014), "Current challenges in information security risk management", *Information Management and Computer Security*, Vol. 22 No. 5, pp. 410-430, doi: 10.1108/IMCS-07-2013-0053, 0968-5227.

Fibikova, L. and Müller, R. (2011), "A simplified approach for classifying applications", *ISSE 2010 Securing Electronic Business Processes: Highlights of the Information Security Solutions Europe 2010 Conference*, in Pohlmann, N., Reimer, H. and Schneider. W. (Eds), Wiesbaden, Vieweg+Teubner, pp. 39-49. ISBN: 978-3-8348-9788-6, doi: 10.1007/978-3-8348-9788-6_4.

Fontana, A. and Frey, J.H., *et al.* (2000), "The interview: from structured questions to negotiated text", *Handbook of Qualitative Research*, Vol. 2 No. 6, pp. 645-672.

Fossey, E., Harvey, C., McDermott, F. and Davidson, L. (2002), "Understanding and evaluating qualitative research", *Australian and New Zealand Journal of Psychiatry*, Vol. 36 No. 6, pp. 717-732.

Gerber, M. and Von Solms, R. (2005), "Management of risk in the information age", *Computers and Security*, Vol. 24 No. 1, pp. 16-30.

Ghernaouti-Helie, S., Simms, D. and Tashi, I. (2011), "Protecting information in a connected world: a question of security and of confidence in security", *2011 14th International Conference on Network-Based Information Systems*, *IEEE*, pp. 208-212.

Halcomb, E.J. and Davidson, P.M. (2006), "Is verbatim transcription of interview data always necessary?", *Applied Nursing Research*, Vol. 19 No. 1, pp. 38-42.

Hubbard, D.W. (2020), *The Failure of Risk Management: Why It's Broken and How to Fix It*, John Wiley and Sons.

ISO Central Secretary (2017), *Information Technology – Security Techniques – Code of Practice for Information Security Controls*, Standard ISO/IEC 27002:2017 International Organization for Standardization, Geneva, CH.

ISO Central Secretary (2018), *Information Technology – Security Techniques – Information Security Management, Systems – Overview and Vocabulary*, Standard ISO/IEC 27000:2018 International Organization for Standardization, Geneva, CH, available at: www.iso.org/standard/73906.html

Kaarst-Brown, M.L. and Thompson, E.D. (2015), "Cracks in the security foundation: employee judgments about information sensitivity", *Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research. SIGMIS-CPR '15: 2015 Computers and People Research Conference*. Newport Beach CA USA, ACM, pp. 145-151, ISBN: 978-1-4503-3557-7, doi: 10.1145/2751957.2751977, available at: https://dl.acm.org/doi/10.1145/2751957.2751977 (visited on 01/31/2022).

Kaspersky (2021), "KSB_statistics_2020_en.Pdf", available at: https://go.kaspersky.com/rs/802-IJN-240/images/KSB%5C_statistics%5C_2020%5C_en.pdf

Leming, R. (2015), "Why Is information the elephant asset? An answer to this question and a strategy for information asset management", *Business Information Review*, Vol. 32 No. 4, pp. 212-219, ISSN: 0266-3821, doi: 10.1177/0266382115616301.

Mason, J. (2017), *Qualitative Researching*, *SAGE Publications*, London.

Niemimaa, E. and Niemimaa, M. (2017), "Information systems security policy implementation in practice: from best practices to situated practices", *European Journal of Information Systems*, Vol. 26 No. 1, pp. 1-20.

Padyab, A., Päivärinta, T. and Harnesk, D. (2014), "Genre-based approach to assessing information and knowledge security risks", *International Journal of Knowledge Management*, Vol. 10, pp. 13-27, doi: 10.4018/ijkm.2014040102.

Päivärinta, T. (2001), "The concept of genre within the critical approach to information systems development", *Information and Organization*, Vol. 11 No. 3, pp. 207-234.

Park, W.-S., Seo, S.-W., Son, S.-S., Lee, M.-J., Kim, S.-H., Choi, E.-M., Bang, J.-E., Kim, Y.-E. and Kim, O.-N. (2010), "Analysis of information security management systems at 5 domestic hospitals with more than 500 beds", *Healthcare Informatics Research*, Vol. 16 No. 2, pp. 89-99, doi: 10.4258/hir.2010.16.2.89, ISSN: 2093-369X.

