Information Classification Policies: An Exploratory Investigation

Erik Bergström, Fredrik Anteryd2,
Rose-Mharie Åhlfeldt School of Informatics,
University of Skövde, Sweden,
{erik.bergstrom, rose-mharie.ahlfeldt}@his.se fanteryd@gmail.com

Abstract

InfoSec policies are considered a key mechanism in information security, and most organizations have one. However, the large majority of security policy research has focused on what policies should include rather than how they are accomplished in practice. To contribute to overcoming the lack of knowledge regarding this crucial aspect, this paper investigates information security policies based on what underlying approaches information classification practices are built on and the perceived ease of turning the policy into practice. To do so, a survey was sent to 284 Swedish government agencies, and 80 of their internal policies were collected as data. The data were analyzed both qualitatively, and qualitatively. The results show that information classification adoption rates are low despite being mandatory and that agencies are struggling in closing the gap between standards and practice. Furthermore, the results also show that information classification policies need to be more specific and give more actionable advice regarding, e.g., how information life-cycle management is included in practice, and where the responsibility for classification is put in the organization.

Keywords: Information security management, information classification, InfoSec policies.

Introduction

The costs associated with malicious breaches are skyrocketing and is expected to increase to more than 2 trillion USD (2,2% of the world's GDP) by 2019, which is a quadrupling since 2015 (Moar, 2015). Information and information systems have become key assets in organizations, and through the selection and application of appropriate policies, standards, and procedures, breaches can be counteracted (Peltier, 2016). According to both practitioners and scholars alike, the information security policy (InfoSec policy) is central to the organization's effort to secure their information assets (Niemimaa, 2017). The InfoSec policy is essentially a direction-giving document that defines the broad boundaries of information security in an organization (Höne & Eloff, 2002b), and supports information security in accordance with business requirements, laws, and regulations (ISO/IEC 27001, 2013).

To work with information security systematically, an information security management system (ISMS), such as the ISO/IEC 27000 series, can be implemented. An important part of an ISMS is asset management, that includes the identification, and valuation of all information in an organization, and defines appropriate protection responsibilities (ISO/IEC 27002, 2013). One of the core activities in asset management is information classification, that has the objective to: "ensure that information receives an appropriate level of protection in accordance with its importance to the organization" ISO/IEC 27002 (2013, p. 15). Information classification values information by assigning a classification value to the information from a confidentiality, integrity and availability perspective. The value, in turn, tells how the information can be handled, stored, processed and communicated, and also serve as input to the risk analysis (Everett, 2011; ISO/IEC 27002, 2013).

It might sound like an easy task to value the information, but investigations into the matter show another picture. The Global Databerg Report looking at practices in 22 countries concluded that 52% of organization's information is dark data where the value has not been identified (Veritas Technologies, 2016). A Forrester report showed that security and risk professionals overlook the information

classification activity (Kindervag, Shey, & Mak, 2015), and a large survey in the UK showed that only 46% of firms covered classification in their security policies (Department for Culture, 2016). Despite the widespread adoption of information classification, the field is under-researched (Oscarson & Karlsson, 2009), and little is known about information classification practices in organizations.

An InfoSec policy either contains both the security objectives and the means and methods required to fulfill the objectives (Karyda, Kiountouzis, & Kokolakis, 2005), or the means and methods are described in lowerlevel policies (Baskerville & Siponen, 2002). In the case of information classification, the InfoSec policy can describe what should be performed, but how it is achieved in the organization can be expressed in an information classification policy (Cosic & Boban, 2010).

When looking at InfoSec policies, most literature is concerned with the questions what, and not how it is accomplished in a context (Niemimaa, 2017). This is important since there is a gap between standard and practice that affects the implementation of such policies. In order to shed light on how policies are accomplished in a particular context, this work selected Swedish government agencies as a target study group. We investigate the prevalence of information classification policies if they follow the national support documentation and the perceived ease of turning the standard into practice. The data collected consisted of responses to a questionnaire sent to 245 Swedish government agencies and information classification security policies used by them. This data was analyzed quantitatively and qualitatively. The results show that adoption rates are low and that the agencies are struggling with implementing information classification. The majority of the investigated agencies have made modifications that deviates from the national support documentation to simplify the implementation which signals that the support is not sufficient in filling the gap between standard and practice.

The remainder of the paper is structured as follows: the next section introduces the background on primarily InfoSec policies, information classification, and information classification policies. This is followed by the research approach and the results. Finally, the results are discussed, and followed by the conclusions and future work.

Study background and motivation

This section introduces the background on InfoSec policies, issues in information classification, and information classification policies.

InfoSec policies

Both researchers and practitioners agree that InfoSec policies are important, and even considered a key mechanism in information security (Doherty, Anastasakis, & Fulford, 2009; von Solms & von Solms, 2004), and most organizations have implemented some kind of InfoSec policy in their organization (Goel & Chengalur-Smith, 2010). Studies on policies are limited, and in a large survey by Siponen, Willison, and Baskerville (2008), only 1.64% of the investigated 1280 papers were about security policies. Nevertheless, InfoSec policies have been studied from several perspectives, such as the structure of the policy (Baskerville & Siponen, 2002; Warkentin & Johnston, 2008), the content (Höne & Eloff, 2002a), how policies are developed (Niemimaa, 2017), and the compliance of the policy (Herath & Rao, 2009; Siponen, Adam Mahmood, & Pahnila, 2014).

