Information Classification Issues

Erik Bergström and Rose-Mharie Åhlfeldt

Informatics Research Centre
University of Skövde, 541 28 Skövde, Sweden
{erik.bergstrom,rose-mharie.ahlfeldt}@his.se

Abstract. This paper presents an extensive systematic literature review with the aim of identifying and classifying issues in the information classification process. The classification selected uses human and organizational factors for grouping the identified issues. The results reveal that policy-related issues are most commonly described, but not necessarily the most crucial ones. Furthermore, gaps in the research field are identified in order to outline paths for further research.

Keywords: information classification, systematic literature review, information security management systems.

1 Introduction

Information security is achieved by implementing, for example, policies, processes, organizational structures, and technical measures. To control these activities, an Information Security Management System (ISMS) is used. As mentioned in [1], one example of a widespread ISMS is the ISO 27000-series [2], that amongst others offer best-practice recommendations for initiating, implementing and maintaining ISMS. In ISMS, asset management is a central activity since it establishes ownership of all organizational assets. The assets are identified by doing an inventory of all assets such as software, physical assets (for example, computers, and network equipment), services (for example, power, and air-condition), people and their skills and experience, intangibles such as the reputation and image of the organization, and the information in the organization [3]. The information can be found in many places in the organization, and take different shapes. After the inventory, ownership or responsibility is designated to all assets, and guidelines are set up for acceptable use of the assets. The objective of doing information classification is to *"ensure that information receives an appropriate level of protection in accordance with its importance to the organization"* [3 p. 15]. The information classification also serves as a major input for the risk analysis that also need to be performed as a part of the ISMS [1].

The information identified as an asset should be classified according to its value, and criticality to the organization, and be protected accordingly. Normally, a classification scheme uses categories in a hierarchical model, where each category is associated with procedures for how to handle the information, and what protection mechanisms it requires. An organization should not use too many classification categories as

K. Bernsmed and S. Fischer-Hübner (Eds.): NordSec 2014, LNCS 8788, pp. 27–41, 2014.
DOI:10.1007/978-3-319-11599-3_2,

complex schemes may become harder and uneconomic to use, and a typical organization might have between three and five categories in a hierarchy [4]. The probably most well-known information classification scheme comes from the US military, and includes the three levels: top secret, secret and unclassified [5]. In a company setting, the equivalent could be public, proprietary and proprietary restricted [4].

The information classification can also change over time, for example, an annual report from a stock market company contains very sensitive information before it is publicized, but the information classification changes at the point of publication.

In a study by Park, et al. [6], ISMS were investigated in five large hospitals. From a checklist compiled from the complete ISO/IEC 27001 (including, for example, human-resource security, physical security, communications and operation's management, and access control), reveals that asset management in general, and information classifications, in particular, were the most vulnerable part of the ISMS. Problems included lack or weak descriptions of classification guidelines, insufficient inventory of assets, and unclear ownership. Hospitals were also investigated in a study by Luethi and Knolmayer [7], where organizational capabilities such as responsibility for assets and information classification was labelled as they lacked some capabilities. Overall, it was found that organizational rather than technical measures and capabilities were lacking.

Several studies highlights the fact that information classification is not a new concept, but still many organizations struggle to complete their information classification [8-12].

To summarise, it is apparent that there are broad issues with applying a widely accepted technique for valuing and classifying information. The aim of this study is to narrow down and identify the issues that occur when information classification is performed, and provide a comprehensive and structured overview of the problems identified in the research field. The analysis is conducted using a systematic literature review (SLR) that contributes to the field primarily by (1) reviewing and summarizing what is known about the issues in the information classification process, and (2) by offering directions for future research.

In this work, the guidelines of Kitchenham and Charters [13] have been followed to elaborate a research question (RQ).

RQ: *What are the main issues in the information classification process?*

To the best of our knowledge, no literature surveys have focused on identifying the issues in the information classification process. Although information classification is a central, and in many cases, a mandatory activity for many organizations, not much attention has been directed at understanding the underlying issues in the process and how they can be reduced or eliminated. Information classification research in general is limited [1] with few research contributions focusing on the classification process itself. Some notable exceptions are Virtanen [14] that proposes a solution for reclassification where previous data is used to recalculate the classification automatically. An approach with the same intent is presented by DuraiPandian and Chellappan [15] and Hayat, et al. [16]. Several authors [17-20], provide guidelines, frameworks or models

with varying degree of detail for how to classify information. Fernando and Zavarsky [21] propose a categorization with thresholds to enable an organization to handle parts of the information lifecycle such as the disposal of data. Fibikova and Müller [22] describe two alternative approaches to classifying information, a process-oriented approach and an application-oriented approach. Several of the contributions predate the commonly used ISO 27000-series standard where many organizations take their stance from today, but they still contribute to the overall understanding of the information classification process and its related issues. There are also some studies describing how to handle issues in the classification process [10], practical tips for implementing classification [8], and why it needs to be done [23], but it is unclear whether these studies are scientifically verified.

