THE MANAGEMENT OF INFORMATION AND CYBERSECURITY AND THE PROTECTION OF INTELLECTUAL CAPITAL - A SYSTEMATIC LITERATURE REVIEW

18.3.2023

Lappeenranta–Lahti University of Technology LUT
Master's Programme in Knowledge Management and Leadership, Master's thesis
2023
Kaj Mikael Paananen
Examiner(s): Professor Kirsimarja Blombqvist
Assistant Professor Henri Hussinki

ABSTRACT

Lappeenranta–Lahti University of Technology LUT

School of Business and Management

Business Administration

Kaj Paananen

The management of information and cybersecurity and the protection of intellectual capital -- a systematic literature review

Master's thesis

2023

101 pages, 21 figures, 3 tables and 1 appendix

Examiners: Professor Kirsimarja Blombqvist and Assistant Professor Henri Hussinki

Keywords: Intellectual capital, management of information and cyber security, knowledge protection, protection of intellectual capital

Ever since Peter Drucker presented the concept of knowledge economy in 1960´s has the importance of intellectual property become more and more recognized. The importance of intellectual capital is emphasized in modern societies and in innovation centric businesses.

This thesis examines the relationship of information and cyber security and intellectual capital. The motivation is to view how the protection of intellectual capital is approached and covered in information and cyber security related research. The subject is interesting and important as the success of an organization is tightly bound with those resources it has in its possession. When the capability to create sustainable competitive advantages is dependent on the intellectual capital, then these resources should be adequately protected.

The thesis is executed as a systematic literature review where the information and cyber security management related research is reviewed. The scope for the systematic literature review is to evaluate how the research addresses the concept of intellectual capital. The research covered 1555 articles written in English and published between 2010 and 2022.

The results demonstrate that the concept of intellectual capital and is sub-concept of information hierarchy are not recognized in information and cyber security management related research. The topic is important as the information and knowledge-based societies and organization´s compete about their place in the sun. By correctly addressing the protection of intellectual property may help the organization to succeed and to protect its most important resources.

The thesis also points, that information and cyber security management related research is focusing on certain areas, like standards and technology. Based on the systematic literature review the research is thin on the areas like interaction with other areas of business areas and management or with leadership.

TIIVISTELMÄ

Lappeenrannan–Lahden teknillinen yliopisto LUT

LUT-kauppakorkeakoulu, Kauppatieteet

Kaj Paananen

Tieto- ja kyberturvallisuuden johtaminen sekä tietopääomien suojaaminen -systemaattinen kirjallisuuskatsaus

Pro gradu -tutkielma 2023

101 sivua, 21 kuvaa, 3 taulukkoa ja 1 liite

Tarkastajat: Professori Kirsimarja Blombqvist ja apulaisprofessori Henri Hussinki

Avainsanat: Tietopääoma, tieto- ja kyberturvallisuuden johtaminen, tiedon suojaaminen, tietopääomien suojaaminen.

Tiedon, tietojohtamisen ja tietopääomien merkitys on jatkuvasti kasvanut siitä lähtien kun Peter Drucker esitteli tietotalouden käsitteen 1960-luvulla. Tieto ja tietopääomat ovat merkityksellisiä modernille yhteiskunnalle ja etenkin innovaatiokeskeisille liiketoiminnoille.

Tässä tutkimuksessa tarkastellaan tietopääomien suojaamista tieto- ja kyberturvallisuuden johtamista käsittelevässä tutkimuksessa. Aihe on kiinnostava ja merkittävä, koska tietopääomilla ja niiden hyödyntämisellä on merkittävä rooli organisaation kilpailukyvyn luomisessa. Tieto- ja kyberturvallisuuden voisi olettaa vastaavan näiden resurssien suojaamistarpeeseen.

Tutkimus suoritettiin systemaattisen kirjallisuuskatsauksena tieto- ja kyberturvallisuuden johtamista käsittelevään tutkimukseen. Tutkimus kattoi 1555 vuosien 2010 ja 2022 välissä julkaistua tieto- ja kyberturvallisuuden johtamista käsittelevää tutkimusta.

Tutkimus osoitti, että tieto- ja kyberturvallisuuden johtaminen ei käytännössä tunnista tai huomioi tietopääomien käsitettä tai sen alakäsitteisiin kuuluvaa tiedon hierarkiaa. Havainto on merkittävä, sillä tiedolla, tietopääomilla ja niiden hyödyntämisellä on merkittävä rooli moderneille yhteiskunnille sekä organisaatioille. Jotta tieto- ja kyberturvallisuus voisi tehokkaasti ja tarkoituksenmukaisesti suojata organisaation tärkeitä resursseja, sen tulisi kyetä myös tunnistamaan ne.

Tutkimuksessa osoitettiin myös, että tieto- ja kyberturvallisuuteen liittyvä tutkimus keskittyy tiettyihin tieto- ja kyberturvallisuuden osa-alueihin, kuten standardeihin tai teknologiaan eikä se esimerkiksi huomioi muita johtamisen osa-alueita tai johtajuutta.

ACKNOWLEDGEMENTS

First, I want to express my deepest gratitude to the Finnish society and to the education system it has available for all of us. Open and curious minds with access to information and knowledge has made us who we are, which is the happiest nation on the planet.

Secondly, I owe a thank you to all my awesome colleagues I have had the pleasure to work with. You have always been open for discussion and ready to ponder over any topic. Equally my deepest respect to those great managers I have had the pleasure to work for. You have guided and encouraged me to the direction where I now happily am.

And last -to my dearest and closest ones, words cannot express my gratitude on the patience and understanding you have demonstrated. The last two and a half years of non-stop home-office work combined with studies has not been a pretty sight -thank you!

ABBREVIATIONS

CISO	Chief information security manager
CMMI	Capability Maturity Model
COBIT	Control Objectives for Information Technologies
DIKW	Data Information Knowledge Wisdom
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
HRM	Human Resource Management
IC	Intellectual Capital
IP	Intellectual Property
IPR	Intellectual Property Rights
IS	Information security
ISM	Information security management
ISMS	Information security management system
ISO	International Standardization Organization
ISRM	Information security risk management
IRM	Information risk management
KM	Knowledge management
NIST	National Institute of Standards and Technology
PCI DSS	Payment Card Industry Data Security Standard
RBV	Resource-based view
SLR	Systematic literature review

Table of contents

List of figures

Tables

1. Introduction

1.1. Research Background

We all have heard the patter “data is the new oil” in different occasions and events. In general, one can agree that there are similarities like, both can be refined for generating value and both can cause damage if they leak from their container.

Information security is activity and discipline which aims on the protection of organizations key information assets, such as data and information in documents and in databases (Whitman & Mattord 2009, von Solms & van Niekerk 2013, Luczak 2014 etc.). The definition on information security refers to the protection of the confidentiality, integrity and availability of information. In research information security has been identified to be a broad umbrella term which is used multiple contexts (Lundgren & Möller 2019, 420-422). Information security is still relatively new area of research where the foundation and background are in technological aspects and in the protection of the information processing technology (Nnolim 2008, 1. von Solms 2006). The resource-based view of the firm has gained popularity as it explains the role of key resources for an organization (Ployhart 2021, 1772). These two areas of research (information security and resource-based view of the firm) have been developing within the last decades and one could assume, that these areas would be linked to ensure both the identification and protection of organizations key assets.

Knowledge has become one of the most important forms of capital for organizations (Drucker 1998) and the organizations capabilities to acquire, create and to utilize intellectual capital “has become the main driver of competitiveness” (Kianto 2007 with reference to Edvinsson and Malone 1997 & Marr 2005). Another key capability for modern organization is the capability to constantly improve its ways of working and to innovate. The organizations innovation capabilities are dependent on its capacity to utilize the intellectual capital is has (Subramaniam and Youndt 2005). Michael Porter (1985) introduced a theory of competitive advantages and strategy. It describes in theory on how a firm can create and sustain advantage in its industry. According to Porter there are two kinds of basic competitive advantages: cost leadership and differentiation. Firms can use their strategies to impact on its position on markets, or even affect the industry structure (Porter 1985 3-7). Firm resources

and especially intellectual capital are a key element in organization´s value creation strategy. As the intellectual capital is seen as the key resource (Martín-de-Castro, Delgado-Verde, López-Sáez, & Navas-López 2011) or the only true "strategic asset" (Meso & Smith, 2000, 1) of an organization, then the safe-guarding and protection of these assets should also be a key focus for it (von Soms & von Soms 2004). When the external environment is constantly changing, the emerging technologies are transforming the competitive environment and the evolving threat landscape is making the mitigation of risks hard, organizations should concentrate their efforts when protecting their success factors. The resource-based view is the approach to identify and to manage these vital firm resources. The information and cyber security management are those activities what an organization would do to protect its property and assets.

The umbrella term information security is used to describe those activities an organization is implementing for protecting its information (Olijnyk 2015, 883). Cybersecurity even it is commonly used interchangeable or in context with the term information security (von Solms & Niekerk 2013, 97) addresses and focuses to the risks raising from the cyberspace and from the more and more interconnected and complex operating environment (Xu, Yung & Wang 2021, 263). Therefore, in this work, both the information and cybersecurity aspects are included, to ensure that the intellectual capital and information security aspects are covered to a sufficient extent.

This study focuses on the protection of organization intellectual capital and information assets. The purpose of the thesis is to examine how intellectual capital is accommodated within information and cyber security management literature. The topic is relevant and interesting because the importance of intellectual capital and knowledge for an organization. As per Barney (1991, 101) the firm resources are the primary source for an organization to gain sustained competitive advantage. The concept of firm resources includes all assets possessed by the organization, including information and knowledge. With these resources the organization can generate value and to gain sustained competitive advantage. In this definition the word sustained indicates that the resources are needed for longer period, and the possession of these resources allow the organization to distinguish from its competitors. These valuable, vital and unique resources should also be the focal point for organizations security management. With the proper understanding of organizations important assets, the activities and

resources of information and cyber security can be directed and steered in the most beneficial way.

1.2. Previous research and research gap

The resource-based view is a very popular management theory for more than thirty years and the topic has been studied broadly (Davis & DeWitt 2021, 1684-1685). The concept of firm resources and intellectual capital are well established and supported with comprehensive amount of research. The knowledge protection is seen as one of the key knowledge management activities (Inkinen, Kianto & Vanhala 2015, 434) and there are studies on the protection of intellectual property (ref. Päällysaho & Kuusisto 2011) but there is not much research on the knowledge protection or knowledge protection related governance (Husted, Michailova & Olander 2013, 5). The protection of knowledge and intellectual property seem to be covering only few categories of intellectual capital. When this seems to be the approach, then consequently the ways on how the protection can be accomplished will be limited. For example, the formal methods on how intellectual property can be protected are intellectual property rights, contracts and labor legislation (Olander, Hurmelinna-Laukkanen, Vanhala & Blomqvist 2019, 5). From the perspective of comprehensive view to the protection of intellectual capital this does not seem like a satisfactory answer.

When the firm resources or in other words, the intellectual capital of an organization is the most valuable asset, there is relatively little research and material focusing on the protection aspects of it. Equally, in the context of knowledge management, the knowledge protection relates mostly to the knowledge sharing in innovation (Hurmelinna 2011, 303). Maybe the rationale for this could be found in information protection and information security related research? As information is an integral part of intellectual capital then maybe information security management provides the answer to this demand.

Information and cyber security are defined as activity which aims to protect the confidentiality, integrity and availability of information (Lundgren & Möller 2019, von Solms & von Solms 2018). Information security is also commonly attached to the protection of information systems (von Solms 2006, Nnolim 2008, Pieters 2011). Does the information and cyber security management related research address the aspect of intellectual capital and the protection of it? These themes and theories have not been studied in conjunction before. The thesis reviews these topics together and seeks to go below the terminology and look for links

and common motifs connecting these two subject areas together. There is a gap in the existing research on the protection of intellectual capital. This thesis and research are an attempt to evaluate the current state and the possible connection in the existing research and to act as a catalyst for future research work.

1.3. Research problem and objectives

The previous research prove that the success of an organization is dependent on the resources and information assets it has in its possession. If, and when the intellectual capital and related information assets are the secret sauce for an organization to enable the development and execution of value creating strategies, then one would assume that these assets would be in the focal point of organizations information and cybersecurity activities. In intellectual capital related research, the protection of aspects is clearly missing. Also, in information & cyber security management related research the link to the concept of intellectual capital is reasonably new and there is no explicit link connecting these topics together.

In addition, the research materials indicate that the definition and role of information and especially cyber security is vague and not in any context with the resource-based view of firm. The role of security is to protect the organization and its valuable assets but in this context the link appears to be missing.

This thesis aims to understand, how the research on the management of information and cybersecurity relates with the resource-based view of a firm. When intellectual capital, information, knowledge, and the capability to create new relevant and useful information is the premise for success or in many cases a matter of survival for the organization, then information and cybersecurity should have very clear role in the protecting of these assets.

The research question (RQ) and sub-questions are the following:

> RQ: Does research on information security / cybersecurity management recognize the concept of intellectual capital?
>
> > SubQ1: Are the theories of information and cybersecurity management and knowledge management synchronized way within the use of the key concepts?
> >
> > SubQ2: Are there any other trends / directions which can be identified in the information security management related research?

In strategic management related research, the resource-based view is commonly used and prevalent. The information and cyber security research are relatively young and not yet concomitant with other research disciplines. The goal for this research is to seek for the link or connection between these two areas of research and theory. The topic is interesting and important, especially on information and knowledge centric businesses and for modern societies. With a holistic and comprehensive view to the protection of organizations key assets, the security objectives can be achieved, and the business strategies can be protected from information and cyber risks. Secondly, a successful study can help to address weaknesses and ambiguities in the concepts of information and cyber security, and by doing so foster the substantive research on the area.