InfoSec policies differ greatly between organizations depending on the value and sensitivity of what needs to be protected, and the potential implications of the damage, modification, and disclosure of the information (Landoll, 2016). Because of the differences in the context of the usage of the InfoSec policy, the literature uses several definitions of what an InfoSec policy should contain (Cram, Proudfoot, & D'Arcy, 2017). One widely used classification of InfoSec policies have been proposed by Baskerville and Siponen (2002) that divides them into three levels: (1) a high-level overall organizational policy, (2) lower-level policies regulating selected information security methods, and (3) a meta-policy describing how policies are created, implemented and enforced. In this work, the term policy is used to describe the direction-giving document regardless of level, but it can be noted that it differs in the literature. For example, Warkentin and Johnston (2008) use the terms policy, procedure, and practice. Landoll (2016)

uses four levels of policies that tie in with standards and frameworks such as ISO/IEC 27001 (2013) and the Federal Information Security Management Act (FISMA); (1) organizational level, (2) security program level, (3) user level, and (4) system and control level. From these classifications of levels of policies, we can derive that regardless of viewpoint, information classification is a part of the organization-wide high-level policy, in a sense that it outlines what should be classified, and according to what classification scheme. This is important so that information is treated similarly, and so that classifications are consistent within the organization. On a lower level is the method or procedure for how to perform the classification. In the case of information classification, the information classification policy could be seen as a procedure that is turned into practice when it is operationalized. In practice, the classification scheme is included and explained in a lower-level policy detailing the how's. Finally, it can be pointed out that the lower-level policies can also assume different names, and be called guideline, policy, procedure or have other practicerelated names, but in this work we choose to call it information classification policy, as this term is the most commonly used one in the literature.

Information classification

Many organizations are struggling in performing information classification, but no coherent view on such causes appear in the literature. A large literature study on information classification issues (Bergström & Åhlfeldt, 2014) gave a scattered view, with issues, e.g. related to the ones performing classification, such as subjective judgement (Glynn, 2011; Kaarst-Brown & Thompson, 2015), and management issues, such as the lack of authority in leaders (Collette, 2006). The largest number of issues were, however, policy-related, and issues include the process of developing the classifications (Baškarada, 2009), and that the standards are too generic to cover characteristics for many organizations (Bayuk, 2010). Authors also describe a situation where the development of an information classification policy that covers organizational requirements but still provides flexibility without being too cumbersome is difficult (Ghernaouti-Helie, Simms, & Tashi, 2011). This balance between details in the classification policy and the organizational practices easily leads to a situation where classification is considered difficult because of it does not fulfill organizational needs (Saxby, 2008).

Information classification is normally performed using a classification scheme, containing a number of levels describing the consequence of a loss of, e.g., confidentiality integrity and availability. In the beginning, information classification practices were used in the military sector, where it was used to classify information on paper, e.g., by labeling documents with top secret, secret, and unclassified from a confidentiality perspective. Today, it applies to all kinds of information, including electronically stored, processed or transmitted information, and not the only from a confidentiality perspective, but also integrity and availability should be considered (ISO/IEC 27002, 2013). In this context, is important to mention that information classification is sometimes referred to as security classification or data classification, and these concepts are sometimes treated as overlapping or separated in literature depending on context. Information, data and security classification aims at protecting information against security breaches, but generally, security classification refers to information where a loss affects the national security. Hence, there is more focus on the confidentiality aspect in security classifications (Gantz & Philpott, 2013). Also, information classification is considered a group activity, as opposed to security classification that is more of a one-man-show (Axelrod, Bayuk, & Schutzer, 2009). Research on classification in other organizations than the ones handling information critical to national security is virtually non-existent (Thompson & Kaarst-Brown, 2005). This was also the conclusion of a study trying to identify information classification practices online (Mikkelinen, 2015).

Information classification is a mandatory activity for government agencies in many countries, such as in the UK (Cabinet Office, 2013), Australia (Australian Government, 2014), and Sweden (MSBFS 2016:1, 2016). It is also well-established in the private sector due to legal requirements, e.g., for protecting personally identifiable information (Raman, Beets, & Kabay, 2014), or to be eligible to be a sub-contractor to the government (Cabinet Office, 2013). Hence, the public sector can be seen as a driver for the implementation of information classification, and with the introduction of EU's General Data Protection Regulation (GDPR) in 2018, information classification is expected to gain further momentum as organizations need to identify and value their information to avoid breaches and large fines (MansfieldDevine, 2016).

Surveys, where information classification is mentioned, normally has a broader scope than just information classification, e.g., covering the whole ISMS, and thereby missing out on many important aspects from an information classification perspective. For example, a large survey on cybersecurity breaches in the UK with more than 1000 respondents reported that only 58% of large firms, and 46% of firms overall covered information classification in their InfoSec policies (Department for Culture, 2016), but it is, e.g., unclear if these firms, rely on the InfoSec policy for classification or if other policies are available. Information classification in Swedish public sector has also been investigated, and in 2014, 43% of the government agencies used information classification, and another 24% were working on implementing it (Swedish Civil Contingencies Agency, 2014). In Swedish municipalities, only 75 of 241 municipalities that answered an information security survey (there are 290 municipalities in total) used information classification, but only ten did it on a regular basis (Swedish Civil Contingencies Agency, 2015). The survey also showed varying responsibility for classifications, and that 58% of the municipalities did not use a specific method (Swedish Civil Contingencies Agency, 2015).

A fundamental problem for organizations is how to share information with others because the classification scheme itself only states how valuable the information is to the own organization, based on the own organization's needs, but not how it is protected. Cherdantseva and Hilton (2013) describes this situation, and argues for consensus use of classification schemes, but recognize that it is hard to achieve, and also that ultimately it does not imply the same level of protection. Niemimaa (2016) shows in her study that information classification was seen as an internal concern and was never discussed within in the investigated organizations network, and their information classification policies were not aligned. This is especially problematic as organizations are increasingly dependent on other organizations for value creation (Partanen & Möller, 2012). This problem is reduced where national initiatives regulate the classification schemes such as in, e.g., the UK (Cabinet Office, 2013), and the US (Gikas, 2010). However, in, e.g., Sweden, the decentralized approach, where government agencies are more independent lead to a situation where information sharing between them become limited which, e.g., inhibits the fight against serious organized crime (Swedish Government Official Reports Series, 2011). Incompatible information classification schemes relate to several aspects of classification, from the language used in the scheme (Oscarson & Karlsson, 2009), which security aspects, such as the CIA triad, are used, and how many levels the scheme consist of. There are also initiatives for synchronizing the protection of information sent between organizational borders, e.g., by using the Information Sharing Traffic Light Protocol (ISTLP) that has been developed to share information between different countries Computer Emergency Response Teams (ENISA, 2013). However, little is known about how organizations develop their internal policies based on standards, and how sharing with incompatible classification schemes are performed in practice. Niemimaa and Niemimaa (2017) studied the crafting of an information classification policy in an ethnographic study, but the focus was on one organization, and how the policy became rather than the content of the policy which is in focus here.