In the following section, the research methodology and the classification factors are explained. In section 3, the classification and analysis of the literature according to the factors are presented. This is followed by section 4 where the results are discussed and section 5 where the conclusions and directions for future research are outlined.

2 Method

The research question will be answered using an SLR following the guidelines from Kitchenham and Charters [13]. SLRs aim to provide a synthesis of the knowledge in an area [24]. The authors are aware of critique against SLRs [25], and acknowledge that the actual search is not the most important step, but the reading and understanding of the area.

Information classification is a term used, for instance, in the ISO 27000 series, and it is a well-established term. However, after surveying a number of publications in research databases and Google Scholar, a number of synonyms were found. The found synonyms to information classification were *"information security classification"*, *"data classification"*, and *"security classification"*. Especially the term *"data classification"* gives many false positives when used as a search string, but the decision was taken to be inclusive and filter manually. The following search query (("security classification" OR "information classification" OR "data classification") AND "information security") was used. The query aims only to limit the classification terms to an *"information security"* context, but otherwise to be inclusive.

The following databases were used for full-text or all-field's searches without any limitations; IEEE Xplore, The ACM Guide to Computing Literature, ScienceDirect (Elsevier), Springer Link and Inspec (Ovid). In total, the searches generated 1545 hits, distributed as shown in Table 1. The reason to choose full-text search and not only search title and abstract were taken after the initial pilot study where initial searches were performed. This initial study revealed several results in publications mentioning information classification where the main focus was something else than information classification. That full-text search makes it more likely to find relevant articles are also consistent with the results from a study performed by Lin [26].

The searches were performed in the weeks of 50-51, 2013, and all results were thereafter downloaded and aggregated into a reference manager. A first rough sorting

was performed by looking at the title, abstract and searches in the full text in order to find out where the word classification was used. Exclusion criteria used in this first sorting was duplicate hits in databases, if the publication were not available, if the same chapter appeared in several books, the result was in another language than English, the search terms only appear in author biography or in the reference list, faulty results as for instance "…information, classification of….", and if the result was in a completely other context than the aim of the study. After this initial sorting, 254 papers remained in focus of the study. Thereafter, a more detailed full-text sorting was performed and where the context was taken into consideration. Then 152 papers remained, and after a final full-text review, 70 papers describing issues with information classification remained.

Table 1. Results of the literature search

Database	Number of results
IEEE Xplore	541
Inspec (Ovid)	42
ScienceDirect (Elsevier)	394
Springer Link	308
The ACM Guide to Computing Literature	290

Kraemer, et al. [27] identify nine thematic categories of human and organizational factors in information security; *external influences, human error, management, organization of CIS* (computer and information security)*, performance management, policy, resource management, technology, training*. The selected factors have been selected as they are broad and inclusive, and should be seen as a starting point for further research. In this work, these factors have been used, but *management* and *organization of CIS* have been merged to one factor, and *training* has been excluded. The merge of *management* and *organization of CIS* was done as a consequence of the results found in the literature study. The mention of management related problems were few, and so intertwined no separation were meaningful. *Training* was removed as a category since none of the papers explicitly mentioned training as a problem but rather as an enabler. When the results were classified into the factors, 18 additional papers were left out of scope as it became apparent that they rather described the consequences of issues with information classification rather than an issue such as for instance over- and underclassification of information as elaborated in section 3.7. In total, 52 papers were classified according to the classification factors.

The analysis performed was descriptive (non-quantitative) as described by Kitchenham and Charters [13], and the analysis used coding techniques as described by Strauss and Corbin [28]. The first step was to use open coding [28] to break down all the data extracted from the literature review into discrete parts to see similarities and differences. The next step was to use axial coding [28] to connect the data to the categories from Kraemer, et al. [27].

3 Classification and Analysis of Literature

The selected literature has been classified according to the factors described by Kraemer, et al. [27]. By categorizing the issues identified in areas, it is possible to better see and understand which factors are the most commonly referred to as problematic. It also serves as a tool for labelling issues that are not necessarily, or naturally referred to as a specific factor explicitly.

In the following sub-sections, we elaborate on the issues found for the respective factors.