With the proper definitions and clear understanding on the importance of intellectual capital and related assets, the different research and subsequently the organizational practices are able to address the security needs. This will hopefully contribute to the development of holistic view on the protection of intellectual capital and on the protection of the most valuable assets of a firm. This would be very beneficial for information and knowledge centric organizations which seek to specialize and to differentiate from their peers and competitors.

1.4. Scope & limitations

The study will be conducted as a systematic literature review where the focus will be on the existing research on the resource-based view and on the protection of intellectual capital.

The focus is on the link between the protection of intellectual capital and on the information and cyber security management research. The scope will be on the protection of firm resources, meaning such assets which are valuable for the organization, rare, imitable, and non-substitutable. Such resources in theory cannot be homogenous, rather they must be unique and rare and therefore important to protect.

For reasons described above, in this work, the regulatory aspects and views on the definitions and on the motivation for the protection of information, data or other assets are excluded. For example, when the information asset is something described in regulation, like for example personal data (GDPR), health related information (HIPAA) or within a contractual / industry frame like payment card related information (PCI DSS). This as the information is such cases does not necessarily present as a resource which can be used to create sustainable competitive advantages for the organization. And both the definitions of the information asset and the motivation for the protection of it are coming outside of the organization -not from an internal need to protect the unique resource and its value, rareness, inimitability and sustainability.

The selected research strategy and method will partly impact to the scope and on the selection of materials. The purpose for the study is to evaluate how the information & cyber security management related research relates to resource-based view and on intellectual capital. The material selection for the literature review will be done by using selected keywords in a search done against research article database. The original research articles need to be acquired from different sources and due this, some of the articles may not be available. Secondly, the material intake and selection will be done by focusing only on documents written in English. The selected research method limits the study on existing research works focusing on information and cyber security management. The other works addressing the topic from other disciplines than information and cyber security are also excluded.

1.5. Theoretical background and methodology

The research question of the thesis attempts to unravel if the information and cybersecurity management pays attention to the most valuable resources of an organization, which according to the resource-based view is the intellectual capital. The purpose of this research is to

study on how the information / cybersecurity management practices of organizations are addressing this need.

Computer and information security capabilities have been established already in early 1980´s, but the security objectives of security strategies have been focusing to protect physical assets and information systems (Nnolim 2007, 1). So even the term information security does indicate that the information would be the subject to be protected, the foundation of the discipline has not been in information, rather in physical elements around it. Also, the emerging use of term cyber, cyber risk and cybersecurity and the inadequate definition of the term "cyber" has blurred the scope and focus of organizations security objectives (Harel, Ben Gal & Elovici 2017, 2, Strupczewski 2021, 1). The unclarity of clear concept of a term may not appear to be an issue, especially in an informal discussion or other interaction. But in an organizational context, like in "organizational strategy, business objectives, or international agreements" the lack of clear definition or significance of it may cause major implications (Schatz, Bashroush & Wall 2017, 53).

In this thesis the information security management is studied in the context of resource-based view. The theoretical models are derived from information and cybersecurity management and from knowledge management theory. The theoretical framework and research hypothesis are visualized in figure 1.

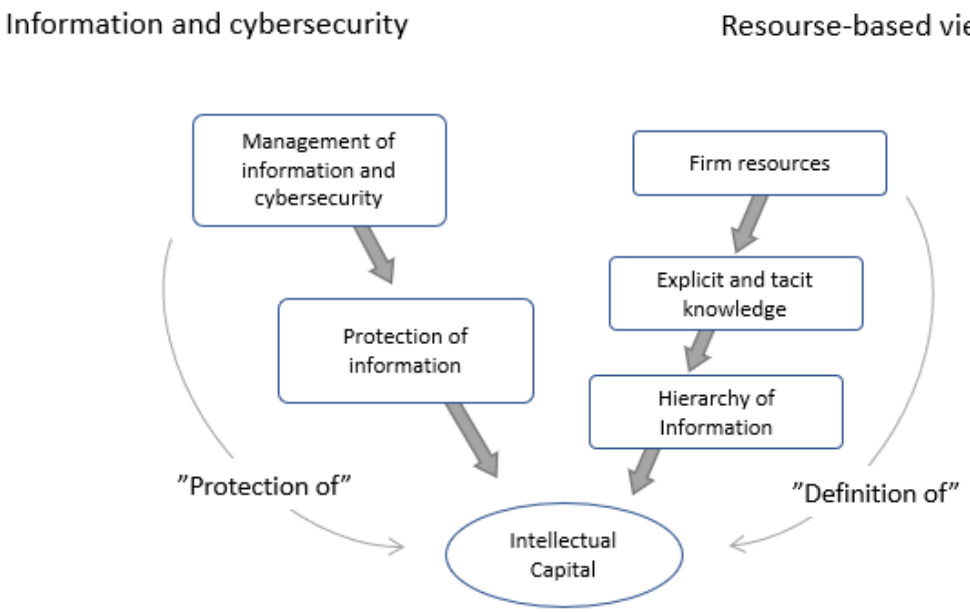


Figure 1. The theoretical framework of the research.

1.6. Structure of the report

Section 1 presents the overall purpose and structure of the thesis. The section introduces the concepts and the theoretical background of the research. It describes the research problem and the specific research questions the thesis attempts to answer to. The section introduces the key concepts and set the theoretical frame for the work. Section 1 also addresses the scope and related limitations of it. The structure and elements of the thesis are presented in figure 2.

Section 2 focuses on the theoretical background and concepts of intellectual capital, information and cybersecurity management. In it an in-depth analysis of existing literature to clarify these concepts and the reasoning for the selected key words. The key theoretical concepts are knowledge management, intellectual capital, knowledge protection, information hierarchy and information & cybersecurity management.

Section 3 describes the research methodology and process. In this section the search and selection of research materials along with the used key words are opened. It also describes the intake process, selection and evaluation of selected research materials which are included in systematic literature research (SLR) along with breakdown of intake, included and excluded materials reported by using the PRISMA model (Prisma 2022).

Section 4 presents the research process along with the summary or results from the systematic literature review (SLR) and on the analysis based on it. In it the categorization of the reviewed research articles is presented and the numeral results of the categorization along with the evaluation on how the concept of intellectual capital and knowledge management are present in the selected information and cybersecurity management related research.

Section 5 is the analysis of the results along with the discussion around the research questions. The Section also includes observations and findings based on the reviewed materials. In this Section also the potential further research topics identified based on this research are presented. includes the discussion and findings made during the research process.

The list of all screened and articles included in the thesis is included as the attachment 1. The overall intake, screening and handling of selected articles of the systematic literature review process is described in chapters 3.6 and 3.7.

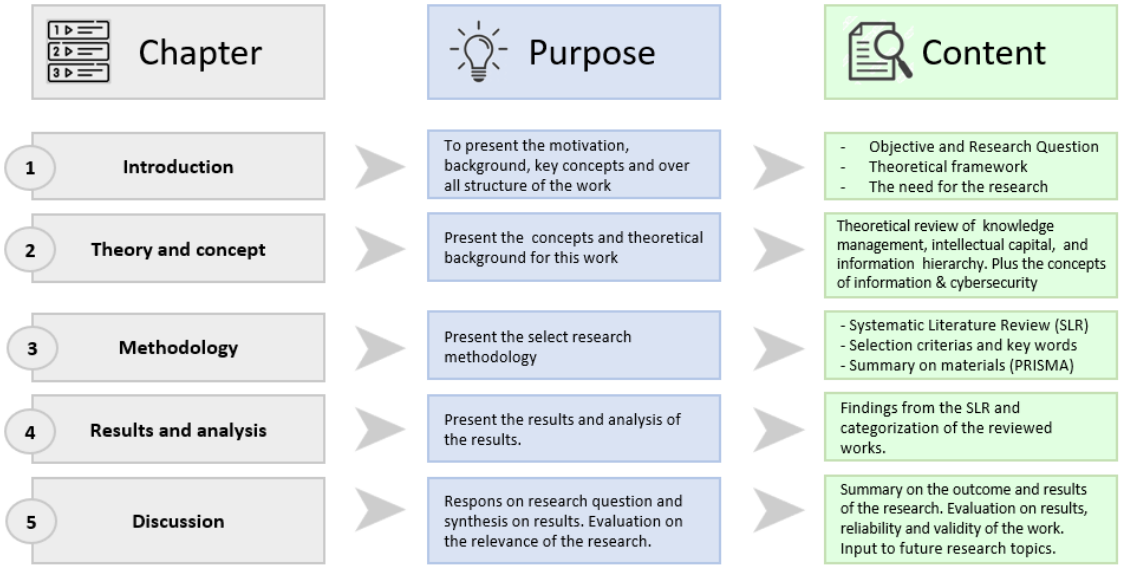


Figure 2. Structure and elements of the thesis.

2. Theory and key concepts

The thesis focuses on studying the relationship between knowledge management and information and cybersecurity around the definition and protection of intellectual capital and information assets. Knowledge management is the discipline focusing on the definition and overall identification and management of knowledge, intellectual capital, and information. Information and cybersecurity management is activity which aims to identify and protect the valuable information assets of an organization. In general, one could assume that these disciplines would be very closely related and that the underlying theories and terminologies would be congruent.

2.1. Resource-based view of the firm

The resource-based view of the firm has become an immensely popular theory around strategic management (Davis & DeWitt 2021, 1684). The resource-based view theory is based

on a view that the success of a firm is dependent on those resources it has in its possession and control (Rothaermel 2012, 5). The resource-based view was developed in 1980 by such authors as Wernerfelt and Barney as a response to the idea where management strategy was focusing mainly on the opportunities on the external markets (Chen, Michael & Wenchen 2021, 1820).

This motivation in this concept is to study the valuable, unique, inimitable resources which are impossible or difficult to replace (Wernerfelt 1984, Barney 1991). These resources "include all assets, capabilities, organizational processes, firm attributes, information, knowledge, etc. controlled by a firm that enable the firm to conceive of and implement strategies that improve its efficiency and effectiveness. In the language of traditional strategic analysis, firm resources are strengths that firms can use to conceive of and implement their strategies" (Barney, 1991, 101). In resource-based view information and knowledge are central elements in value creation and when building sustained competitive advantage (Barney, 1991, 102).

A related concept to resource-based view is knowledge management. It is activity which aims to ensure that the information and knowledge resources the organization has, are benefitting its efforts to gain competitive advantage (Hussinki, Kianto, Vanhala & Ritala 2017, Alavi & Leidner 2001, 113). Knowledge management is about managing processes for creating, storing/retrieving, transferring, and applying knowledge (Alavi & Leidner 2001, 114). Hussinki et al. (2017, 1599) also describe the concept of strategic knowledge management. It encompasses all those activities organization needs to set and manage and monitor it's the knowledge assets it has and which it needs in future. One of the identified knowledge management practices is knowledge protection. However, the knowledge protection is not addressed or focused and its treated separately from other knowledge management practices (Hussinki at al. 2017, 1599, Inkinen 2016, 234). As proven earlier, the intellectual capital, information and knowledge are essential and vital resources for an organization. The capability to create sustainable competitive advantages are dependent on these resources. Therefore, the protection of intellectual capital, information and knowledge need to be understood in more detail, to be able to understand and to define the these in practice.

2.2. Knowledge, information, and data

In information security related research there are various forms on how information or data is addressed like “Information is a valuable resource that is critical for an organization’s success” (Tu, Yuan, Archer & Connelly 2018). “Information is an asset that has value to an organization” (Ramli & Aziz 2012, 57). “Information security applies to the -- business sensitive information of organizations” (Anttila & Jussila 2018, 586). “Valuable data” (Gill, Zavarsky & Swar 2021, 371).

These different terms used resonate with the knowledge management theory, but there seems to lack of systematicity and taxonomy. In knowledge management theory the key activity for organization is the capability to deal with information, turn it to knowledge and to gain competitive benefit by doing so (Nonaka 1994). This indicates that there is an inherent hierarchy relating to information, data and knowledge.

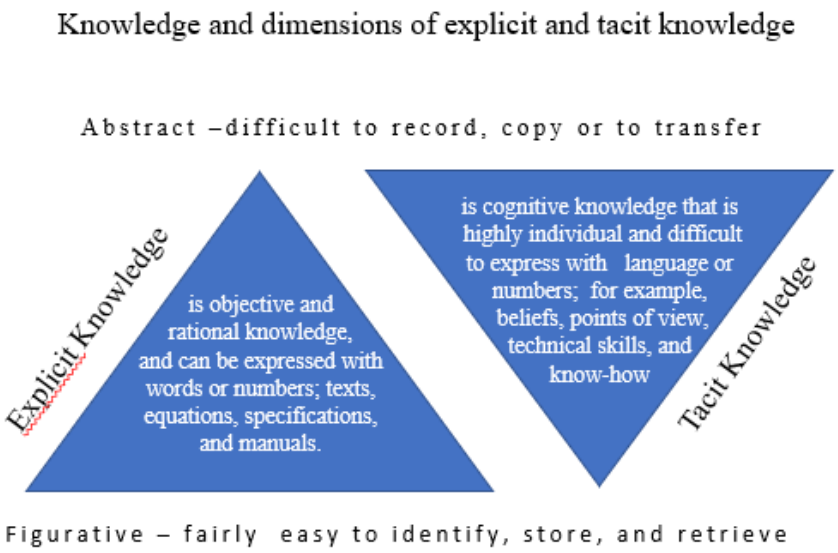


Figure 3. Dimensions of explicit and tacit knowledge (Polanyi 1966, Wellman 2009, Magnier-Watanabe & Benton 2017).