Finally, the responsibility for information classification is another issue described in the literature. The recommendations given in ISO/IEC 27002 (2013) are that the information owners should be responsible for information classification. A similar recommendation is given in the Swedish support documentation developed by the Swedish Civil Contingencies Agency (Andersson et al., 2011) that is based on ISO/IEC 27002 (2013), with the aim of alleviating implementation in organizations. Many times information classification is owned by senior executives, and the task to perform the classification is delegated to, e.g., the information owners. It can, however, be hard to get acceptance from all to drive the implementation of a classification scheme in an organization (Collette, 2006), and to clearly define the ownership (Janczewski & Xinli Shi, 2002).

Information classification policies

There are a number of studies on InfoSec policies in different sectors, e.g., Stahl, Doherty, and Shaw (2012) investigated the role and purpose of InfoSec policies through a critical theoretical lens on 25 publicly available policies in the UK healthcare sector. However, when looking at lower-level policies, we have been unable to find any specifically investigating information classification policies. There are studies targeting other lower-level policies, for example, Goel and Chengalur-Smith (2010) have done a study on metrics in US university email policies.

Sweden differs from most other countries in the organization of government agencies. The ministries (or government departments) are headed by a minister and are divided into government agencies (or bureaus or offices) that handle a specific sector of public administration. The difference is that in Sweden, the government agencies are not a part of a department like most other countries, but independent. Ministers in Sweden are not allowed to decide on activities in the government agencies directly, so this kind of decisions must be made by the government instead. In practice, this entails a larger degree of autonomy for the agencies, with a lesser degree of central control. This has practical implications, e.g., for ISM as it is recommended that all agencies follow ISO/IEC 27001, and ISO/IEC 27002, and hence thereby implement information classification (MSBFS 2016:1, 2016), but not specify exactly how to do so. In other words, it is up to the individual agency to select their approach including the classification scheme as long as they classify the information. This has led to proliferation, and many agencies have developed their practice based on ISO/IEC 27002 and complementary documentation developed to support the implementation of ISO/IEC 27002 (Andersson et al., 2011). In combination with the principle of public access to official records, Swedish government agencies make good study objects as they represent a wide range of functions critical for society, but also with a wide array of practices for information classification.

It is important to recognize that ISMS and the methods used as a part of the ISMS are based on best practices (Niemimaa & Niemimaa, 2017), and organizations face institutional pressures to adopt such practices (Hsu, Lee, & Straub, 2012). This pressure to comply comes from, e.g., legislation, as in Japan, where ISO/IEC 27001 is mandated for many government contracts (Gillies, 2011). However, turning standards into practice is easier said than done, and many scholars have recognized a gap between formal and actual processes in information security management (Njenga & Brown, 2012; Shedden, Smith, & Ahmad, 2010; Siponen, 2006; Taylor & Brice, 2012). Nevertheless, the gap between standard, and practice in the area of information classification has not attracted much attention from scholars. One notable work is from Niemimaa and Niemimaa (2017), that studied the translation from best practice on information classification into local policy and how that was turned into practice at an organization. This study found that the best practice prescriptions were insufficient for local action and that they offered a plan that fell short because of the complexity of actual organizational life (Niemimaa & Niemimaa, 2017). Not much other insight on the perceived ease in which standards are transformed into practice in the area of information classification exist, as existing research is more focused on the classification itself, and how it is performed, rather than how it is implemented, and what challenges lie therein.

Research approach

In this section, the research objectives are introduced, followed by the study design where it is described how the data was collected. Finally, how the analysis was performed is presented.

Research objectives

The research objectives are based on the background information introduced in the previous section. The research objectives are divided into areas, where one area has the objective to investigate the prevalence of documented information classification policies in governmental Sweden. The second area investigates aspects of the information classification policies, and the last area has the objective to investigate the perceived ease of turning the standard into practice.
The research objectives have been formulated as to:

- Investigate the prevalence of documented information classification policies in Swedish government agencies.
- Provide a characterization of information classification policies in Swedish government agencies based on:
    - what role(s) are responsible for information classification,
    - when the classification is performed, and
    - what standard or approach the information classification method is based on.
- Identify factors that impact the perceived ease of turning the information classification policy into practice.

Study design

To answer the research objectives posed, a survey was designed. Survey was chosen as a method for collecting data as it supports collection from a large group in a systematic and standardized way (Oates, 2006). A questionnaire was sent out using email, and recommendations from Bryman and Bell (2011) for email questionnaires was followed to increase the answering frequency. The email avoided including attachments and was written in plain text to allow for easy forwarding and replying as it was sent to the registered address of each agency included in the study. The email contained a brief introduction stating it was a research project, and that information classification was the focus. Furthermore, a brief description that the ISO/IEC 27000 standards are vague in describing information classification followed, and that we aimed to collect best practices from Swedish government agencies. Additionally, it was mentioned that the questionnaire contained six sections and that it would take approximately 15-20 minutes to answer the questions. Furthermore, it was stated that the results would be presented anonymously, and a request to send their internal information classification policy and their internal information classification scheme for analysis. Finally, one of the authors signed as responsible for the data collection with contact information. From a methodological viewpoint, it could be argued that there are other ways of collecting the data, e.g., via telephone interviews or a web survey. The main reasons for choosing email is that it allows for longer answering times than telephone, and an email is easy to forward in the organization as a mean for finding someone that can answer the questions. Furthermore, attaching a document to an email is potentially easier than uploading them to a website.