3.1 External Influences

Information classification has been around for a long time in the military sector. Several authors believe one of the problems with information classification is its military roots and that the confidentiality model cannot be transferred directly from a military to a corporate setting [5, 19, 29-34]. The underlying reasons for this belief are that it is originally developed as a process for controlling information flow on paper that has moved to electronic ones [9, 35], and that when the business world adopted the process, they only adopted the multilevel concept but not the routines for staff clearance and authorization [19]. In the commercial world, generally different categories for information classification apply, but they tend to not be hierarchical according to Winkler [36].

3.2 Human Error

Humans are many times seen as a weak link when it comes to information security, and when it comes to information classification, these are some human related issues identified. The main problem is that all information in an organization has to be classified, and that all staff in an organization that handles the data or has access to it needs to understand and apply classification. Several authors acknowledge a problem with subjective judgement, including [8, 19, 37-39] and consistency in the classifications [17]. This might be due to too complex schemes [19], schemes that do not fit business people´s needs [33], or a lack of skills [40].

3.3 Management and Organization of CIS

Collette [10] identifies that there is often a lack in the authority of leaders (for example, the chief information security officer) that can drive through a whole classification program from planning to implementation. This can be because of a lack of political power in the organization of information security [10]. There can also be a lack of centralized asset control and a need to better define ownerships and asset responsibilities [41].

3.4 Performance Management

Several issues are related to the information lifecycle management (ILM) in which information is identified and classified after what value the information possesses. The value of information can change over time, and it is possible that cost and resources are wasted if information, for example, is classified as more important than it is. The fundamental problem for an organization is to identify their information capital [35, 39], and decide its value [42, 43]. From an ILM perspective, also information provenance, where the source and modification history of the information is included needs to be considered [44]. The information provenance and preservation or curation of data is important, especially from a governmental viewpoint to prevent information leakage [44]. There might, however, be a drawback with the introduction of more sophisticated models for evaluating the value of information, because it can in turn lead to more sophisticated information classification models [45].

From an ILM perspective, information can reside in different stages such as in use or archived, and have different value at different points in time. For this to happen, information needs to be reclassified to keep an up-to-date classification which is another issue identified by several authors [14, 22, 35]. The underlying problems why reclassification can be problematic are connected to, for instance, changes in organizations, where users shift domains and projects [15], no well-defined automated mechanisms, leaving the job to humans [34], and a tendency to refrain from declassification [46].

3.5 Policy

Some authors describe the process of developing a classification scheme as problematic in a general way [33, 37], but also the usage, and the enforcement of the classification schemes and policies governing information classification are problematic. Several authors relate the problematic situation of information classification to the standard or framework publishers. Bayuk [5] describes the generic guidelines provided in standards as too generic to cover system characteristics for many systems used in enterprises. Janczewski and Xinli Shi [41] argue that there is a lack of specific standards for health information classification. The lack of more detailed guidelines creates a difficulty of developing robust schemes that cover the requirements from the organization, but still provide flexibility without being too cumbersome [9]. This leads to a situation where people find it difficult to classify information because the scheme does not fit their needs [33]. Many times, the classification schemes turn out to be too complex, which leads to disuse [33, 47] or that new classifications are developed in different business organization units [33]. Examples of the creation of new categories to better suit the organizations needs come mainly from the governmental sector where, for instance, the usage of “sensitive but unclassified” [46, 48] has been introduced. This kind of undefined categories raises the question of both the legitimate use of the information and the category itself [46].

The security policy of an organization has a direct relationship with information classification [45], and when the organization classifies information according to a

classification scheme, it automatically classifies according to a hierarchical model. This leads to an assumption that the organization uses a similar hierarchy for responsibility and for accessing the information among the users [45], which is not necessarily the case.

The policy might be extra critical when placing data in the cloud [36, 49, 50], or when outsourcing [51]. The central problem is that if the policy is not clearly defined, or correct information values are defined, it is possible that highly sensitive data are migrated [52]. The policy might need to be extra fine-grained [53], and passed to the cloud providers [54] to avoid some of the problems. The problem is similar even if the information is not placed in a cloud, but rather shared with other organizations. The usage of organization specific policies and classification schemes, combined with the sharing of data is described as one of the biggest obstacles, especially in the governmental and military sectors. The main issues here are to align what equals one category in one organization to another organization's categories, and to align the rules for handling the information [55]. Just the fact that the many ways of implementing the classifications, which in turn leads to increased difficulties of sharing information are described by [56-58].

Finally, many organizations use data privacy policies, but there are interdependencies to the information classification process. When data is consolidated, privacy breaches might arise as a result of the consolidation [59, 60].