One way to construct a hierarchy is to focus on the different types of knowledge. Michael Polanyi (1966, 4) presented the model of tacit and explicit knowledge, as presented in figure 3. The reasoning behind this split is the fact that the part of knowledge which can be presented in words and numbers is a very limited part of “the entire body of possible

knowledge" (Nonaka 1994, 16). The explicit knowledge is something which can be codified, stored and transmitted easily. When tacit knowledge is something more deeply connected in ways of working, activities and actions in different contextual situations, or like Polanyi expressed it "we know more than we can say" (Nonaka 1994, 16).

The method of only using the explicit and tacit dimensions of knowledge may not be fully satisfying, as there are other relating terms used both in knowledge management and in information security. Terms and concepts as data and information require definition and relationship to knowledge. For example, Alavi & Leidner (2001, 109) discuss on the interrelationship between knowledge, data and information and demonstrate a hierarchical view on the relationship of data, information and knowledge. This model is also called the data-information-knowledge-wisdom (DIKW) hierarchy (Aven 2012, Rowley 2006) figure 4.

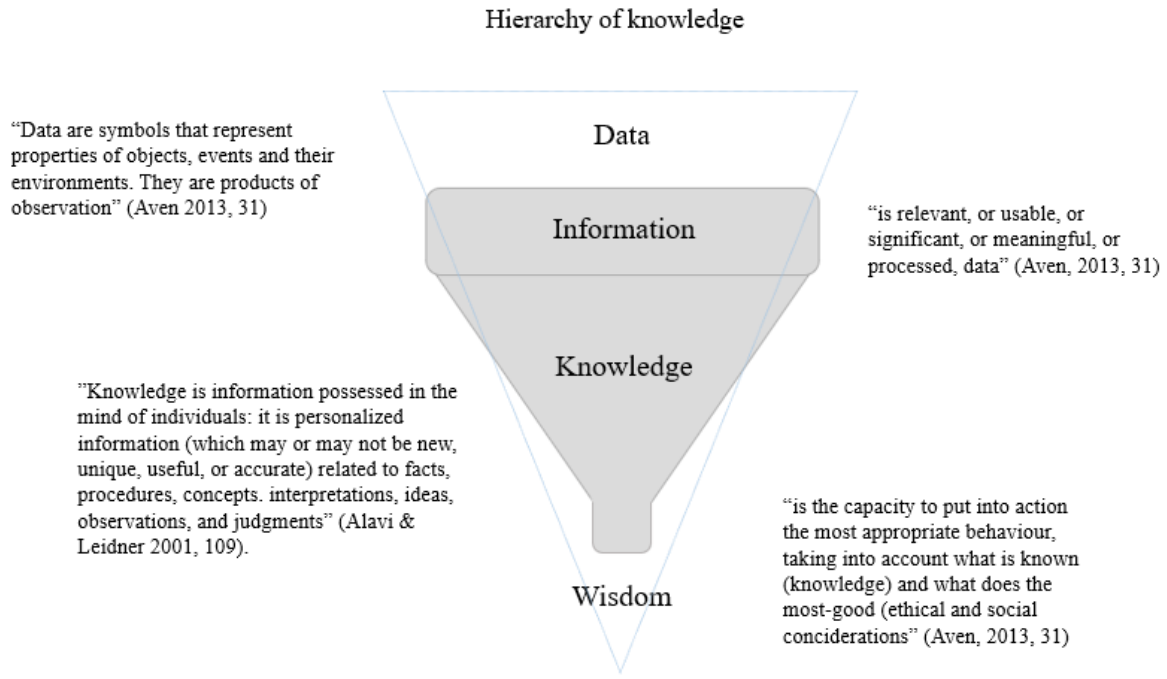


Figure 4. DIKW hierarchy (Alavi & Leidner 2001, Aven 2012)

The DIKW model and hierarchy sets and describes the hierarchy between different terms, like data, information, knowledge and wisdom. In this model, data is in the lowest level of it. Data is made of symbols and values in unstructured and unorganized format. The data

itself is purposeless and alone it does not serve any decision making or action in any meaningful way.

The second level of DIKW model is information. It is the outcome of cleaned, organized and/or structured data in certain context and after an interaction or analysis made by the consumer of the data. The consumer, or user of the data can be either human or a system. In brief, information is meaningful for its user, it provides value for the consumer of it.

The third level of DIKW model is knowledge. In organizational perspective knowledge and knowing is a "condition gained through experience or study – enabling individuals to expand their personal knowledge and apply it to the organization's needs" (Alavi & Leidner, 2001, 110). Knowledge is something deeper than just summary of fragments of information, it is something what the consumer of that particular information can use for gaining deeper understanding and base for "well-reasoned decisions" and actions (Magnier-Watanabe & Benton 2017, 326).

The highest level of DIKW model is wisdom (Aven 2012, Rowey 2005). Wisdom is perceived as "exhibiting two categories of attributes". First, learning from experiences and different sources of information and knowledge and secondly being able to reflect these in the context of the particular situation, circumstance and factors to make right use of information and knowledge for being able to do "right judgement". (Rowley 2006, 1248)

To summarize, the concepts of information, knowledge and the different sub-concepts and hierarchy relating to them is relatively large and multileveled subject. To be able to identify and to focus to the valuable assets of an organization, it is crucial to be understand the multiple concepts. Data, information, and knowledge are just layers of a larger overall concept. Knowledge is also something, which is divided into explicit and to tacit knowledge. By understanding these dimensions, it becomes clear, that the information protection aspects cannot be addressed or treated as something, where a purely technical measures, like encryption would solve the needs.

2.3. Intellectual Capital

Organizations are dependent on their physical and financial assets, but it is the intellectual capital elements which make the difference, and which sets the organization apart from

competitors (Marr 2008). The definition intellectual capital is often used interchangeably with other terms like intangible assets, intangible resources, invisible wealth (Kianto 2007, 343, Marr 2008, 5, Choong 2008, 612).

Intellectual capital together with physical capital and financial capital are the vital resources of organizations, figure 5 (Marr 2008, 6). Intellectual capital includes those non-monetary assets, which are intangible, and they supply value and future gains for the organization (Choong 2008, 628). Dumay (2016, 16) defines intellectual capital being all and everything that everyone in the organization knows, like intellectual material and property, knowledge, experience, information which will supply value and competitive benefit for it. In conclusion, knowledge and information are components in organizations intellectual capital.

Systematic approach to identify and to assess the intellectual capital organization will help it to prioritize and to manage its resources effectively (Marr 2008, 7). The same approach can be used to ensure that the information and cyber security activities are covering these key assets the organization has.

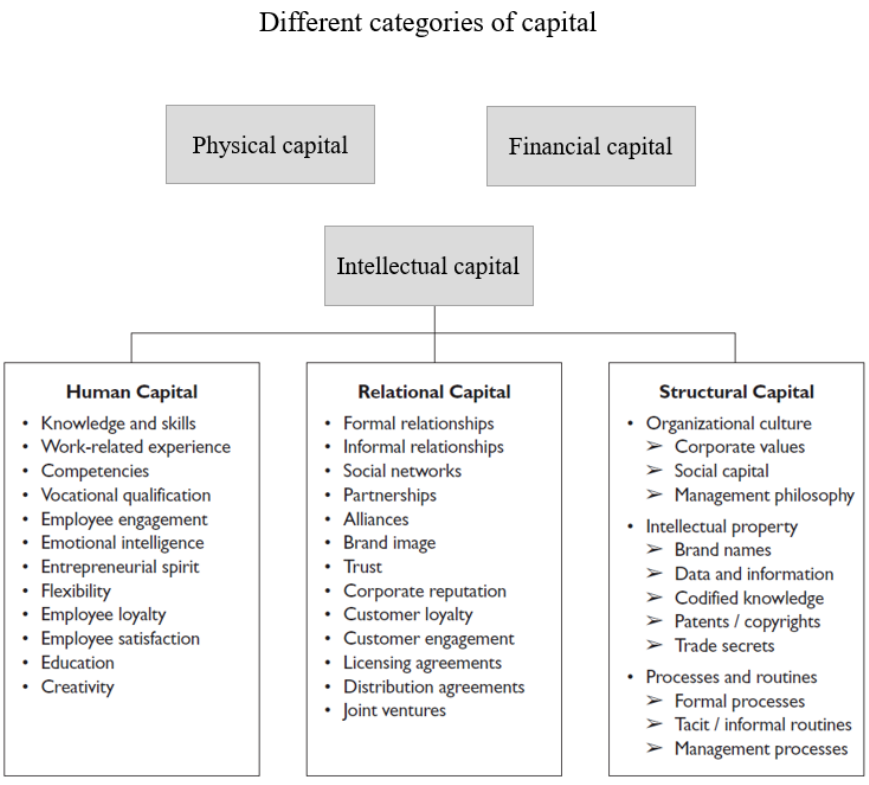


Figure 5. Categorization of capital and intellectual capital (Marr 2008)

2.4. Knowledge protection

Knowledge protection is one of the identified ten knowledge management practices, however its not described in more detail (Inkinen et al. 2015). Also Husted, Michailova & Olander (2013, 6) indicate that there is very little research on the knowledge sharing, protection and on the organizational governance around it. Also, the practices on how organizations implement "knowledge protection strategies" vary widely based on the organization's characteristics and capabilities (de Faria & Sofka 2010, 956). The importance for knowledge protection is increasing as organizations have their operations spread in multiple geographical areas and when they participate on inter-organizational R&D activities (Husted et al. 2013). Hurmerlinna-Laukkanen (2011, 304) emphasizes the need to focus on the knowledge protection when working with knowledge intensive innovations.

Knowledge protection can be divided into formal and informal (Päällysaho & Kuusisto 2011). Hurmelinna-Laukkanen (2011, 305) further define that the knowledge protection can be built on "institutional and formal or more informal mechanisms". This is indicating that the organization as a legal entity can be active in the protection of its valuable assets. The formal mechanisms of protection comprise of legal and regulatory based methods, such as intellectual property rights, contracts and labor legislation (Olander, Hurmelinna-Laukkanen, Vanhala & Blomqvist 2019, 5). Päällysaho & Kuusisto (2008) introduce the concept of formal, semi-formal and informal protection methods for protecting the intellectual capital -figure 6.

Examples of proactive ways for organization to protect its intellectual capital are: patents, copyrights, trademarks and trade secrets (de Faria & Sofka, 2010, 956, Hurmelinna & Puumalainen 2007, 96). There is also criticism on this approach or the adequacy of it, as very limited number of all innovations end up as patents or trademarks, plus the use of such controls may be costly and difficult (de Faria & Sofka 2010, Hurmelinna-Laukkanen 2011). Also, the fact that much of the knowledge of an organization is tacit, its protection with the ways described above may be difficult (de Faria & Sofka 2010, 958).

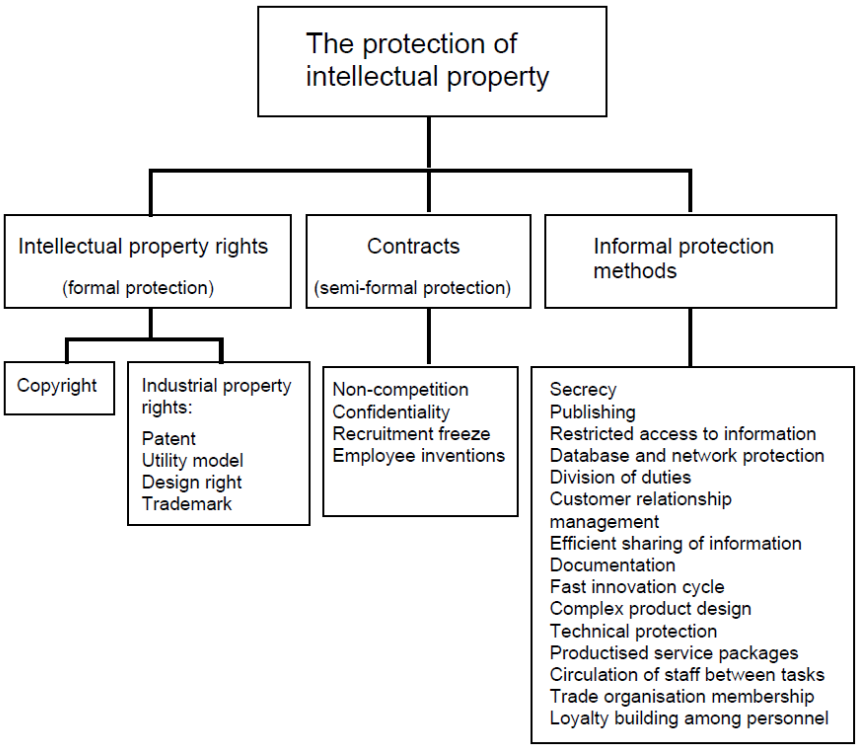


Figure 6. Protection methods for protecting intellectual capital (Päällysaho & Kuusisto 2008,7).

As the legal and contractual mechanisms do not provide sufficient coverage for knowledge protection, other methods such as human-resource management practices (HRM) (Olander et al. 2019, 5) and controlling of knowledge flows (Hurmelinna-Laukkanen 2011, 313) can be used. What is noticeable, is the lack of connection to typical security controls which are typically presented in the context of information security. The rate examples are the technical protection (Päällysaho & Kuusisto 2008) or the concealment (Hurmerinta-Laukkanen & Puumalainen 2007) when done by using technical means.