The questions started with a demographic section regarding the number of employees classified into small (0-50 employees), medium (51-500 employees), and large (501 or more employees) as this value can be difficult to find. Other demographic information such as sector and responsible ministry are easier to find so to decrease the size of the survey only one question was included in this part.

The other five sections each targeted one of the research objectives and were composed of one main question that depending on the answer was followed up with additional questions. The follow-up questions asked to explicate the answers to avoid short answers such as yes and no to provide a rich dataset.

There are currently 442 government agencies in Sweden (Statistics Sweden, 2018), but of which 245 were included in this work. The excluded agencies are primarily embassies, consulates, and Swedish courts as they represent two categories of agencies with similar functions and interests. The included agencies represent a wide range of functions for the society, including, e.g., the Armed Forces, the Tax Agency, the Police, the Pensions Agency, and the Transport Administration. Many of the included agencies handle systems and information that are critical to society, but most of them handle little or no information that could be expected to cause exceptionally grave damage to national interests.

The questionnaire and request for their internal policies were sent via email to the registered email address of each agency. In practice, this was done by downloading the registry for government agencies at Statistics Sweden (Statistics Sweden, 2018), and with the use of the function mail merge, an individual email was sent to the respective agency automatically. The emails were sent from a personal address, allowing for us to reply to partial answers, and for initiating dialogue where needed. Mail merge was used again to automate the reminders by subtracting the agencies that had already replied from the registry.

In Sweden, the transparency in access to information is central to the public and media, and the principles are regulated in the Public Access to Information and Secrecy Act (Regeringskansliet, 2009). According to the principles, government agencies are required to reply to requests promptly, at least with an acknowledgment if it takes some time to reply to the request. As the questions are in the area of information security, some agencies preferred not to participate or send their internal policies. A policy on information classification could be considered not to contain any secrecies, and the information in it should be public. However, as many policies that were already sent to us contained mappings between information classification levels and named systems, handling routines and other types of information that from a secrecy perspective could be seen as they are in a grey area concerning whether it is public

information or not, the decision was taken to not escalate the communication with the agencies that denied access.

In total, four requests for the information were sent out, over a period of one year to allow long answering times. Some of the agencies were in the process of deciding their policies and needed some months to get them formally decided. A decision was taken to wait and include them to get a higher answering frequency. Furthermore, since the requests were sent to the registered email address of the respective agencies, but the respondents in most cases were inside the organization some time to circulate the request, and to find the correct respondent was included in the time between the reminders. Mainly senior information security roles, such as CISO, CSO or CIO answered the request.

Despite the fact that nine agencies denied the request, the vast majority of the feedback from the agencies were positive, and several of them expressed that they would like to take part of the results.

Analysis

The data collected from the survey were both quantitative and qualitative. The questions that were possible to quantify were quantified and compiled give a better representation of the overall picture of the results and give a better understanding of the distribution of the answers. The qualitative answers in the survey were compiled and complemented with a separate analysis of data extracted from the collected internal information classification guidelines. In practice, a large spreadsheet was created where all answers from the survey were inserted. This spreadsheet was then complemented with extracts from the collected policies. For each of the research objectives, one separate spreadsheet was created. In each of these spreadsheets, the results were coded with open coding following the recommendations from Strauss and Corbin (1998) to find, e.g., similarities and differences. This led to an initial categorization with a high granularity of the results that were thematically coded into lists of known or anticipated themes depending on question following the recommendations from Ayres (2008).

Research findings

The findings are presented according to the objectives formulated in the previous section.

The prevalence of documented information classification policies

When the first request was sent out, there were 245 government agencies that received a request to answer the survey. 217 agencies (~89%) replied to the survey, but of these 217 agencies, 28 replied they lack administrative responsibility or have zero employees and that they are subordinated another agency, and in practice follow their regulations. In total only nine out of the 245 government agencies denied the request. One of the replies that can be seen as a typical answer from this category was: "*several of the questions that have been asked is deemed as covered by secrecy. Hence, we will not answer the questionnaire*" (A large government agency under the Ministry of Defence). In total, 178 (~73%) government agencies have actively participated in the study after the fourth and final reminder.

Even though there is a mandate to implement information classification in all government agencies, all have not yet been able to implement it yet. Of the 178 participating agencies, 103 (~58%) replied they are using information classification, while 75 replied they are not using information classification or that they are in the process of implementing it. This is in line with a previous study performed by Swedish Civil Contingencies Agency (2014) where 43% of the agencies responded they are performing classification, and another 24% were in the process of establishing or approving the implementation. Of the 103 agencies, 82 (~80%) sent their internal information classification policy, InfoSec policy or other documents related to information classification, totaling 122 documents consisting of 1024 pages. The information classification policies received were in some cases complemented with the overall InfoSec policy for coherency, as they contained references, but the vast majority only sent their information classification policy.

Responsibility for information classification

To investigate the responsibility for information classification, open questions were formulated to ask if it is specified who is responsible, and if so, which role(s). The answers were also extracted from the policies sent by most of the agencies.

In total, 97 agencies replied they had specified a responsible, 50 stated that they had not decided any responsibility, and 6 gave a non-definitive answer. Among the agencies answering that they have not decided responsibility, the absolute majority have not done so because they do not do information classification or are in the process of implementing it. However, there are eight agencies that claim to use information classification but lack a designated responsible. Reasons given include, e.g., that a role as responsible for information security exists, but information classification is not mentioned specifically or that it is not specified in their policy.

The reason for classifying six agencies as to have a non-definitive answer is that they said they had some responsibility, e.g., some role or indirect roles, not covering the whole agency or only for some types of system or information. A typical answer from this category is: "*Maybe not clear. I [Chief Information Officer] am responsible for information security, including information classification, but the respective system owners are responsible for risk analysis and information classification of their systems. The question is how aware they are about it…"* (A large government agency under the Ministry of Health and Social Affairs).