3.6 Resource Management

Resource management issues are primarily related to costs of classifying information. The costs of information classification are twofold [10]: the cost and effort of developing the classification scheme with appropriate controls [9, 17, 47, 61, 62] and the cost of training all staff [10]. For organizations required by law to classify information, costs can be more easily motivated, but for non-regulated organizations, it can be difficult to justify the efforts as they don't directly lead to revenue generation [10]. Hayes [11] captures the resource management issues as *"it can prove difficult to get colleagues excited about a business case for valuing data. There's just too much of the stuff, and the task is too daunting"* [11, p. 61].

3.7 Technology

Several tools for automatic information classification exist, but there are many questions about what kind of information or data they can manage, and how the information is classified. One of the fundamental problems within autonomous systems is to automatically evaluate the information and classify it [16]. There are also issues with overclassification when data is taken from several sources and automatically consolidated [63]. Overclassification and underclassification for that matter are not an information classification problem per se, but rather a consequence of the usage of the information classification scheme, regardless if it is manual or automated. There are consequences with over- and underclassification of information, such as unintended operational consequences that are hindering people from doing their job when metadata is used to label

information that in turn hinders them from accessing the information [52], or when information is overclassified to protect the asset owners [64].

Everett [52] believes it is not possible to just solve the problem of information classification by adopting technology since it is very much a human and process problem, and that even if a tool existed, automatic classification based on key words and phrases without the need for manual intervention are not available anyway.

Due to characteristics such as decentralized storage, ad-hoc relationships with other data sources, and the volatility of the data itself, makes it very challenging to enforce information classification [61]. Wei, et al. [65] describe a situation where many platforms, different development languages and static and dynamic content became an insurmountable obstacle.

In order to be able to enforce the classification it is important to point out that after a piece of information has been classified according to the classification scheme, it needs to be labelled accordingly. This labelling or tagging has several issues. Firstly, there are issues with the representation on a binary level, because computer systems normally do not enforce labelling [36]. Furthermore, not all kinds of information allow direct labelling [22], for example, if high granularity on the classified information exist, potentially each cell in a database needs to be labelled which makes it almost impossible to establish and maintain the protection when information is aggregated [66]. The implementation of labels also causes issues in orthogonal systems, where it is hard to trace classifications outside a single application [67], and when implementing the authorization runtime in access control systems [68]. Finally, there are also challenges when labelling in virtualized systems and in cloud computing [17].

One big question raised by many is on what level of granularity the information classification needs to be performed. This might, to some extent, be organizational specific, but it is clear that many are struggling with granularity and the implications of it. It is normally quite easy to protect, for instance, an entire database if all included data have the same classification [66]. If the granularity is on a lower level, e.g. an individual cell in a database or every email, every file or even sentences in a text document, it can enable access to information [69, 70], but it can also inhibit it. This is especially true when information is combined and the aggregated information automatically gets assigned the highest classification of the combined data [69]. In parallel to the discussion of increasing granularity, there is also a question of decreasing the granularity to reduce the amount of classifications [28].

4 Discussion

An overview of the findings is presented in Table 2, where publications are classified according to the corresponding factors. It is important to point out that the issues found should not be measured in a quantitative way, but rather be seen as a more frequently mentioned issue. The *policy* factor, for example, is not more important or a more severe inhibitor than *management and organization of CIS* even though it has a greater number of publications mentioning the issue. If, for instance, there is a lack of leadership in the organization, there might be no information classification at all, regardless of how suitable and applicable the policy is.

It should also be mentioned that most of the publications only appear in Table 2 once, which means that they only discuss one of the factors. This is because most of the publications does not describe information classification issues, but rather mentions it in relation to something other, that is in focus of their work.

Table 2. Overview of findings

Factors	Publications
External influences	[5], [9], [19], [29], [30], [31], [32], [33], [34], [35], [36].
Human error	[8], [17], [19], [33], [37], [38], [39], [40].
Management and organization of CIS	[10], [41].
Performance management	[14], [15], [22], [34], [35], [39], [42], [43], [44], [45], [46].
Policy	[5], [9], [33], [36], [37], [41], [45], [46], [47], [48], [49], [50], [51], [52], [53], [54], [55], [56], [57], [58], [59], [60].
Resource management	[9], [10], [11], [17], [47], [61], [62].
Technology	[16], [22], [36], [52], [54], [61], [63], [64], [65], [66], [67], [68], [69], [70].