2.5. Information security

Security as a generic term is “the quality of state of being secure -to be free from danger” (Whitman & Mattord 2009, 8). It’s the activity of protecting organization and its assets from risks and intentionally caused damage. Security is a fundamental part of every organization’s operation´s, but the way and how security is understood and how it is managed varies

remarkably (Ekelhart, Fenz, Klemen & Weippl 2007, 1). Information Security is activity where the confidentiality, integrity and availability of information is protected from attacks. The use of the term "security" indicates that there is an enemy which is jeopardizing the asset. (Pieters 2011, 327.) Information security is typically defined by using the CIA triad, where the C presents confidentiality, I integrity and A availability (Lundgren & Möller 2019, Von Solms & Von Solms 2018, 4). There is also some criticism on this definition as it is not seen very practical of well defined (Andersson 2003).

As pointed in chapter 2.1 the knowledge protection was not fully addressing the security aspect of knowledge protection, rather it related more to sharing and innovation (Inkinen 2016, 234) and open innovation (Inkinen et al. 2015, 434). In chapter 2.4. it is proven that the knowledge protection does not fully address all the protection possibilities or techniques. There is a common consensus that organization needs to protect its key assets, but how the protection activities are executed and managed is a different thing.

The activity focusing to the protection of information and on preventing unauthorized access to it is information security (Kazemi 2018, 1). Kazemi also emphasizes that information security is also about protecting information systems and that the terms information security and computer security are used interchangeably (2018, 1).

In research, Information Security is described as the part of computer science which focus on "how to protect information systems form malicious users" (Pieters 2011, 326). This term indicates that the subject of protection are the information systems. This was also the starting point as in the early days of information security, when the focus was the protection of physical locations, hardware and software from threats (Whitman & Mattord 2009, 3). To ensure a common understanding on security needs and on those threats against the assets a categorization of loss types has been used. The categorization includes three types of loss events: loss of integrity, loss of availability of services and loss of confidentiality. (Lane 1985, 1)

When organizations have realized the importance of intellectual assets and on the role these have when generating sustainable competitive advantage (Barney 1991) the focus on the protection of information has risen. This especially together with the rapid technological advancements and changes in the operating environment created a demand for information security (Singh, Gupta & Ojha 2014, 644) and moved the focus towards the protection of information rather than just focusing on the IT infrastructure (Gerber & von Soms 2004, 17).

The commonly used way to define information security is to use the so-called CIA triad. It uses three attributes, where the C presents confidentiality, I integrity and A availability (Lundgren & Möller 2019, Von Solms & Von Solms 2018, 4). In this definition, the word "security" has a specific meaning. It indicates that there is an enemy which is jeopardizing the information asset (Pieters 2011, 327). The discussion on information security would be unfounded if the discussion would only focus purely to the information or IT / computer security as the reality is, that information is gathered, processed, transmitted and stored by using various IT solutions. To address this the US Committee on National Security Systems (CNSS) defines information security as the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information (CNSS 2022, 106). So, in comprehensive approach information security should include both IT asset and information asset perspectives. Whitman & Mattord (2009, 8-9) further develop the concept based on the CNSS definition and structure the components of information security to four areas. These are network security, computer and data security, policy and management of information security. Figure 7– components of information security by Whitman & Mattord (2009).

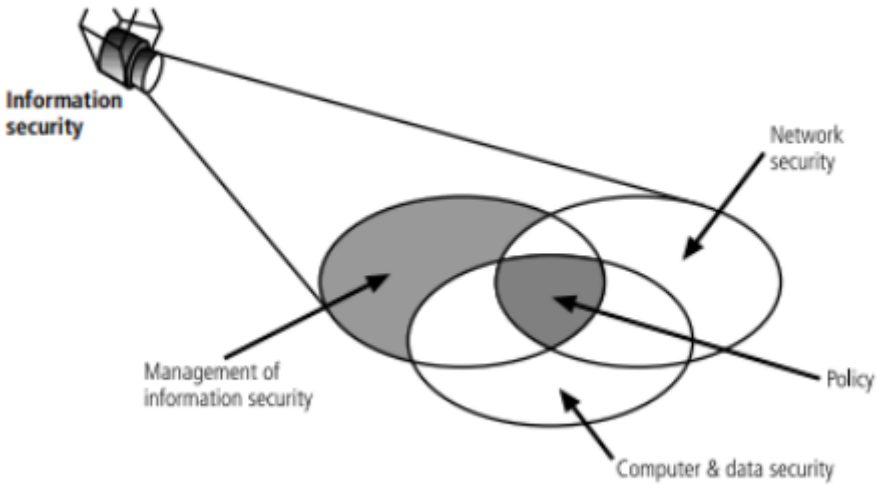


Figure 7. Components of Information Security (Whitman & Mattord 2009)

In conclusion, information security includes those activities, which the holder of the information and IT assets, is running to prevent an unauthorized and hostile operator for getting access to these assets, to manipulate those and to make sure that the information and IT assets are available when needed. There is also some criticism on this definition as it is not seen very practical of well defined (Andersson 2003). Another driver for the discussion is

the argument, that organization have made large investments in their IT systems and that these systems need to be protected from various kind of threats and malicious acts. Examples of these other kind of threats are communications failure or employee mistake and external disasters such as flood or lightning. (Gerber & von Solms 2005, 17.) The need to further explore and to develop the definition has extended it to include also non-repudiation, accountability, authenticity and reliability of information resources (von Solms & van Niekerk 2013, 99). In conclusion, the information security discipline has evolved from pure IT component security towards the protection of organizations IT investments and information assets. The information security domain has grown broader and at the same time it has become extensive and complex domain (von Solms & van Niekerk 2013, 97). This development has also triggered the interest of the different communities, national governments, standards organizations, think tanks, academics and commentators to involve and to provide their inputs via different initiatives (Thompson, Ryan, Slay, Jill & McLucas 2016, 54, 55). All these factors are causing the information security to be a relatively nascent subject topic.

2.6. Cybersecurity

Cyber security is relatively new concept, it become to the wider awareness and use only after 2008 (Xu, Yung & Wang 2021, 263). The term cybersecurity has been absorbed into and it is used in context or interchangeably with the term information security (von Solms & Niekerk 2013, 97). If there are challenges with the emerging and vague definition of information security, then it won´t become any easier with the introduction of another parallel term. Cybersecurity has become a “fundamental issue” which affects many parties from individuals to societies and even national security (Schatz, Bashroush & Wall, 2017, 53, Renaurd, von Solms & von Solms 2019, 622-623). The changing, developing and increasingly more technology dependent society is prone to cyber security incidents and more and more people will be impacted by them (Jones, Collins, Levordashka, Muir & Joinson 2019, 1). The clear definition and understanding of the concept will help people to understanding the threats and by so to plan and to implement proper countermeasures (Iqbal & Anwar 2020, 687). Strupczewski (2021, 135) has approached the definition of cyber security via the definition of cyber risk:

> *"Cyber risk is an operational risk associated with performance of activities in the cyberspace, threatening information assets, ICT resources and technological assets, which may cause material damage to tangible and intangible assets of an organisation, business interruption or reputational harm. The term 'cyber risk' also includes physical threats to the ICT resources within organisation."*

To emphasize the fact, that cyber risks are not just and only something happening in the digital environment and with bits or code the term cyber is combined with the term physical, here cyber-physical (NIST 2013). The motivation for this, is to point-out how everything is connected and how humans and different systems interact with each other and with the physical world around us (Rajkumar, Lee, Sha, Stankovic 2010) and for example in Karangelos & Wehenkel (2022). Harel, Gal & Elovici (2017, 2) approach the same purpose by using the concept Cyber Phenomenon to describe how everything is based on computers and on how everything is connected.

There appears to be a gap between the practitioners and researchers, as the terminology has been implemented to use, even it appears to lack the clear and commonly understood terms. The nascent and developing vocabulary together with insufficient definition and imprudent use of use of term cyber security will cause ambiguity (Schatz, Bashroush & Wall 2017, 54-55). The existing definitions on cyber security focus on hardware and software and fail to focus on human elements in the context of cyber security (Cains, Flora, Taber, King & Henshel 2021, 3). Even there has been a genuine attempt to create a universal and commonly used definition the definitions still appear to be relatively complex and subjective on the operator or the definition. The term has been a subject of academic literature, but it is still used broadly and broadly. (Craigen, Diakun-Thibault & Purse 2014, 13.) Cains et al. (2021, 6-7) investigated the existing definitions and used an expert elicitation to compose a more comprehensive definition for cyber security.

> *"--the iterative process of maintaining quantifiable levels of cyber system dependability and control over verifiable data provenance, confidentiality, integrity, and accessibility (CIA) via comprehensive system awareness, human factor and effects characterization, resource protection and management, accurate intrusion detection, threat prediction and prevention, resilient system functionality, and systemic solutions in a cost-limited environment of sociotechnical interactions between diverse dimensions and factors, despite evolving security standards and variations in security competence."*

The clear and more defining meaning is needed and the demand from various stakeholder groups, including organization management like board of directors (BoD) will drive the use of unambiguous and accurate terminology (Renaurd, von Solms & Von Solms 2019, 622-623). Schatz et. al (2017, 66) clarify the concept by adding the dimensions of subject, where and defining the object to be protected (data and assets).

> *"The approach and actions associated with security risk management processes followed by organizations and states to protect confidentiality, integrity and availability of data and assets used in cyber space. The concept includes guidelines, policies and collections of safeguards, technologies, tools and training to provide the best protection for the state of the cyber environment and its users."*

In essence, cybersecurity addresses and focuses to the fact, that all users, devices, computers and systems are interconnected, thus part of our physical world and environment. The concept of cybersecurity focuses on protecting the users, data & information and different type of assets in this environment.

2.7. Management of information and cybersecurity

Information and cybersecurity management is an area which is focusing on the management of organizations information and cybersecurity operations so, that they support and contribute to the overall purpose and targets of the organization (Whitman & Mattord 2009). Researchers see that management´s role in information security is increasing (Soomro, Shah & Ahmed 2016, 220). The importance on information security management has not always been recognized. There are multiple reasons where one of the dominating ones, is the fact that information security and the related literature has mainly focused on technological issues, and to a lesser extent on strategies, security standards and policies (Perez-Gonzáles, Preciado, Solana-Gonzales 2019, 1263).

The reasoning and rationale on this can be found from the development of information security in an organization. Nnolim (2007) describes the development of the purpose and target of information security as presented in figure 8. The development has started from the protection of large computer centers. Gradually, as the systems have moved towards distributed model and as the importance of connectivity has increased on protecting IT systems and

networks. And when business has implemented more and more business applications, the focus has moved on business information systems.

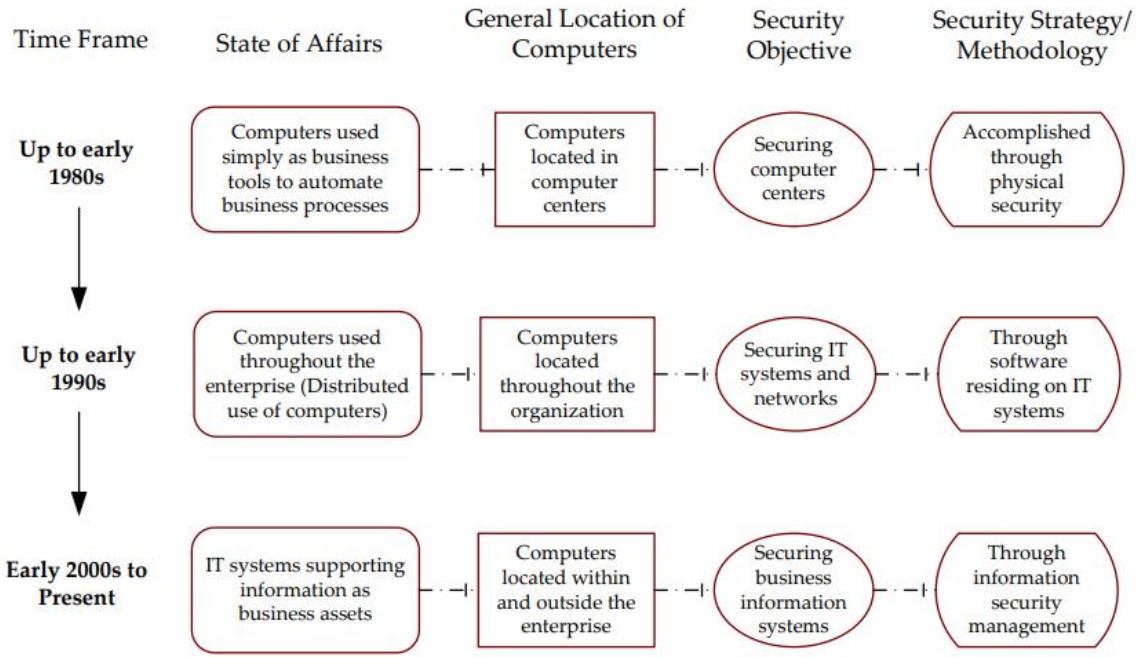


Figure 8 – Development of the scope of security Management (Nnolim 2007, developed from Vermeulen and von Solms 2002).

The basis of information security and information security management is in the protection of information technology assets (Singh, Gupta & Ojha 2013, 644). The protection of these assets is becoming a broader topic as the information security is not only about technology it also encompasses processes, and people (Veiga & Eloff 2007, 361). One driver also affecting on the development and on the need of information security are security incidents. Security incidents which relate to information systems or networks may cause major impact to the subject organization. Therefore, organizations need to be prepared to prevent incidents and to handle incident response when preventive methods are not sufficient. (Baskerville, Spagnoletti & Kim 2014.) von Solms & Niekerk (2010, 478) also stress the importance of personnel knowing the "good information security practice" and the need for having the adequate information security knowledge in the organization.