Among the agencies that had designated responsibility to a specific role, the responsibility differs significantly. When investigating the result, five groups of responsibility can be determined. The largest group of 26 agencies follows the recommendations in ISO/IEC 27002 (2013) or a variant of it. They claim that the responsibility for classification is the information/system/process/object owner. 23 agencies put the responsibility clearly in the line organization, either at the highest management level or in the middle management. Variants of roles that were named include; Chief Information/Security Officer, Head of Communications, and Administrative Director. In 12 of the agencies, a shared approach to responsibility was taken. Either the responsibility was shared among several different roles within the same organization, or it was clarified that the formal responsibility is in the line organization, but in practice, it is delegated to, e.g., information owners. Eight of the agencies claim that the responsibility to classify is delegated to all employees, or to all employees that create or handle information. Finally, the last group could be considered other responses than the groups described above. Most common in this group is to assign the responsibility to the archivist, but also, e.g., the IT department was mentioned.

When classification is performed

Open questions were formulated to investigate when the classification is performed in the agencies. The questions asked if it is clarified when information classification should be made and when re-classification should take place, and how they have reasoned around this.

In total, of the agencies answering this question (n=80), 39 agencies state that they have clarified when information classification should take place, and 41 have not done so. Among the agencies that had not clarified when, the majority did not answer why, but around 10 of the agencies are in the process of deciding or are in a pre-study aiming at deciding.

Among the agencies that do have clarified, there are some themes that can be identified. Firstly, all of them have decided when information classification should be performed, but a number of them have not decided when re-classification should be performed. When viewing only on when information classification should be performed there are some differences between the agencies. There is one group that details that classification should be performed when a new system is introduced or procured, while the other group has an ambition that all information should be classified when it is created or sent to the agency. This difference can largely be explained by different approaches to information classification. Several of the agencies do not do any classification at all on the information, but rather on a system level,

i.e., to classify what kind of information that exists, and potentially could exist in the systems. The other alternative is to classify all incoming or created information regardless of system.

For re-classification, variations of the following reasons are given as triggers: when a system is changed, upgraded, developed, integrated or retired, or revisions that are time-bound, e.g., annually or biannually, when new types of information are introduced or removed, when there are changed organizational practices, changed legal requirements, changes in threats or risks or severe incidents. For re-classification there are also some that use vague descriptions, e.g. that it is "*also every employee's responsibility to make a new classification of information if its value has changed*" (A large government agency under the Ministry of Justice), and that re-classification "can also be done when necessary" (A large government agency under the Ministry for Rural Affairs).

What standard or approach the information classification method is based on

A fundamental aspect of information is the ability to share it and to be able to do that; standardized information classification schemes are one piece of the puzzle, especially in a government agency context as they should be natural information exchangers. One open question targeting this was asked, and 100 of the 103 agencies that have adopted information classification answered the question. The majority, 76 of the agencies have based their classification model on the model developed by Andersson et al. (2011), that in turn is based on ISO/IEC 27002 (2013). 14 agencies have developed their own classification model. Six agencies follow the regulation RA-FS 2008:4 issued by the Swedish National Archives (2008). Four of the agencies under the Ministry of Defence follow the regulation FFS 2003:7 (Swedish Armed Forces, 2003), which handles information critical to society and presents a classification scheme complete with handling routines.

Among the agencies developing their own model, there are references to following ISO/IEC 27001 (2013), ISO/IEC 27002 (2013), models developed by private companies, and models inspired by universities in the US and UK. There is no common denominator among these agencies, and they represent a wide range of functions for society.

The agencies following the regulation RA-FS 2008:4 are not in any particular sector, and it is interesting to note that the regulation is only partly about classification, but mainly about archiving practices for government agencies.

Factors that impact the perceived ease of turning the policy into practice

There were 73 answers to this open question, varying from just one word as an answer to longer descriptions. To present the results, classifications into three categories; easy, moderate and hard were made. The results show that 28 government agencies perceived it as easy, 30 as a moderate, and eight as hard. Seven government agencies were in the process of implementing information classification, and could not evaluate it yet.

Several of the agencies expressed that information classification in itself is an easy task to perform and that the issue lies in identifying the information that is to be classified, due to e.g., complex systems, what delimitations to make, if the information has many user groups both externally, and internally, and in systems where parts of the systems are outsourced. A typical answer in this category came from a large agency under the Ministry of Education and Research: "*The model [for information classification] is not complicated. To judge WHAT should be classified is harder*".

Furthermore, several agencies raise the issue of subjective judgment, i.e., that different groups classify the same or similar information differently, and, e.g., one of the agencies said *"[t]o classify is a "judgment sport." It requires coordination to get it done as similarly as possible in different parts of the organization*" (A large government agency under the Ministry of Health and Social Affairs). There are several mentioning the importance of pedagogical support in explaining and clarifying how to perform information classification, and several have developed additional supporting material beyond the

information classification policy to educate staff subjected to information classification. Related to subjective judgment is also the understanding of the information classification scheme, and several aspects of it emerged. Some argue it is even hard to understand the fundamental concepts, such as confidentiality, integrity, and availability, and to separate them from each other. Also, some of the agencies use a tighter connection between the information classification scheme, and the security controls so that a level of consequence in the classification scheme is met by requirements on the security controls. This, in turn, creates a problem for some in understanding the security control requirements, and to questions whether or not they fulfill the requirements of these controls.

Also, the need for tools supporting the management and reporting of information classification was mentioned as problematic, especially since there are no tools recommended. Finally, it is also expressed that there is too little support from the supporting documentation, a lack of good examples that could be applicable for organizations, and there is a lack of templates for organizations to adopt.

Discussion

In total, 178 government agencies participated in the study, and it was found that 58% of them use information classification. Of the agencies classifying information, 80% sent their internal information guidelines for analysis, which is indeed a high value, especially considering previous studies' struggle to obtain examples of information classification policies.