Policy turns out to be a very widely used term to depict several different things. The literature mixes the use of policy, guideline, scheme, matrix and model for describing the information classification process and its associated documentation. In this work, the original terms used by the respective authors have been used to a great extent, both to highlight the issue itself, but also to keep the accuracy in the classification. There are not necessarily any correct term to use, but ISO/IEC uses the term *information classification scheme* to describe the classification scheme and its associated meta-information [3]. It is recommended that an organization use the policy term with care as it otherwise might reduce the influence of the information security policy, but also to limit confusion when referring to the policy. Clearly, the information security policy is a managerial document that in turn can mandate the use of information classification as a part of the asset management. To support in the classification, an information classification scheme with guidelines should be used. This also highlights the connection to *management and organization of CIS*, since the lack of a clear scheme and guidelines is a management issue. In turn, this affects several of the other factors since they are intertwined and depend on clear guidelines. The external influences are affected if the classification scheme is not adapted to the

organization, and if the guidelines are hard to interpret, human *error* can lead to subjective judgement and consistency issues. The lack of an information lifecycle management perspective in the guidelines might affect archiving of information and inhibit reclassification, and therefore, also affect the *performance management*. Finally, a lack in *resource management* might also connect to the management since if too few resources are invested into creating the guidelines and the classification scheme, the classification process can suffer.

The lack of a formalized process description for information classification might be one of the answers to why it is a problematic task to perform. For example, both ISO and COBIT uses information classification as a part of their asset management, but the processes are described very generally, which is because of the general nature of the standards. If the standards are to fit all, they need to be on a general level, but we firmly believe that the processes could be explained more in detail to avoid some of the problems identified in this paper. There are some process descriptions trying to describe the information classification process, for example [71], but we strongly believe an even more detailed process model is needed to facilitate information classification in practice.

It is of course not possible to develop generic guidelines that fit exactly for all organizations, and each individual organization needs to develop their own scheme with their own classification categories. This leads to a situation where more or less compatible classification schemes need to co-exist and be mapped together every time data is to be outsourced, put in a cloud or shared. More detailed guidelines and a process description will, at least, provide a common language and a common view that will decrease the tensions in such situations.

Furthermore, there is a notable lack of papers describing the use of information classification in ISMS. To a certain extent, this is explainable by a low adoption rate, combined with a low interest from academia in studying ISMS [72].

From another perspective, it is possible to ask if information classification and the ISMS are the wrong way for organizations to take as a part of their information security work. Siponen and Willison [73] agree with the previously mentioned results about the issues of being too generic in the guidelines from the standards issuer, but also adds that the standards have not been validated but rather fostered to an appeal to common practice and authority which is an unsound basis for a true standard. Furthermore, it is added that the ISMS process is likely to be fallible because of this [73].

Much research is performed in the areas that relate to, or make an impact on the information classification process. Automatic classification, using, for instance, different techniques from machine learning and linguistics seem to be a growing field. Access control mechanisms and models are researched in a number of ways, for example, on giving access to more fine-grained data, which it is important since it enforce the information classification when access is to be granted to a specific piece of information. There is also research about the labelling part of the information classification process, and topics include, for instance, how labelling inside a text document, individual cells in a database or individual emails are to be labelled. Not all the issues identified in the SLR will be solved by technology, but clearly it will play an increasingly important role in decreasing the impact in some of the issues.

Finally, the factors selected for classification could be developed further. There are possibilities to increase the granularity of the respective factors to create a more detailed view over the issues. The fundamental problems of classifying issues in this domain are the lack of common terms and the lack of a clear process description. If a well-accepted and well-used process description existed, this literature survey would have used it as a framework for classifying the issues.

5 Conclusions and Further Research

In this work, a comprehensive review of the current status of issues in the information classification process is presented and classified into human and organizational factors. Although the SLR returned a large amount of publications, few focus on the issues of the information classification process itself. It is very evident that more research is needed in this field, so that issues can be better understood and avoided or have their impact decreased when implementing ISMS in an organization. Furthermore, in the light of the found issues, it is essential to investigate the enablers to information classification.

Additionally, it is obvious that the management factor is more important than portrayed in the existing body of literature and that more research is needed to understand the roles and effects of the *management and organization of CIS*. Partly, this problem is due to the lack of a common formalized process description of information classification, but also to a lack of using a common language to describe the process.

There are many other aspects of the classification process that needs further investigation. The connection to information lifecycle management (ILM) could be investigated from many perspectives. Firstly, one can explicitly connect the information classification process to the ILM, and secondly, will that alleviate the work with the classifications?

Finally, there are few examples of papers describing the empirical work with information classification, especially in relation to ISMS. Mainly, the literature is focused on theoretic work, for instance, automatic classification, and how to achieve finer granularity and labelling. If the information classification process is going to expand from a need in most organizations to something comprehensible and performed, more real-world examples are needed.