The concept of information security management (ISM) are those management activities organization does to protect its information assets. Information security management "comprises the set of activities involved in configuring resources in order to meet the information security needs of an organization" (Singh, Gupta & Ojha 2013, 645). In fact, information management system should be seen as a part of the management systems, it is the structured way, on how the organization is managing the protection of its information assets (Arkhipova 2022, 26, Antoniou 2018, 2). Von Solms (2000) describes the development of information security in three waves. The first wave was the technical view and focus on information security (as described earlier). The second wave is management. The recognition on the need for having formal and structured management of information security. The second wave brought the dedicated information security managers, policies and procedures to organizations. As the importance of information security increased the need to be able to formally measure the effectiveness of the information security management the third wave arrived. The third wave brought the need for standardization, certifications, security awareness and the measuring of the effectiveness of information security activities. Standards are tools, which the organization can use to ensure that their information and cybersecurity practices are comprehensive (Taherdoost 2022, 1-2, Silva, Hsu, Backhouse & McDonnell 2016, 68). Also, the increasing need to standardize and to be able to evaluate and to compare the management of information security level with peers, business partners and other organizations has fostered the implementation of different information / cybersecurity standards (von Solms & von Solms 2001, 308). Following and committing into the relevant standards can also prove that the organization is committed to "secure business practices" (Siponen & Willison 2009, 267). When the concept of information security management and it´s positioning in an organizational frame is relatively new, these standards may provide aid, support and boost to the development of it. There is a variety of standards which can be used, an organization looking for a suitable standard frame should evaluate multiple aspects, like the industry it is on, the size and geography of its business activities etc. (Taherdoost 2022).

Despite the partly overlapping obscure definitions on information and cybersecurity, the subjects link together in the larger organizational perspective. The management of information and cybersecurity can be combined to the same notion. The information and cybersecurity do relate to the same purpose of protecting the assets organization existing in a different form (Von Solms & von Niekerk (2013, 101) presented in figure 9.

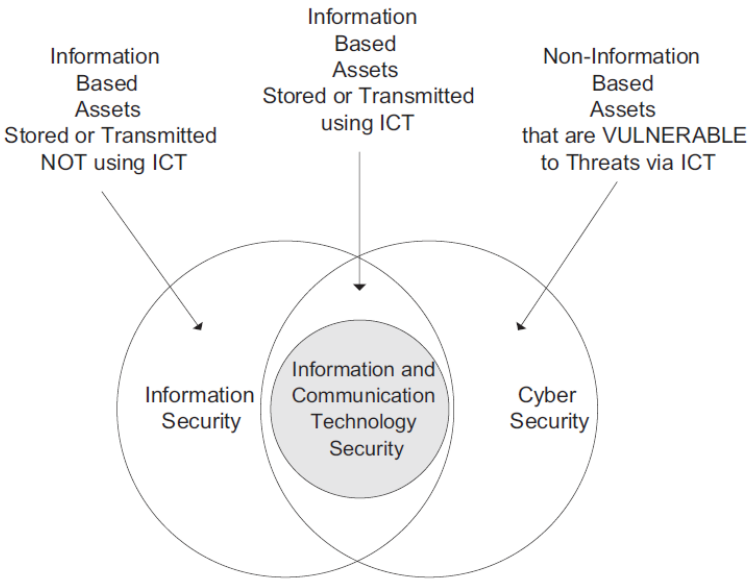


Figure 9. The relationship between information and cybersecurity (von Solms & von Niekerk 2013).

2.8. The role information and cybersecurity in protection of organizational assets

In earlier chapters 2.1 to 2.3 it was proven that the intellectual capital is the most valuable resource of an organization. For example, Barney and Porter prove that the intangible resources of a firm, allow the creation of sustained competitive advantage and also the management and mitigation of "external threats and avoiding internal weaknesses" (Barney 1991, 99). Information security, as described in chaper 2.4 is activity, which aims for protecting organizations information assets and the related information technology assets. Cybersecurity (chapter 2.5) relates to activities which the organization does to protect its assets and operations against threats and risks raising from the globally connected operating environment. Information and cybersecurity management is hereby those activities, devoted by the management of the organization, to protect its business-critical assets, business capabilities and operations against security threats and risks.

3. Methodology

The methodology part of the work describes the research process in detail and provides information and visibility on how the research question(s) are approached and how the research work was conducted. In methodology part, the execution and process of the systematic literature review is demonstrated. This includes the used search words, the selection of sources for materials, the screening and the selection process of materials.

3.1. Purpose for the research

The previous research prove that organizations are dependent on data, information, and knowledge to be able to be successful and to create sustainable competitive advantage. Research and literature show that this intellectual capital is the most valuable assets for an organization. To safeguard organization and its key assets, it must also focus on protecting its intellectual capital. When intellectual capital is nonfinancial and intangible in its nature and therefore, they are difficult to identify, measure and manage (Martín-de-Castro et. al 2011, 649) then how will the organization handle this need?

The concepts of information and cybersecurity include a promise and supposition that they are activities which aim for protecting the organization and its valuable assets. But what is the relationship between the research on information and cybersecurity and intellectual capital? Does the intellectual capital related knowledge management and information & cybersecurity management? Are the concepts and background the same, does these disciplines relate to each other and do they supplement each other's? Based on the theoretical underpinnings, knowledge management deals with the organization´s most valuable knowledge resources, whereas the knowledge management and information & cybersecurity use same terms and they appear to be connected. However, both disciplines are relatively emergent and there is also criticism on the vague terminology relating to information and cybersecurity.

Purpose for this thesis is to evaluate how the protection of intellectual capital is presented in knowledge management and in information and cybersecurity related research.

3.2. Research methodology and research process

In the research approach part, the research strategy, process and selected methods are explained. The purpose for the study is to understand the link between the management of information and cyber security and the intellectual capital in research. As addressed earlier, information is a strategic asset which needs to be protected to ensure the success of the organization. The study was performed as a systematic literature research (SLR) to research how the two disciplines are approaching the intellectual capital topic. As demonstrated in paragraph 1.1 both concepts (intellectual capital and information & cyber security) are relatively new and the related research has developed during the same period, the research covers a long time period to evaluate if consistency can be identified.

3.3. Systematic literature review (SLR)

To achieve the objective and to answer to the research question the study is performed as a systematic literature review (SLR). As the systematic literature review focuses on the existing research and literature relevant for the research question, it provided a practical way for searching the answers (Aveyard, 2014, 2, Hirsijärvi et al. 1997). A systematic literature review was selected as the research method as it provides view on the existing research and materials on the subject. This can be very useful also in situations where the materials and evidence are very scattered. Systematic literature review can also be easily replicated to validate or to compare the results later. The research method can also be justified due the relatively emergent nature of the topics. (Lame 2019, 1633-1634)

Systematic literature review is a precise and reproducible method, which is used to identify, evaluate and to condense existing research and source materials (Fink 2005, 3). The purpose of SLR is to search for the answer to the specific research question and to project the existing research of the topic (Hirsijärvi, Remes and Sajavaara 1997, 108-109, Lame 2019, 1633). The literature review must be performed systematically and reported precisely. Also, the key concepts used in search must be defined, to ensure that the larger and more complex meanings can be understood by the reader (Hirsijärvi et al. 1997, 240). Elementary part of the SLR process is the identification, screening and selection of materials. This must be done in

a meticulous way so that all steps and criteria's in the material intake phase are clearly and unequivocally presented and documented. Purpose for it is to evidence the process on how the selected materials included in the review were screened, selected, extracted and how the results are reported. (Borrego, Fosters & Froyd 2014, PRISMA 2020).

Figure 10 – the five phases of systematic literature review (Borrego et al. 2014).

Borrego et al. (2014) present the systematic literature review and identify five phases in it. The first phase is to formulate and to establish the particular research questions which the research is addressing. The second phase is about identifying relevant sources from where the materials for the research and review could be found. In the third phase the precise key-words, attributes and other rules are defined and pinned to the search and material intake process. The fourth phase is to perform the actual review and analysis of the discovered materials. The fourth phase also includes the summary of results on reviewed articles. In the fifth phase of the review the review summary and synthesis are prepared. The systematic literature review process and its five steps are presented in figure 10.

3.4. Search strategy and source for research materials

The selection of sources for information for the research is very important and one should pay attention on the credibility of the source and the material (Costin, Ionescu & Gherghina 2020). The use of specific and specialized databases for searching the source material for the research is useful and efficient (Hirsjärvi et al. 1997, 86). In this research the purpose was to evaluate how the information and cybersecurity related research relates to knowledge management and to concept of intellectual capital. To achieve this, a comprehensive range of materials was needed. The existing scientific research article databases fulfill this requirement and need very well. There are many research article databases which can be used for this purpose (Visser, Eck & Waltman 2021).

Some of the most used research article databases are Web of Science and Scopus. There are also new databases like Dimensions which provide comprehensive amount of different scientific journals. (Singh, Singh, Karmakar, Leta & Mayr 2021, 12). From pure number of publication records the Dimensions looks attractive -table 2.

Table 1. Number of journals and publication records indexed in Web of Science, Scopus and Dimensions (Singh et al. 2021, 11).

	Web of Science[a]	Scopus	Dimensions
No of journals indexed	13,610*	40,385**	77,471***
Approximate number of publication records (article + review) indexed in the three databases (2010–18)	13,218,007	18,058,418	28,130,484

[a]Includes SCIE (9397 journals), SSCI (3497 journals), AHCI (1843 journals)

*Updated June 2020

**Updated June 2020

***Updated May 2020

To evaluate the most suitable and relevant database a basic key word search was performed to all three databases (Web of Science, Scopus and Dimensions). These databases were selected as they focus on scholarly material, and they include proper search functions. For example, Google Scholar was excluded as the search functionalities are limited and by using

the other dedicated research article databases the access to the original research papers is easier.

The evaluation search was a search the search with key words “Intellectual Capital” AND “Information Security”. The search was done against the abstracts. The search was limited from records published between years 2000 to year 2022. The results from this search were (comparison run 9th April 2022):

- Scopus 52 search results
- Web of Science 41 search results
- Dimensions 10 search results

Based on these qualification criteria’s the search was done by using Scopus database.

3.5. Database search and search attributes

As described in earlier section Scopus was selected as the database for primary search. The database holds millions of articles and offers multiple ways and combinations to scope the search the relevant source materials, like key words, targeting the keyword search to certain database elements of article name, abstract, key words (Hirsjärvi et al. 1997, 87-90).

The search from Scopus database was done by using following rules and attributes:

- Keywords: “information security management”, “cyber security management” AND “cybersecurity management”
- Search done against: Article title, abstract, keywords
- Range from 2000 to 2022 (search date 9th April 2022)

Search results with the search total 1555 results (figure 16)

Note: The research work was started in April 2022 and therefore the number of published research articles from 2022 was limited as shown in figure 11.

3.6. Research article intake and exclusion

When the primary selection of source materials has been done with a database search, the search results may not all be relevant for the research. Therefore, an article intake and exclusion phase must be completed to ensure that the selected materials are relevant from the viewpoint of the research question (Borrego et al. 2014, 54).

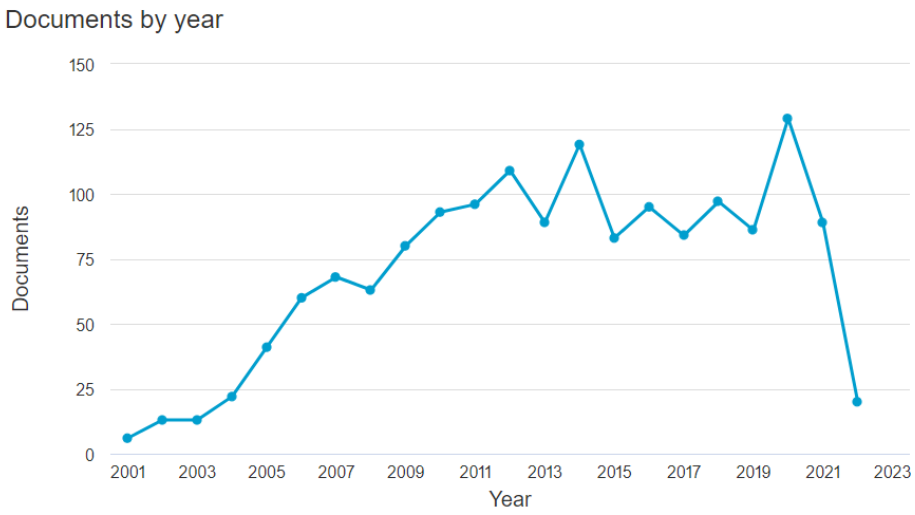


Figure 11. Number of search results on key words

The thesis is about the concept of intellectual capital both in knowledge management and in the management of information and cyber security. Therefore, the selected articles must be relevant for the management aspect and on the concept of intellectual capital.

Intake criteria:	Article is about the definition or classification of information and about the protection of it in a corporate context.
Exclusion criteria:	Article covers only limited aspect of information security (like technical questions for instance data encryption, user awareness or regulatory aspects like personal data protection & privacy). Also work related to mathematical modelling without any relation to information classification or definitions will be excluded.