One reason for organizations struggling with information classification comes from not knowing when to perform classification or re-classification. This issue is complicated by the fact that information can change value over time, and that there are not any mechanisms for detecting this automatically. In the light of the found weaknesses in assigning responsibility for classification, or by putting it in the line organization can create a situation where the responsibility exists, but classification does not happen. The top management support is a key enabler for information classification (Ku, Chang, & Yen, 2009), but the results show that more is needed.

It is hard to assess the perceived ease of use quantitatively, and the classification into easy, moderate and hard should be seen as an indication that more than half of the agencies experience difficulties. The qualitative answers digging into the causes are more interesting and reveal that classification in itself is an easy concept, but a lack in conveying the how's from a standard or national recommendation perspective makes it difficult for organizations to adopt them. The results presented in this paper coincide and support the work performed by, e.g., Siponen (2006), and Niemimaa (2017) where it has been concluded that standards give little support on how to turn them into practice. This study shows, additionally, that even if there is national support documentation supporting the implementation of the standard, it is hard to turn information classification into organizational practice.

Standards like ISO/IEC 27002 (2013) assume that information classification is similar to security classification which is problematic considering that many organizations use practice described by, e.g., Fibikova and Müller (2011), and Collette (2006), where applications or systems are classified rather than the information in them. More research on how to realize these approaches are needed as they provide a viable way for organizations to decrease the classification burden potentially.

The dataset collected during this work is rich, and especially, the internal policies contain many other aspects that could be investigated further. Some of such aspects overlooked in literature are, for instance, the relation between information classification and information life-cycle management that is emphasized in, e.g., ISO/IEC 27002 (2013); nevertheless, little is known on how this can be achieved in practice (AlFedaghi, 2008). Other aspects are, e.g., how levels of consequence are mapped against security controls and how application-oriented classification (Fibikova & Müller, 2011) is performed in practice and the implications of using this approach.

Conclusions and future work

The purpose of this study has been to investigate information classification policies from several aspects. A broad study targeting Swedish government agencies was set up to investigate what underlying approaches practices are built on, in what way practices differ from the national support documentation and the perceived ease of turning policies into practice. To the best of our knowledge, this is the first broad study into information classification policies in the field.

The study shows that the adoption rates among Swedish government agencies are low, especially considering that it is mandatory. The classification practices differ greatly between agencies, which should affect the ability to share information between them, and protect received shared information as originally intended.

Moreover, the results indicate that the transition from standard into practice has been difficult for the investigated organizations, and a majority are struggling with information classification. This conclusion is strengthened by a number of scandals concerning classified information in Sweden in the recent years. For example, in 2017, the leakage of millions of personal records and data about the infrastructure of Sweden was exposed (Anderson, 2017). The data came from the Swedish Transport Agency, and lead to costing the job of both the general director and ministers in the Swedish government.

It is well-described in the literature that standards offer little support in how a policy is accomplished in practice, but in the end, that is what organizations need to do. Where national support, sectorial recommendations or other support or best practices exist with the aim of closing the gap between standard and practice it is important to consider being more specific and give more actionable advice regarding; explaining the steps performed in a classification, which competencies are needed, how to include information life-cycle management in practice, establish clearer responsibilities, and more clearly convey how the security aspects are used. Furthermore, if more examples, templates, and tools could be provided, better information sharing and coherence between organizations could be enabled. These recommendations should be seen as recommendations for any organization, public or private alike, trying to formulate an information classification policy.

The study does not answer all reasons why there are certain differences between agencies or why decisions have been made regarding certain choices. Even the combination of the survey answers and the information classification policies leave some gaps, and from a methodological viewpoint, new insight in the field of information classification policies can be obtained if, e.g., longitudinal follow-up studies are carried out. Additional knowledge into why practices have turned out in a certain way might be obtained through followup interviews with staff that implements and uses classification, especially since most of the answers in this work came from management roles responsible for classification.

The collected data could be analyzed in other ways, e.g., by using the critical lens used by (Stahl et al., 2012) to review the truthfulness, clarity, legitimacy, and sincerity to find additional advice for policy developers. This work also slightly tackles the area of compliance, not only regarding organizations following regulations but also when the policy is turned into practice. Some aspects could be investigated further from a compliance perspective, e.g., the underlying reasons why there are not compliance, intentions, and motivations behind it.

Finally, the authors welcome more studies on information classification practices from, e.g., other parts of the world, and the private sector as there are still many facets of information classification that need to be investigated more in-depth.

References

Al-Fedaghi, S. (2008). On Information Lifecycle Management. Paper presented at the Asia-Pacific Services Computing Conference, 2008. APSCC '08. IEEE.

Anderson, C. (2017). Swedish Government Scrambles to Contain Damage From Data Breach. Retrieved from https://www.nytimes.com/2017/07/25/world/europe/ibm-sweden-data-outsourcing.html

Andersson, H., Andersson, J.-O., Björck, F., Eriksson, M., Eriksson, R., Lundberg, R., . . . Starkerud, K. (2011). Verksamhetsanalys. Myndigheten för samhällsskydd och beredskap.

Australian Government. (2014). Information security management guidelines – Australian Government security classification system Version 2.2. Attorney-General's Department, Retrieved from https://www.protectivesecurity.gov.au/informationsecurity/Documents/INFOSECGuidelinesAustralianGovernmentSecurityClassificationSystem.pdf.

Axelrod, C. W., Bayuk, J. L., & Schutzer, D. (2009). Enterprise Information Security and Privacy: Artech House.

Ayres, L. (2008). Thematic coding and analysis. The Sage encyclopedia of qualitative research methods, 868-869.

Baškarada, S. (2009). Analysis of Data. In Information Quality Management Capability Maturity Model (pp. 139-221): Vieweg+Teubner.

Baskerville, R., & Siponen, M. (2002). An information security meta - policy for emergent organizations. Logistics Information Management, 15(5/6), 337-346. doi:10.1108/09576050210447019

Bayuk, J. (2010). The utility of security standards. Paper presented at the 2010 IEEE International Carnahan Conference on Security Technology (ICCST).