References

1. Oscarson, P., Karlsson, F.: A National Model for Information Classification. In: AIS SIGSEC Workshop on Information Security & Privacy (WISP 2009), Phoenix, AZ, USA (2009)
2. ISO/IEC 27000: Information technology – Security techniques – Information security management systems – Overview and vocabulary. ISO/IEC (2014)
3. ISO/IEC 27002: Information technology – Security techniques – Code of practice for information security controls. ISO/IEC (2013)

4. Axelrod, C.W., Bayuk, J.L., Schutzer, D.: Enterprise Information Security and Privacy. Artech House (2009)
5. Bayuk, J.: The utility of security standards. In: 2010 IEEE International Carnahan Conference on Security Technology (ICCST), pp. 1–6 (2010)
6. Park, W.-S., Seo, S.-W., Son, S.-S., Lee, M.-J., Kim, S.-H., Choi, E.-M., Bang, J.-E., Kim, Y.-E., Kim, O.-N.: Analysis of Information Security Management Systems at 5 Domestic Hospitals with More than 500 Beds. Healthc. Inform. Res. 16, 89–99 (2010)
7. Luethi, M., Knolmayer, G.F.: Security in Health Information Systems: An Exploratory Comparison of U.S. and Swiss Hospitals. In: 42nd Hawaii International Conference on System Sciences, HICSS 2009, pp. 1–10 (2009)
8. Glynn, S.: Getting To Grips With Data Classification. Database and Network Journal 41, 8–9 (2011)
9. Ghernaouti-Helie, S., Simms, D., Tashi, I.: Protecting Information in a Connected World: A Question of Security and of Confidence in Security. In: 14th International Conference on Network-Based Information Systems (NBiS), pp. 208–212 (2011)
10. Collette, R.: Overcoming obstacles to data classification [information security]. Computer Economics Report (International Edition) 28, 8–11 (2006)
11. Hayes, J.: Have data will travel - [IT security]. Engineering & Technology 3, 60–61 (2008)
12. Kane, G., Koppel, L.: Information Protection Function One: Governance. In: Kane, G.K., Lorna (eds.) Information Security, ch. 1, pp. 1–11. Elsevier, Boston (2013)
13. Kitchenham, B., Charters, S.: Guidelines for performing Systematic Literature Reviews in Software Engineering. Keele University and Durham University Joint Report (2007)
14. Virtanen, T.: Design Criteria to Classified Information Systems Numerically. In: Dupuy, M., Pierre, P. (eds.) Trusted Information. IFIP, vol. 65, pp. 317–325. Springer, Boston (2001)
15. DuraiPandian, N., Chellappan, C.: Dynamic information security level reclassification. In: 2006 IFIP International Conference on Wireless and Optical Communications Networks, Bangalore, India (2006)
16. Hayat, Z., Reeve, J., Boutle, C., Field, M.: Information security implications of autonomous systems. In: Proceedings of the 2006 IEEE Conference on Military Communications, pp. 897–903. IEEE Press, Washington, D.C. (2006)
17. Eloff, J.H.P., Holbein, L.R., Teufel, S.: Security classification for documents. Computers & Security 15, 55–71 (1996)
18. Feuerlicht, J., Grattan, P.: The role of classification of information in controlling data proliferation in end-user personal computer environment. Computers & Security 8, 59–66 (1989)
19. Parker, D.B.: The classification of information to protect it from loss. Information Systems Security 5, 9–15 (1996)
20. Kwo-Jean, F., Shu-Kuo, L., Chi-Chun, L.: A study on e-Taiwan information system security classification and implementation. Computer Standards & Interfaces 30, 1–7 (2008)
21. Fernando, D., Zavarsky, P.: Secure decommissioning of confidential electronically stored information (CESI): A framework for managing CESI in the disposal phase as needed. In: 2012 World Congress on Internet Security (WorldCIS), pp. 218–222 (2012)
22. Fibikova, L., Müller, R.: A Simplified Approach for Classifying Applications. In: Pohlmann, N., Reimer, H., Schneider, W. (eds.) ISSE 2010 Securing Electronic Business Processes, pp. 39–49. Vieweg+Teubner (2011)
23. Everett, C.: Building solid foundations: the case for data classification. Computer Fraud & Security 2011, 5–8 (2011)