Pedersen, B., Delmar, C., Falkmer, U. and Grønkjær, M. (2016), "Bridging the gap between interviewer and interviewee:d an interview guide for individual interviews by means of a focus group", *Scandinavian Journal of Caring Sciences*, Vol. 30 No. 3, pp. 631-638, ISSN: 1471-6712, doi: 10.1111/scs.12280.

Rees, J. and Allen, J. (2008), "The state of risk assessment practices in information security: an exploratory investigation", *Journal of Organizational Computing and Electronic Commerce*, Vol. 18 No. 4, pp. 255-277, ISSN: 1091-9392, doi: 10.1080/10919390802421242, available at: www.tandfonline.com/doi/abs/10.1080/10919390802421242 (visited on 01/31/2022).

Richmond, V.P., McCroskey, J.C. and McCroskey, L.L. (2005), "Organizational communication for survival: making work", *Work*, Vol. 4, Allyn and Bacon.

Riege, A. (2005), "Three-dozen knowledge-sharing barriers managers must consider", *Journal of Knowledge Management*, Vol. 9 No. 3, pp. 18-35.

Sajko, M., Rabuzin, K. and Baca, M. (2006), "How to calculate information value for effective security risk assessment", *Journal of Information and Organizational Sciences*, Vol. 30 No. 2, pp. 263-278.

Shameli-Sendi, A., Aghababaei-Barzegar, R. and Cheriet, M. (2016), "Taxonomy of information security risk assessment (ISRA)", *Computers and Security*, Vol. 57, pp. 14-30.

Shannon, C.E. (1948), "A mathematical theory of communication", *The Bell System Technical Journal*, Vol. 27 No. 3, pp. 379-423.

Shedden, P., Ahmad, A., Smith, W., Tscherning, H. and Scheepers, R. (2016), "Asset identification in information security risk assessment: a business practice approach", *Communications of the Association for Information Systems*, Vol. 39, pp. 297-320, ISSN: 15293181, doi: 10.17705/1CAIS.03915, available at: http://aisel.aisnet.org/cais/vol39/iss1/15/ (visited on 01/31/2022).

Siponen, M. (2006), "Information security standards focus on the existence of process, not its content", *Communications of the ACM*, Vol. 49 No. 8, pp. 97-100.

Sonalkar, N.S., Mabogunje, A.O. and Leifer, L.J. (2012), "A visual representation to characterize moment to moment concept generation in design teams", *DS 73-1 Proceedings of the 2nd International Conference on Design Creativity Volume 1*.

Stine, K., Kissel, R., Barker, W., Lee, A. and Fahlsing, J. (2008), *Guide for Mapping Types of Information and Information Systems to Security Categories: appendices*, Tech. rep. National Institute of Standards and Technology.

Tankard, C. (2015), "Data classification–the foundation of information security", *Network Security*, Vol. 2015 No. 5, pp. 8-11.

Thaler, R.H. and Sunstein, C.R. (2009), "NUDGE: improving decisions about health, wealth, and happiness", Penguin.

Thorburn, M. and Stolz, S.A. (2020), "Understanding experience better in educational contexts: the phenomenology of embodied subjectivity", *Cambridge Journal of Education*, Vol. 50 No. 1, pp. 95-105.

Veritas (2015), "The databerg report: see what others don't", available at: http://info.veritas.com/databerg_report

Wangen, G. and Snekkenes, E. (2013), "A taxonomy of challenges in information security risk management", *Proceeding of Norwegian Information Security Conference/Norsk informasjonssikkerhetskonferanse-NISK 2013-Stavanger*, 18th-20th November 2013, Akademika Forlag.

Webb, J., Maynard, S., Ahmad, A. and Shanks, G. (2014), "Information security risk management: an intelligence-driven approach", *Australasian Journal of Information Systems*, Vol. 18 No. 3, pp. 1449-8618, doi: 10.3127/ajis.v18i3.1096.

Yates, J. and Orlikowski, W.J. (1992), "Genres of organizational communication: a structurational approach to studying communication and media", Vol. 29.

Corresponding author
Simon Andersson can be contacted at: simon.andersson@ltu.se