Bergström, E., & Åhlfeldt, R.-M. (2014). Information Classification Issues. In K. Bernsmed & S. FischerHübner (Eds.), Secure IT Systems (pp. 27-41): Springer International Publishing.

Bryman, A., & Bell, E. (2011). Business Research Methods (3rd edition ed.): Oxford University Press, USA.

Cabinet Office. (2013). Government Security Classifications April 2014 Version 1.0 – October 2013. Cabinet Office, Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251480/Government-Security-Classifications-April-2014.pdf.

Cherdantseva, Y., & Hilton, J. (2013, 2-6 Sept. 2013). A Reference Model of Information Assurance & Security. Paper presented at the Availability, Reliability and Security (ARES), 2013 Eighth International Conference on.

Collette, R. (2006). Overcoming obstacles to data classification [information security]. Computer Economics Report (International Edition), 28(4), 8-11.

Cosic, Z., & Boban, M. (2010, 10-11 Sept. 2010). Information security management - Defining approaches to Information Security policies in ISMS. Paper presented at the IEEE 8th International Symposium on Intelligent Systems and Informatics.

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

Department for Culture, Media & Sport,. (2016). Cyber Security Breaches Survey 2016 Main Report. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/521465/Cyber_Security_Breaches_Survey_2016_main_report_FINAL.pdf

Doherty, N. F., Anastasakis, L., & Fulford, H. (2009). The information security policy unpacked: A critical study of the content of university policies. International Journal of Information Management, 29(6), 449-457. doi:http://dx.doi.org/10.1016/j.ijinfomgt.2009.05.003

ENISA. (2013). Security certification practice in the EU: Information Security Management Systems - A case study, v.1, October 2013. Retrieved from https://www.enisa.europa.eu/publications/securitycertification-practice-in-the-eu-information-security-management-systems-a-casestudy/at_download/fullReport

Everett, C. (2011). Building solid foundations: the case for data classification. Computer Fraud & Security, 2011(6), 5-8. doi:http://dx.doi.org/10.1016/S1361-3723(11)70060-4

Fibikova, L., & Müller, R. (2011). A Simplified Approach for Classifying Applications. In N. R. Pohlmann, Helmut; Schneider, Wolfgang (Ed.), ISSE 2010 Securing Electronic Business Processes (pp. 3949): Vieweg+Teubner.

Gantz, S. D., & Philpott, D. R. (2013). Chapter 2 - Federal Information Security Fundamentals. In S. D. P. Gantz, Daniel R. (Ed.), FISMA and the Risk Management Framework (pp. 23-52): Syngress.

Ghernaouti-Helie, S., Simms, D., & Tashi, I. (2011). Protecting Information in a Connected World: A Question of Security and of Confidence in Security. Paper presented at the 14th International Conference on Network-Based Information Systems (NBiS).

Gikas, C. (2010). A General Comparison of FISMA, HIPAA, ISO 27000 and PCI-DSS Standards. Information Security Journal: A Global Perspective, 19(3), 132-141. doi:10.1080/19393551003657019

Gillies, A. (2011). Improving the quality of information security management systems with ISO27000. The TQM Journal, 23(4), 367-376. doi:doi:10.1108/17542731111139455

Glynn, S. (2011). Getting To Grips With Data Classification. Database and Network Journal, 41(1), 8-9.

Goel, S., & Chengalur-Smith, I. N. (2010). Metrics for characterizing the form of security policies. The Journal of Strategic Information Systems, 19(4), 281-295. doi:https://doi.org/10.1016/j.jsis.2010.10.002

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems, 47(2), 154-165. doi:https://doi.org/10.1016/j.dss.2009.02.005

Hsu, C., Lee, J.-N., & Straub, D. W. (2012). Institutional Influences on Information Systems Security Innovations. Information Systems Research, 23(3-part-2), 918-939. doi:10.1287/isre.1110.0393

Höne, K., & Eloff, J. H. P. (2002a). Information security policy — what do international information security standards say? Computers & Security, 21(5), 402-409. doi:http://dx.doi.org/10.1016/S01674048(02)00504-7

Höne, K., & Eloff, J. H. P. (2002b). What Makes an Effective Information Security Policy? Network Security, 2002(6), 14-16. doi:https://doi.org/10.1016/S1353-4858(02)06011-7

ISO/IEC 27001. (2013). Information technology – Security techniques – Information security management systems – Requirements. In: ISO/IEC.

ISO/IEC 27002. (2013). Information technology – Security techniques – Code of practice for information security controls. In: ISO/IEC.

Janczewski, L., & Xinli Shi, F. (2002). Development of Information Security Baselines for Healthcare Information Systems in New Zealand. Computers & Security, 21(2), 172-192. doi:http://dx.doi.org/10.1016/S0167-4048(02)00212-2

Kaarst-Brown, M. L., & Thompson, E. D. (2015). Cracks in the Security Foundation: Employee Judgments about Information Sensitivity. Paper presented at the Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research, Newport Beach, California, USA.

Karyda, M., Kiountouzis, E., & Kokolakis, S. (2005). Information systems security policies: a contextual perspective. Computers & Security, 24(3), 246-260. doi:https://doi.org/10.1016/j.cose.2004.08.01

Kindervag, J., Shey, H., & Mak, K. (2015). The Future Of Data Security And Privacy: Growth And Competitive Differentiation. Retrieved from Cambridge, MA.: https://www.forrester.com/report/The+Future+Of+Data+Security+And+Privacy+Growth+And+Competitive+Differentiation/-/E-RES61244

Ku, C.-Y., Chang, Y.-W., & Yen, D. C. (2009). National information security policy and its implementation: A case study in Taiwan. Telecommunications Policy, 33(7), 371-384. doi:http://dx.doi.org/10.1016/j.telpol.2009.03.002

Landoll, D. J. (2016). Information Security Policies, Procedures, and Standards: A Practitioner's Reference. Boca Raton, FL: CRC Press.