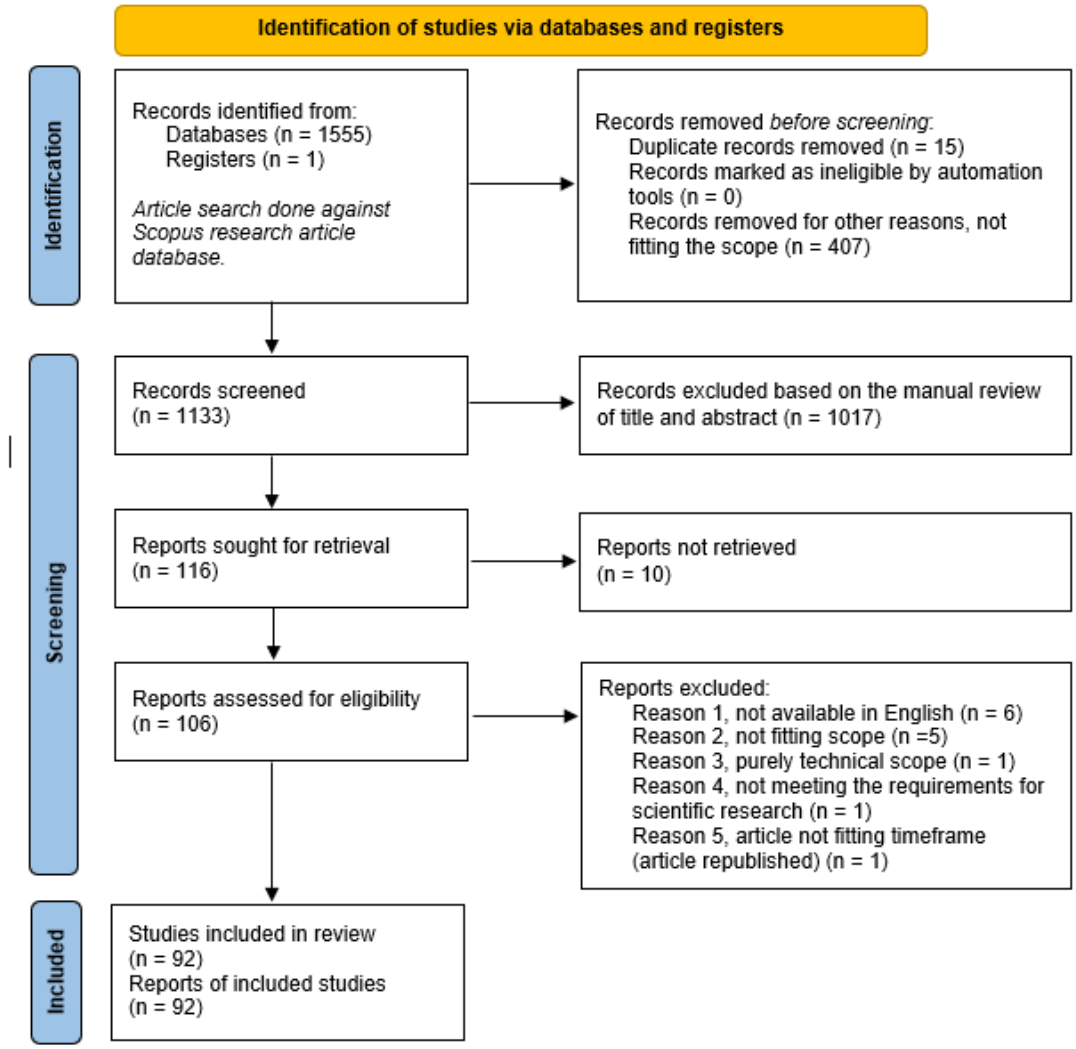
The material intake, selection and screening process are described by following the PRISMA model (Page, McKenzie, Bossuyt, Boutron, Hoffmann, Mulrow et al. 2020). The primary search database was selected to be Scopus, as it includes materials from multiple research article databases. From Scopus it was possible to conduct a search against different attributes and elements of research articles. The first phase of the literature review was done against the data available in Scopus database. After the initial screening of the materials the original research articles were acquired from available sources. The process follows the five steps described by Borrego et al. (2014). The process and the selection of materials is presented and broken down in table 2.

3.7. The practical research material intake and screening process

The previous chapter described the theoretical model and selected research method selection. As the research and review process has included both database searches and manual work, the combined process is described here. The practical process is structured in the five-step model presented by Borrego et al. (2014).

The selected source which was identified as the source for the required research materials was Scopus research article database (ref. Borreigo et al. 2014 phase 2). The identification of the plausible materials for the systematic literature review was done by using the search functionalities available in the Scopus database search. In the search, the defined key words were used, as described in chapter 3.4. To achieve sufficient coverage, the search was extended to the article title, key words and abstract. All this information was available via Scopus database and search functionalities. The search results (described in table 4) were extracted to Microsoft Excel spreadsheet named “Articles – master (Scopus).xlsx”.

Table 2– Description of the material selection process and results (PRIMA)



From the identification phase, the selected potential and relevant sources were screened in the phase 3 (Borreigo et al. 2014). This was done by screening the article subject and scope via detailed evaluation of the article topic and key words and the abstract of it. If the article was appearing to be relevant from the research question perspective and if it did not fall under the exclusion triggers it was included to the systematic literature review. If the object was not identified relevant or it felt under the exclusion trigger it was excluded. The inventory and status of this screening work was maintained in Excel spreadsheet named “Articles scanning - phase 2.xlsx”. This spreadsheet was the extraction from the potential works tagged in the “Articles – master (Scopus).xlsx” spreadsheet. In this spreadsheet all the

selected and included articles were numbered with a unique identifying number. This number is then used later in this report in the results and analysis part to indicate the source.

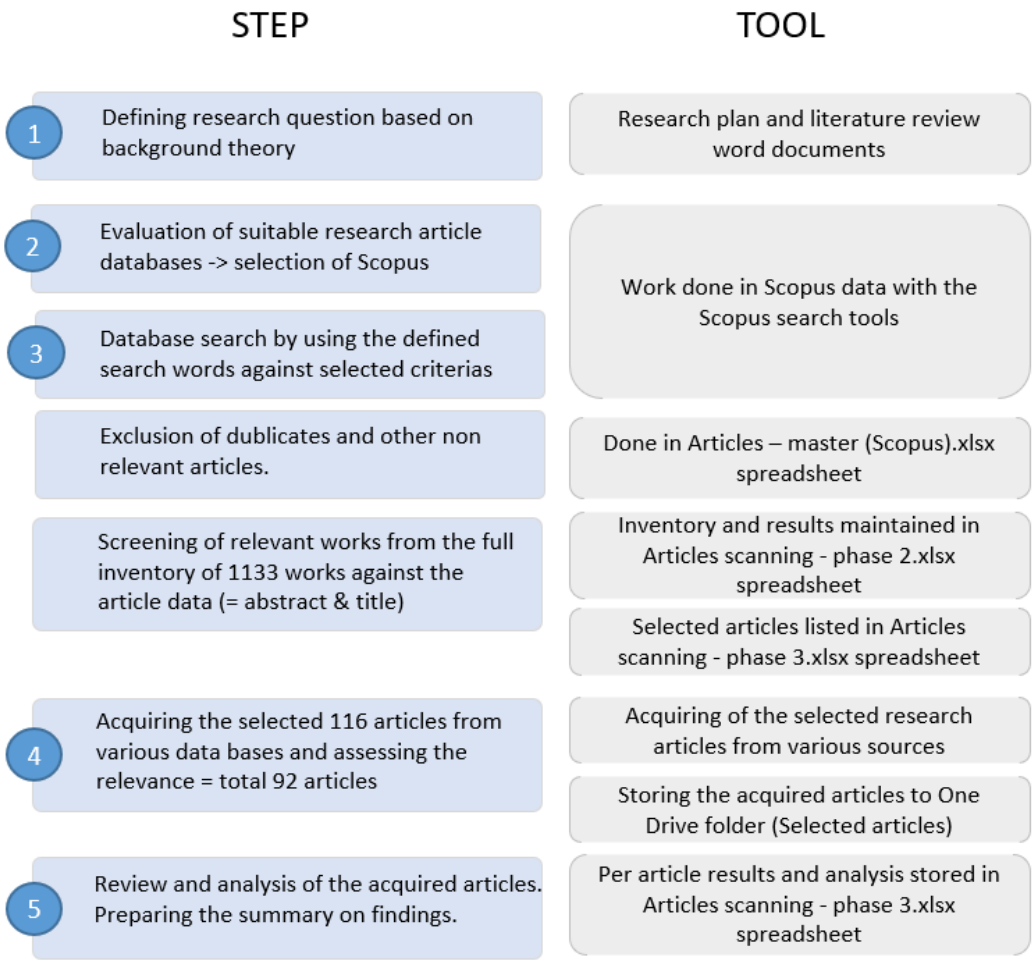


Figure 12. Research process steps and the used tools (based Borrego et al. 2014).

For the phase 4 (Borreigo et al. 2014) all the items listed in the "article scanning - phase 2.xlsx" spreadsheet was acquired and downloaded for the review. In this phase some of the articles were excluded as these are not available free of charge, or the original article was in other language than English (as the abstracts for some works are in English even the original work is written in other language). Also, some works was excluded as the content turned out to be out of the scope or otherwise meeting the exclusion trigger. The results from the detailed analysis and review were gathered to "Articles scanning - phase 3 (analysis).xlsx" spreadsheet. The use of Excel spreadsheet allowed the easy creation of categorization and calculation models needed for the summary and synthesis in phase 5 (Borreigo et al. 2014).

The categorization, statistics and references to articles were done based on the numbering and data categories and validation created in this Excel spreadsheet. The steps and tools used in the research process are presented in figure 12.

4. Results and analysis

4.1. Summary of key results and findings

In this thesis the research layout seeks the answer to the question on how the resource-based view and the protection of intellectual capital is present in information and cybersecurity management related research. The research was performed as a systematic literature review on information and cyber security management related research done between 2010 and 2022.

Intellectual capital and knowledge are proven to be the most valuable resource for organization (Kianto 2007, 343). With the intellectual capital the organization has, it can create sustainable competitive advantages and create success (Marr 2008, 3). The information and cyber security management are a function, which aims to protect the important and valuable information of an organization (von Solms & Niekerk 2013, 99). As these functions and disciplines appear to be closely related, one would assume that the key concepts and theories would be linked and that the organizations most valuable assets would be in the scope of the information and cyber security activities.

The key findings and results of this study are

- The resource-based view and information and cyber security management are not related. The information and cyber security related research very rarely touch the area of intellectual capital. Based on the systematic literature review the concept of intellectual capital is not considered in the context of information and cyber security management. On rare cases the closest relation can be observed in the use of the term

"intellectual property" (table 3). However, the concept and term are not opened or explained more specifically.

- The information and cybersecurity discipline does not recognize the concept of the hierarchy of information. The use of the concepts information, data, information asset or resource appears to be indefinable. The importance of information or cyber security are justified generally with a statement like "information is the most important asset of an organization" (Martin 2021, Sterbak, Segec & Jurc 2021, Culot, Nassimbeni, Podrecca & Sartor 2021, Grishaeva & Borzov 2020, Diéguez, Bustos & Cares 2020, Khan, Tanwar & Rana 2020, Tsochev & Stankov 2020, Diéguez, Bustos & Cares 2020, Akinyemi, Schatz & Bashroush 2020. Kala Kamdjoug, Nguegang, Fosso & Wamba 2019).

- The information and cyber security discipline appears to be technology centric. Even there are plenty of discussion and work addressing that information security extend outside the purely technical domain, there is still a tendency that the materials focus on the protection of information processing technologies (Kim & Kim 2021, Gill, Zavarsky & Swar 2021, Sterbak, Segec & Jurc 2021, Genchev 2020, Bergström, Karlsson & Åhlfeldt 2020, Brunner 2016, Mir, Wani & Ibrahim 2013).

- Information and cyber security management related research focuses to internal aspects and activities on security. More precisely, the focus on research articles is commonly on defining or modelling of information & cyber risks, in the use of technology or in information and cyber security related international standards (Mirtsch, Blind, Koch & Dudek 2021, Culot, Nassimbeni, Podrecca & Sartor 2021, Fonseca-Herrera, Rojas & Florez 2021, Aleksandrova, Vasiliev & Aleksandrov 2020, Safonova, Lontsikh, Golovina, Elshin, & Koniuchov 2020, Diéguez, Bustos & Cares 2020, Akinyemi, Schatz & Bashroush 2020).

- There was surprisingly little work on business alignment, cross discipline topics or on information (Govender, Kritzinger & Loock 2020, Pérez-González, Preciado & Solana-Gonzalez 2020, Luma & Abazi 2019) or cyber security leadership (Da Silva 2022).

4.2. Intellectual capital and security related research

The material identification and intake for the research was done by using the selected research article database search. The search with the selected key words supplied an inventory of 1555 potential research articles. These identified articles were screened based on their title and abstract. It became noticeably clear already in this phase, that the concepts "information security management" and "cybersecurity management" are used very widely. These concepts are used in descriptive way to cover almost any topic in the field of information and cyber security.

Olijnyk (2015) completed a study on the information security related research. Based on it, a larger activity on information security related research has started after 1994. This is supported by the data gathered for this research from Scopus research article database. Figure 13 shows the number of research articles found from Scopus with the search term *information protection*.