24. Wohlin, C., Runeson, P., da Mota Silveira Neto, P.A., Engström, E., do Carmo Machado, I., de Almeida, E.S.: On the reliability of mapping studies in software engineering. Journal of Systems and Software 86, 2594–2610 (2013)
25. Boell, S., Cezec-Kecmanovic, D.: Are systematic reviews better, less biased and of higher quality? In: European Conference on Information Systems (2011)
26. Lin, J.: Is searching full text more effective than searching abstracts? BMC Bioinformatics 10, 1–15 (2009)
27. Kraemer, S., Carayon, P., Clem, J.: Human and organizational factors in computer and information security: Pathways to vulnerabilities. Computers & Security 28, 509–520 (2009)
28. Strauss, A., Corbin, J.: Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory. Sage Publications, Inc., Thousand Oaks (1998)
29. Gantz, S.D., Philpott, D.R.: Federal Information Security Fundamentals. In: Gantz, S.D.P., Daniel, R. (eds.) FISMA and the Risk Management Framework, ch. 2, pp. 23–52. Syngress (2013)
30. Grandison, T., Bilger, M., O'Connor, L., Graf, M., Swimmer, M., Schunter, M., Wespi, A., Zunic, N.: Elevating the Discussion on Security Management: The Data Centric Paradigm. In: 2nd IEEE/IFIP International Workshop on Business-Driven IT Management, BDIM, pp. 84–93 (2007)
31. Jafari, M., Fathian, M.: Management Advantages of Object Classification in Role-Based Access Control (RBAC). In: Cervesato, I. (ed.) ASIAN 2007. LNCS, vol. 4846, pp. 95–110. Springer, Heidelberg (2007)
32. Lindup, K.R.: A new model for information security policies. Computers & Security 14, 691–695 (1995)
33. Parker, D.B.: The strategic values of information security in business. Computers & Security 16, 572–582 (1997)
34. Ramasamy, H.V., Schunter, M.: Multi-Level Security for Service-Oriented Architectures. In: Military Communications Conference, MILCOM 2006, pp. 1–7. IEEE (2006)
35. Bunker, G.: Technology is not enough: Taking a holistic view for information assurance. Information Security Technical Report 17, 19–25 (2012)
36. Winkler, V.: Chapter 3 - Security Concerns, Risk Issues, and Legal Aspects. In: Winkler, V. (ed.) Securing the Cloud, pp. 55–88. Syngress, Boston (2011)
37. Baškarada, S.: Analysis of Data. In: Information Quality Management Capability Maturity Model, pp. 139–221. Vieweg+Teubner (2009)
38. Booysen, H.A.S., Eloff, J.H.P.: Classification of objects for improved access control. Computers & Security 14, 251–265 (1995)
39. Ku, C.-Y., Chang, Y.-W., Yen, D.C.: National information security policy and its implementation: A case study in Taiwan. Telecommunications Policy 33, 371–384 (2009)
40. Puhakainen, P., Siponen, M.: Improving employees' compliance through information systems security training: an action research study. MIS Q. 34, 757–778 (2010)
41. Janczewski, L., Xinli Shi, F.: Development of Information Security Baselines for Healthcare Information Systems in New Zealand. Computers & Security 21, 172–192 (2002)
42. Al-Fedaghi, S.: On Information Lifecycle Management. In: Asia-Pacific Services Computing Conference, APSCC 2008, pp. 335–342. IEEE (2008)
43. Aksentijevic, S., Tijan, E., Agatic, A.: Information security as utilization tool of enterprise information capital. In: MIPRO, 2011 Proceedings of the 34th International Convention, pp. 1391–1395 (2011)
44. Ager, T., Johnson, C., Kiernan, J.: Policy-Based Management and Sharing of Sensitive Information Among Government Agencies. In: Military Communications Conference, MILCOM 2006, pp. 1–9. IEEE (2006)