Mansfield-Devine, S. (2016). Data classification: keeping track of your most precious asset. Network Security, 2016(12), 10-15. doi:http://dx.doi.org/10.1016/S1353-4858(16)30116-7

Mikkelinen, N. (2015). Analysis of information classification best practices. University of Skövde, Skövde.
Moar, J. (2015). CYBERCRIME AND THE INTERNET OF THREATS. Retrieved from Basingstoke, UK:
Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet, (2016).
Niemimaa, E. (2016). A Practice Lens for Understanding the Organizational and Social Challenges of Information Security Management. Paper presented at the PACIS.
Niemimaa, E. (2017). Crafting Organizational Information Security Policies: Tampere University of Technology.
Niemimaa, E., & Niemimaa, M. (2017). Information systems security policy implementation in practice: from best practices to situated practices. European Journal of Information Systems, 26(1), 1-20. doi:10.1057/s41303-016-0025-y
Njenga, K., & Brown, I. (2012). Conceptualising improvisation in information systems security. European Journal of Information Systems, 21(6), 592-607. doi:10.1057/ejis.2012.3
Oates, B. J. (2006). Researching Information Systems and Computing. London: Sage.
Oscarson, P., & Karlsson, F. (2009). A National Model for Information Classification. Paper presented at the AIS SIGSEC Workshop on Information Security & Privacy (WISP2009), Phoenix, AZ, USA.
Partanen, J., & Möller, K. (2012). How to build a strategic network: A practitioner-oriented process model for the ICT sector. Industrial Marketing Management, 41(3), 481-494. doi:https://doi.org/10.1016/j.indmarman.2011.05.002
Peltier, T. R. (2016). Information Security Policies, Procedures, and Standards: guidelines for effective information security management: CRC Press.
Raman, K., Beets, K., & Kabay, M. E. (2014). Developing Classification Policies for Data Sixth Edition. In Computer Security Handbook (Vol. Vol. 1, pp. 1885-1903): John Wiley & Sons, Inc.
Regeringskansliet. (2009). Public Access to Information and Secrecy Act. Retrieved from Stockholm:
Saxby, S. (2008). News and comment on recent developments from around the world. Computer Law & Security Review, 24(2), 95-110. doi:http://dx.doi.org/10.1016/j.clsr.2008.01.013
Shedden, P., Smith, W., & Ahmad, A. (2010). Information security risk assessment: towards a business practice perspective. Paper presented at the Australian Information Security Management Conference 2010.
Siponen, M. (2006). Information security standards focus on the existence of process, not its content. Commun. ACM, 49(8), 97-100. doi:10.1145/1145287.1145316
Siponen, M., Adam Mahmood, M., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. Information & Management, 51(2), 217-224. doi:https://doi.org/10.1016/j.im.2013.08.006
Siponen, M., Willison, R., & Baskerville, R. (2008). Power and practice in information systems security research. ICIS 2008 Proceedings, 26.
Stahl, B. C., Doherty, N. F., & Shaw, M. (2012). Information security policies in the UK healthcare sector: a critical evaluation. Information Systems Journal, 22(1), 77-94. doi:10.1111/j.13652575.2011.00378.x
Statistics Sweden. (2018). Välkommen till det allmänna myndighetsregistret [Welcome to the public government registry]. Retrieved from http://www.myndighetsregistret.scb.se/Default.aspx
Strauss, A., & Corbin, J. (1998). Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory. Thousand Oaks: Sage Publications, Inc.
Swedish Armed Forces. (2003). Försvarsmaktens föreskrifter om säkerhetsskydd [Armed Forces' Regulations on Security] FFS 2003:7. In. FM LOG/TF-redaktionen, Stockholm: Försvarsmakten.
Swedish Civil Contingencies Agency. (2014). En bild av myndigheternas informationssäkerhetsarbete 2014 – tillämpning av MSB:s föreskrifter [A picture of governmental agencies work with information security 2014 - application of the Swedish Civil Contingencies Agency guidelines] (978-91-7383-478-0). Retrieved from https://www.msb.se/Produkter-tjanster/Publikationer/Publikationer-fran-MSB/En-bild-av-myndigheternasinformationssakerhetsarbete-2014/

Swedish Civil Contingencies Agency. (2015). En bild av kommunernas informationssäkerhetsarbete 2015 [A picture of the municipalities work with information security 2015] (978-91-7383-619-7). Retrieved from https://www.msb.se/RibData/Filer/pdf/27967.pdf

Swedish Government Official Reports Series. (2011). SOU 2011:80 Informationsutbyte vid samarbete mot grov organiserad brottslighet [Information exchange in collaboration against serious organized crime]. Retrieved from http://www.regeringen.se/493fcf/contentassets/ea7da1c1f60f462192da93a831f9785c/informationsutbyte-vid-samverkan-mot-organiserad-brottslighet

Swedish National Archives. (2008). Föreskrifter om ändring i Riksarkivets föreskrifter och allmänna råd (RA-FS 1991:1) om arkiv hos statliga myndigheter [Regulations on amendment to the National Archives regulations and general advice (RA-FS 1991: 1) about archives with government agencies] RA-FS 2008:4. Retrieved from https://riksarkivet.se/rafs?pdf=rafs/RA-FS%20200804.pdf

Taylor, R. G., & Brice, J., Jr. (2012). Fact or fiction? A study of managerial perceptions applied to an analysis of organizational security risk. Journal of Organizational Culture, Communications and Conflict, 16(1).

Thompson, E. D., & Kaarst-Brown, M. L. (2005). Sensitive information: A review and research agenda. Journal of the American Society for Information Science and Technology, 56(3), 245-257. doi:10.1002/asi.20121

Warkentin, M., & Johnston, A. C. (2008). IT governance and organizational design for security management.

Veritas Technologies. (2016). The Databerg Report: See what others don't: Identify the value, risk and cost of your data. Retrieved from http://info.veritas.com/databerg_report von Solms, B., & von Solms, R. (2004). The 10 deadly sins of information security management. Computers & Security, 23(5), 371-376. doi:http://dx.doi.org/10.1016/j.cose.2004.05.002