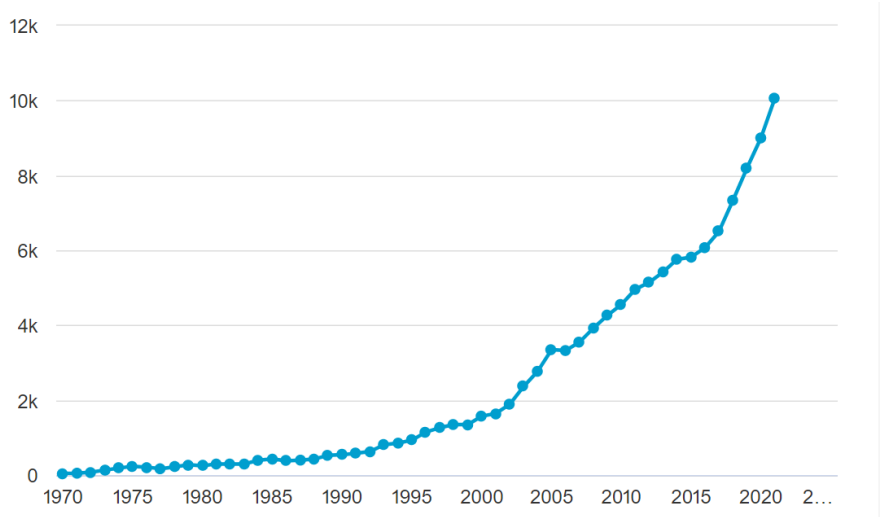


Figure 13. Research articles in Scopus database with key term information protection.

Equally by using the search term *information security* the search results follow the same order, as shown in figure 14. The concept of cybersecurity is also relatively new, the concept has become more commonly used and recognized only after 2008 (Xu et al. 2021, 263). This is supported by data in Scopus research article database show in figure 15.

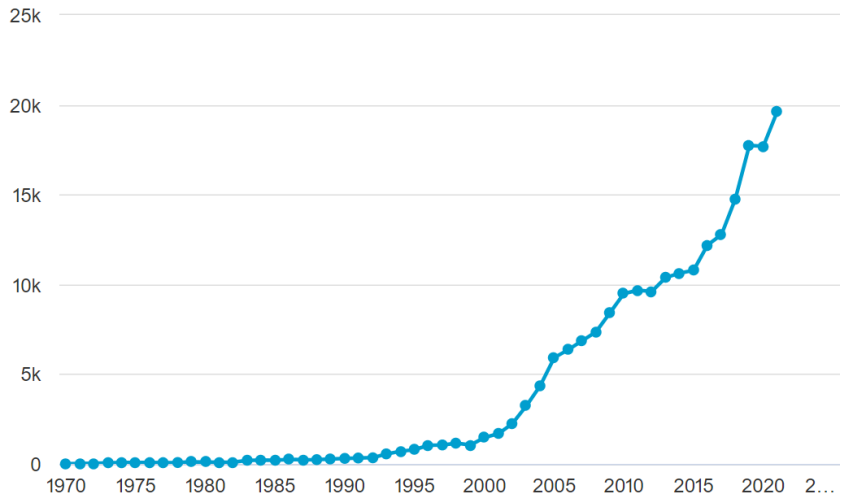


Figure 14. Research articles in Scopus database with key term information security.

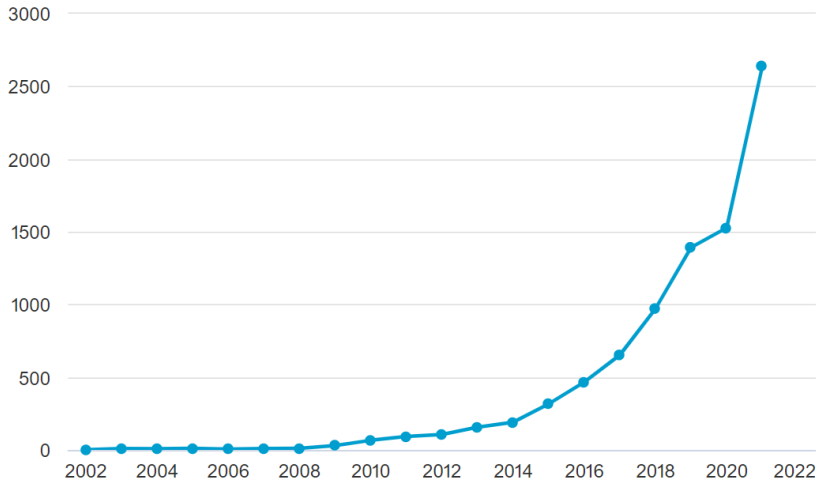


Figure 15. Research articles in Scopus database with key term cybersecurity and with cyber AND security.

In this research the link between the resource-based view of the firm, intellectual capital and information and cyber security are reviewed. This appears to be very unknown and unexplored territory as there appears to be very little research covering both these domains. The number of research articles relating to information security and intellectual capital is presented in figure 16 and the number of papers covering both the information security and firm resources are presented in figure 17.

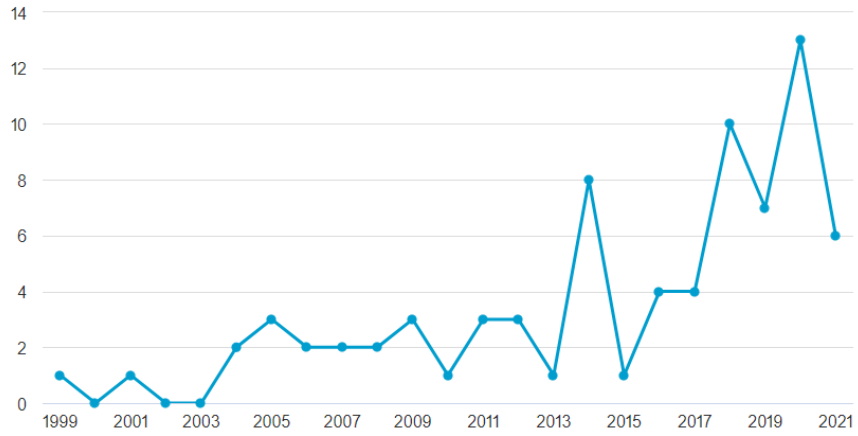


Figure 16. Research articles in Scopus database with key term information security AND intellectual capital.

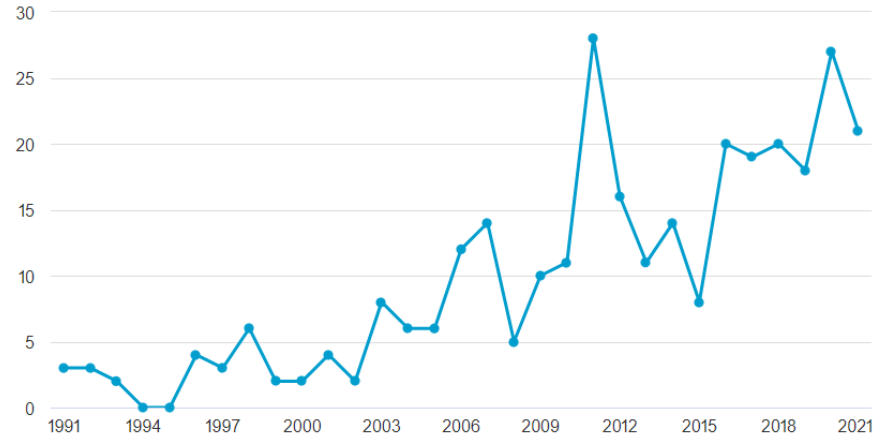


Figure 17. Research articles in Scopus database with key term information security AND firm resources.

4.3. Selected research articles

After the screening of the identified 1555 articles was done, an inventory of 116 articles was selected. The initial selection was done based on the information which was available in Scopus research article database (title, key words, abstract). For the screening phase the selected articles were needed to be acquired. The selected research articles are published and available in various sources. Some of the articles are part of a book or set of conference papers. This adds the difficulty to find the original document. In addition, some of the

selected articles were not found or available, or these were not available in English and therefore excluded. In total 24 articles from the inventory of selected articles were either excluded or not found.

The reasons for exclusion are:

- 10 articles were not found
- 6 articles were only available in other language than English
- 5 articles were focusing on a such area (like governmental or healthcare) or into a single country specific topic that it was not relevant for the research question
- 1 article which has a purely technical scope
- 1 article which does not meet the requirements of a scientific research
- 1 article which is re-published and does not fit the timeframe

The selected articles for the literature review were from 2010 to 2022. Figure 18 shows the split of selected research articles per year. The research was started on April 2022 and therefore the number of research articles from that is limited. Otherwise, the selected articles cover the selected time period relatively evenly.

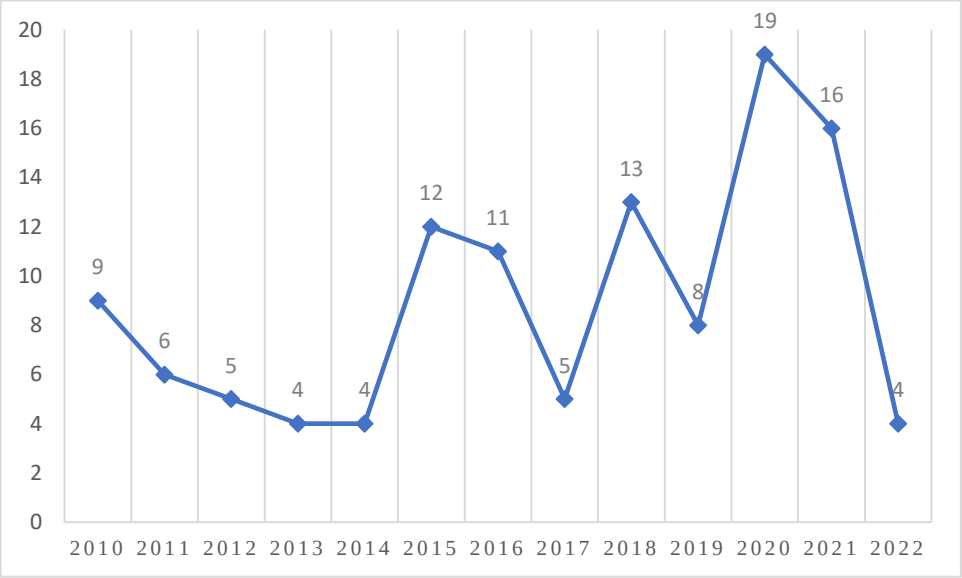


Figure 18. The split of the selected research articles per year

4.4. The relationship between the resource-based view and information and cyber security management do

In the thesis the research question related to the relationship between intellectual capital and information & cyber security management. In the concept of hierarchy of information, the different dimensions relating to information are defined (Aven 2012, Rowey 2005). On dimension of the information hierarchy is knowledge and in related knowledge management theory, one of the identified ten knowledge management practices is knowledge protection (Hussinki et al. 2017, 1597). Olander (2011) has also approached knowledge protection by identifying "formal and informal mechanisms for knowledge protection and sharing". Päällysaho & Kuusisto have also published work on the protection of intellectual property (Päällysaho & Kuusisto 2008 and 2011). This proves that the protection of intellectual capital is an already identified theme. The value of knowledge and respectively the intellectual capital of an organization is recognized. The topic has not been treated in that detail for example in knowledge management as it is seen separate from other strategic knowledge management practices (Hussinki et al. 2017, 1599).

When the protection of intellectual capital is recognized and when the mission of information and cyber security is closely relating to the protection of organizations assets, then the expectation would be that this would also include the intellectual capital. Based on this literature review this appears not to be the case. The results of the literature review prove that information & cybersecurity management do noes do not recognize the concept of intellectual capital or it does not relate or connect to it in any prominent way. From the screened 1555 and selected 116 articles only 4 were using the terminology or concepts relating to the resource-based view or to intellectual capital (Ilvonen, Jussila, Karkkainen, & Päivärinta 2015, Ahmad, Tscherning, Bosua & Scheepers 2015, Delak & Damij 2015, Hassan, Ismail & Maarop 2014). In addition, three works were related to knowledge management from some of the aspects, either terminology or the recognition of the data-information-knowledge-wisdom (DIKW) hierarchy (Zemtsov & Astakhova 2021, Stoll, Felderer & Breu 2013, Aksentijevič, Tijan & Agatič 2011). When comparing these seven works to the entire inventory of works, these stand for only 0,5% of all selected research articles.

4.5. The concept of information hierarchy is not used in information and cyber security management

Information and cyber security are defined as the protection of the confidentiality, integrity and availability of information. In the resource-based view and in the intellectual capital theory there is a concept on information hierarchy. This is described with the use of the DIKW model (Aven 2012, Rowey 2005). This hierarchy does not seem to be used or referenced at all in the information & cybersecurity management related research. The terms data and information are used interchangeably and clearly without any hierarchical structure (Gill, Zavarsky & Swar 2021, Schatz 2021, Antoniou 2018, Naseer, Shanks, Ahmad & Maynard 2016, 2, Sidi, Daud, Ahmad et al. 2017, 1, Hugl 2013, 579). Even these terms are same as in the DIKW model, they are not inherited from it. The use of the intellectual capital related terminology is relatively relaxed and based on the research not systematic in any way or level. In the reviewed articles only in 16 of these the intellectual capital or property was mentioned (table 3). However, the dimensions, terminology or concept did not link to information hierarchy, the reference was more like the use of an individual word without any other indication on bridging the concepts. From the 92 articles reviewed the terminology relating to resource-based view is presented in table 3.

In information and cyber security management related research the DIKW model and concepts are not used. The overall use of the terminology and concepts appear to be very creative but inconsistent not only towards the resource-based view but also with in the information and cyber security research. A common practice seems to be the use of key term, e.g., information in the combination of other descriptive words. For example, the different use of the term information is illustrated in figure 19 (for example in Antoniu 2018, Tu, Yuan, Archer & Connelly 2017, Shamala & Ahmad 2016, Tatar & Krabacak 2012). And for asset in figure 20 (for example in Susukailo, Opirsky & Yaremko 2022, Schatz 2021, Steward 2017, Sidi, Daud & Ahmad et al. 2016, Shameli-Sendi, Aghababaei-Barzegar & Cheriet 2016, Soomro, Shah & Ahmed 2015.