45. Arutyunov, V.V.: Identification and authentication as the basis for information protection in computer systems. Sci. Tech. Inf. Proc. 39, 133–138 (2012)
46. Seifert, J.W., Relyea, H.C.: Do you know where your information is in the homeland security era? Government Information Quarterly 21, 399–405 (2004)
47. Saxby, S.: News and comment on recent developments from around the world. Computer Law & Security Review 24, 95–110 (2008)
48. Feinberg, L.E.: FOIA, federal information policy, and information availability in a post-9/11 world. Government Information Quarterly 21, 439–460 (2004)
49. Velev, D., Zlateva, P.: Cloud Infrastructure Security. In: Camenisch, J., Kisimov, V., Dubovitskaya, M. (eds.) iNetSec 2010. LNCS, vol. 6555, pp. 140–148. Springer, Heidelberg (2011)
50. Wilson, P.: Positive perspectives on cloud security. Information Security Technical Report 16, 97–101 (2011)
51. Freeman, E.: Information and Computer Security Risk Management. In: Ghosh, S., Turrini, E. (eds.) Cybercrimes: A Multidisciplinary Analysis, pp. 151–163. Springer, Heidelberg (2011)
52. Everett, C.: Building solid foundations: the case for data classification. Computer Fraud & Security 2011(6), 5–8 (2011)
53. Adiraju, S.K.: Security Considerations in Integrating the Fragmented, Outsourced, ITSM Processes. In: 2012 Third International Conference on Services in Emerging Markets (ICSEM), pp. 175–182 (2012)
54. Chaput, S., Ringwood, K.: Cloud Compliance: A Framework for Using Cloud Computing in a Regulated World. In: Antonopoulos, N., Gillam, L. (eds.) Cloud Computing, pp. 241–255. Springer, London (2010)
55. Hilton, J.: Improving the secure management of personal data: Privacy on-line IS important, but it's not easy. Information Security Technical Report 14, 124–130 (2009)
56. Wang, W., Peng, G., Lu, G.: Agricultural Informationization in China. In: Ordóñez de Pablos, P.L., Miltiadis, D. (eds.) The China Information Technology Handbook, pp. 271–297. Springer US (2009)
57. Boonstra, D., Schotanus, H.A., Verkoelen, C.A.A., Smulders, A.C.M.: A methodology for the structured security analysis of interconnections. In: Military Communications Conference - MILCOM 2011, pp. 1267–1272 (2011)
58. Wrona, K., Hallingstad, G.: Controlled information sharing in NATO operations. In: Military Communications Conference - MILCOM 2011, pp. 1285–1290 (2011)
59. Karat, J., Karat, C.-M., Brodie, C., Feng, J.: Privacy in information technology: Designing to enable privacy policy management in organizations. International Journal of Human-Computer Studies 63, 153–174 (2005)
60. Vrhovec, G.: Beating the privacy challenge. Computer Fraud & Security 2011, 5–8 (2011)
61. Kulkarni, A., Williams, E., Grimaila, M.R.: Mitigating Security Risks for End User Computing Application (EUCA) Data. In: 2010 IEEE Second International Conference on Social Computing (SocialCom), pp. 1171–1176 (2010)
62. Tsai, W.T., Wei, X., Chen, Y., Paul, R., Chung, J.-Y., Zhang, D.: Data provenance in SOA: security, reliability, and integrity. SOCA 1, 223–247 (2007)
63. Newman, A.R.: Confidence, pedigree, and security classification for improved data fusion. In: Proceedings of the Fifth International Conference on Information Fusion, vol. 2, 1402, pp. 1408–1415 (2002)
64. Taylor, L.P.: Chapter 8 - Categorizing Data Sensitivity. In: Taylor, L.P. (ed.) FISMA Compliance Handbook, 2nd edn., pp. 63–78. Syngress, Boston (2013)

65. Wei, W., Shengzhong, Y., Hong, H.: Design of Portal-Based Uniform Identity Authentication System in Campus Network. In: 2010 International Conference on Multimedia Communications (Mediacom),, pp. 112-115 (2010)
66. Blyth, A., Kovacich, G.L.: IA and Software. Information Assurance, pp. 191–212. Springer, London (2006)
67. Demsky, B.: Cross-application data provenance and policy enforcement. ACM Trans. Inf. Syst. Secur. 14, 1–22 (2011)
68. Ashley, P., Vandenwauver, M., Siebenlist, F.: Applying authorization to intranets: architectures, issues and APIs. Computer Communications 23, 1613–1620 (2000)
69. Burnap, P., Hilton, J.: Self Protecting Data for De-perimeterised Information Sharing. In: Third International Conference on Digital Society, ICDS 2009, pp. 65–70 (2009)
70. Alqudah, B.I., Nair, S.: Toward Multi-Service Electronic Medical Records Structure. In: Suh, S.C., Gurupur, V.P., Tanik, M.M. (eds.) Biomedical Engineering, pp. 243–254. Springer, New York (2011)
71. Etges, R., McNeil, K.: Understanding data classification based on business and security requirements. ISACA Information Systems Control Journal 5 (2006)
72. Fomin, V.V., de Vries, H.J., Barlette, Y.: ISO/IEC 27001 information systems security management standard: exploring the reasons for low adoption. In: EUROMOT 2008 Conference, Nice, France (2008)
73. Siponen, M., Willison, R.: Information security management standards: Problems and solutions. Information & Management 46, 267–270 (2009)

http://www.springer.com/978-3-319-11598-6

Secure IT Systems
19th Nordic Conference, NordSec 2014, Tromsø, Norway, October 15-17, 2014, Proceedings
Bernsmed, K.; Fischer-Hübner, S. (Eds.)
2014, XII, 296 p. 81 illus., Softcover
ISBN: 978-3-319-11598-6