Table 3. The terms used on intellectual capital.

The used term	number of works	Article(s)
intellectual property	9	- Susukailo, Opirsky & Yaremko 2022 - Schatz & Bashroush 2018 - Anttila & Jussila 2018 - Sidi, Daud, Ahmad et al. 2017 - Soomro, Shah & Ahmed 2016 - Warkentin & Mutchler 2014 - Ng, Ahmad & Maynard 2014 - Korhonen, Hiekkanen & Mykkänen 2012 - Tatar & Karabacak 2012
Intellectual asset	3	- Naseer, Shanks, Ahmad & Maynard 2016 - Baras, Othman, Ahmad & Ithnin 2015 - Bergström & Åhlfeldt 2014
Knowledge	4	- Fonseca-Herrera, Rojas & Florez 2021 - Shamala, Ahmad 2016 - Agudelo, Bosua, Ahmad & Maynard 2015 - Hugl 2013
Intellectual capital	1	- Aksentijevič, Tijan, Agatič 2011

The description in figures just like in articles don't present any hierarchy. For example, Aksentijevič, Tijan & Agatič (2011) use the terms data -information and knowledge in combination with business strategy, to describe the importance and usage of information. Generally, the information and cyber security management related research appears to use both concepts of data and information (e.g., Haufe, Brandis, Colomo-Palacios & Stantchev 2017, 27).

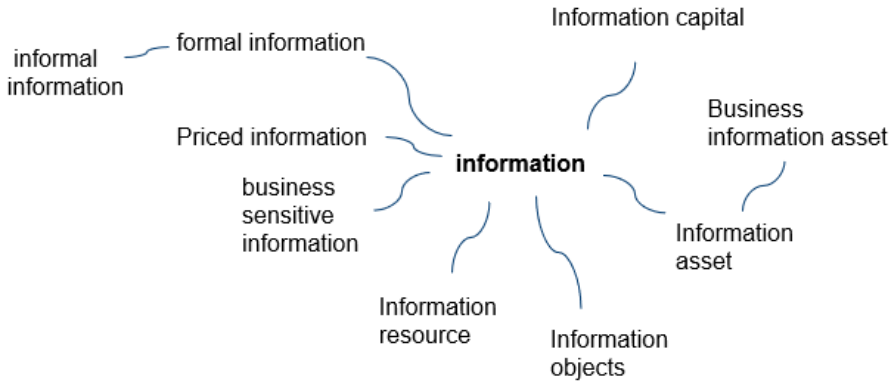


Figure 19. The different concepts on information in reviewed research materials

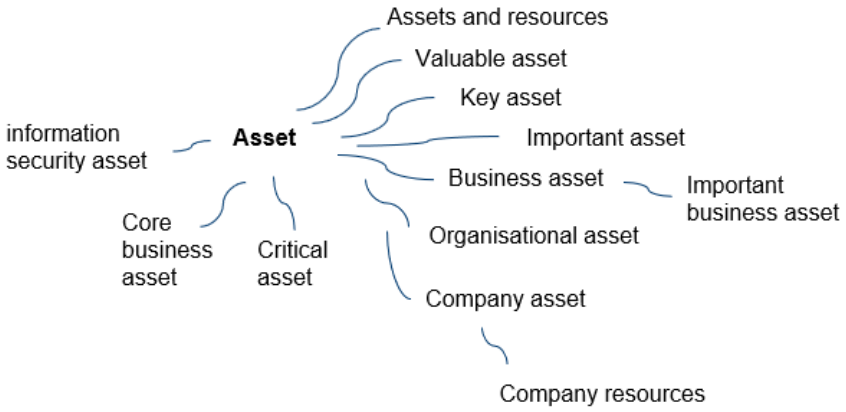


Figure 20. The different concepts on asset in reviewed research materials

4.6. Information and cyber security management is technology centric

Information and cyber security management literature appears to be technology focused. The purpose for the security function is to protect the information processing systems (Martin 2021, Sterbak, Segec & Singh 2021, Douchek, Nedomova, Luc & Novak 2020, Genchev 2020). Also, the concept of information asset (Susukailo, Opirsky & Yaremko 2022, Kim & Kim 2021, Mirtsch, Blind, Koch & Dudek 2021, Wu, Wang, Cheng & Dai 2021) is used with lack of clarity and in relatively relaxed manner. For example, assets are described as "computers, printers, cloud storage, application software" (Sterbak, Segec & Jurc 2021, 381). The concept of information is also seen as something tangible. For example, in Mir,

Wani & Ibrahim (2013) describe that information which is now stored in computers was previously retained in “secure file cabinets”. In Sidi, Daud, Ahmad et al. (2017) “the information resources” are hardware, software and data.

4.7. Information hierarchy and information and cyber security

The scope for information and cyber security appears to be focusing on those technical systems which are used in data and/or information processing and storing. Following Polanyi’s work, the focus is on the protection of information existing in explicit form (Polanyi 1966, 4 and Nonaka 1994, 16). Figure 21 presents the scope of information and cyber security in context of the DIKW hierarchy.

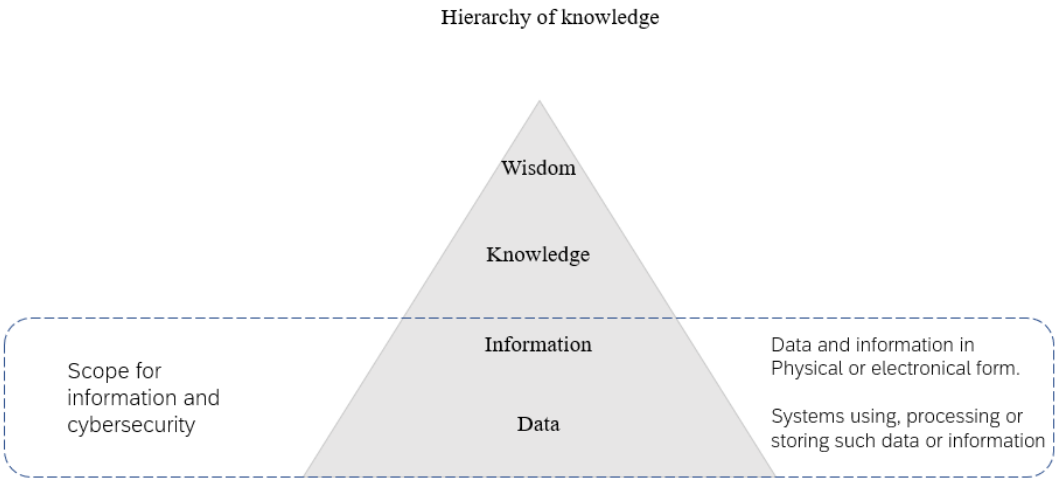


Figure 21. The coverage of information and cybersecurity management

4.8. Information and cyber security management are inward oriented

As a part of the systematic literature review a categorization of reviewed works were done. The categorization demonstrates that information and cyber security related research focuses on information and cyber security centric issues. For example, linking the information and cyber security to other disciplines or to business seem to be relatively rare. The reason for this can be the fact, that information and cyber security management is a relatively new field

and that the relationships and interaction with other research has not yet been established (Iivonen, Jussila, Kärkkäinen & Päivärinta 2015, 3941)

The majority of the reviewed research articles seem to be focusing on internal aspects and activities of information and cyber security. The internal aspects and activities cover works where the topic relates on the content of international security standards or on the implementation of these standards, security governance, identifying key security controls or in works focusing to the automation of security controls. The articles focusing on standardization present the single largest category with 18 articles. This presents almost 20% of the reviewed works. When calculating all the works focusing on the standards, development of information security management, taxonomy, automation of security controls, governance or risks / risks assessments this covers 60% of all reviewed articles. Table 3 presents the biggest categories of research articles.

Table 3. Categorization of reviewed articles

#	Category	# of articles
1	ISM Standards	18
2	maturity/modelling of ISM	15
3	Depiction/development of ISM	10
4	Risk assessment (IRM / ISRM)	7
5	Other	7
6	Key activities in ISM	6
7	Automation & workflow related	5
8	Governance	4
9	HR and organization	4
10	KM	4
11	Challenges in ISM	4
12	Key risks	3
13	Taxonomy	2
14	Information classification	2
15	Role of CISO	1
---	Excluded articles	24
	Total	116

Another category on internal questions and matters are the modelling / maturity evaluation models on information and cyber security. From selected articles 15 falls on this category. This category includes articles with a theoretical aspect where the article attempts to either present a model for assessing the maturity of and organizations information security

management system (Arkhipova 2022, Monev 2020, Sulistyowati, Handayani & Suryanto 2020). Or alternatively the article presents a model for evaluating the investments on information security (Wu, Wang, Cheng & Dai 2021, Shichkina & Fatkieva 2021, Lakhno, Malyukov, Yerekesheva 2020 etc.).

What is notable, is the lack of research related to other disciplines or business areas. Also, the information and cyber security leadership is an area where only one article was identified (Da Silva 2022). In reviewed articles 4 works related on human resources management (Alzahrani & Seth 2021, Govender, Kritzinger & Loock 2020, Pérez-González, Preciado, Solana-Gonzalez, Luma & Abazi 2019) and one in enterprise architecture (Diefenbach, Lucke & Lechner 2019)

5. Conclusions and discussion

5.1. Research and research work

The purpose of the thesis is to evaluate how information and cyber security related research addresses and relates to the resource-based view. As proven in section 2.1 - 2.3 intellectual capital is the most important asset of a modern organization.

Information and cybersecurity management are activities which aim to protect the valuable information assets of an organization (ref. Horne, Ahmad & Maynard 2016, 1). The research was conducted as a systematic literature review where the focus was on information and cyber security management related research. The time frame for the selected research materials was research published between 2010 and April 2022. The systematic literature review is a method which includes an analysis, evaluation and synthesis of the selected materials (Onwuegbuzie, Leech & Collins 2012, 2). In this research the scope was to review how the research relates on the intellectual capital. The systematic literature review can also be used to reveal gaps in the existing research and thus bring up new areas and questions for future research (Salminen 2011, 10-11). This is exactly how this study contributes, it proves a gap and weakness in current definition and theory on information and cyber security related research.

5.2. Answering the research questions

Based on the systematic literature review, the information and cybersecurity management related research done during years 2010 to 2022 is not connected resource-based view in any way nor does it recognize the concept of information hierarchy.

The information and cybersecurity management research uses the concept of information in broad and unstructured way. Other terms like assets and data are also commonly used without any obvious constructive structure or hierarchy. This finding is also supported by literature as it is identified that it lacks consistency in terminology and semantics (Alshaikh, Maynard, Ahmad & Chang 2015). The fact, that only a small share of individual articles were based on the knowledge management theory also confirm the missing link.

The contribution of the thesis is on identifying the gap in the current research and on the weakness in the concept of information security.

5.3. Discussion on the results

The information and cybersecurity management disciplines are relatively new. In fact, the information security has been raising as a "societal concern" only from the turn of the millennium (Olijnyk 2015). The resource-based view and the concept of intellectual capital has also been gaining focus during the same period, but apparently the two disciplines have not been influencing each other.

In knowledge management the concept of the hierarchy of information has been introduced. This concept is not used in information and cyber security management. This results in a conceptual conflict. The research of information and in cybersecurity justify the importance of the subject, and the need for information security as information is the most valuable asset of an organization. And yet address the information protection only on data and explicit information either in electronical or physical form.

It is also stated that the entire concept of information security management is "fragmented and conceptually unclear" (Anttila & Jussila 2018). In principle there seems to be a tendency,

where the relatively broad area of information security is approached only from a certain limited aspect like cryptology (Kangle 2020). This leads to a limited view and understanding on the subject and to the situation where the overall research of the topic is approached by focusing on individual phenomenon or topics like technology or security incidents (Naseer, Maynard & Desouza 2021). This can lead to an outcome where the different researchers and research projects are working with the same topic and in worst case generating overlapping or conflicting concepts. (Siponen, Oinas-Kukkonen 2007, 60)

On the other hand, information security related research appears to have a technical focus and the research is focusing on technical aspects (Kim & Kim 2021, Culot, Nassiembeni & Sartor 2021). This can also be observed in a lack of interdisciplinary work and on work focusing on isolated topics and areas (Siponen, Oinas-Kukkonen 2007, 60-61). Also, the technical, organizational and managerial topis are not combined, rather these topics are discussed separately and independently (Anttila & Jussila 2018). In conclusion information and cybersecurity management have developed independently and without any major interplay with other disciplines, like human or social sciences (Anttila & Jussila 2018). What is surprising is, that information security & cyber security it appears not be connected to business strategies or to business management (Kim & Kim 2021).

Information and cybersecurity management seem to be enamored with information security management standards. Majority of works reviewed in this systematic literature review was somehow relating to information security management standards. The articles were focusing on either presenting the structure of the standards, the key areas of it or on the implementation of it. As described in chapter 2.7 information and cybersecurity management appears to be a relatively new and unknown territory for organization and for management. Therefore, the interest and focus to standards may be explained those being used as maps or guidebooks on how and what the information and cybersecurity management is about. This especially, when there was only one article which had a critical view on the real benefits what the organization could gain from the implementation of information security management standards (Anttila & Kajava 2010).

When the knowledge protection is seen as a separate process from the other strategic knowledge management activities (Hussinki et al. 2017, 1599) and when the definition or concept of it is not described in detail in knowledge management theory (Inkinen et al. 2015), one would expect that the information and cybersecurity would fill this need. Based on the

research this is not the case. Few studies were addressing this by introducing the concept of knowledge security [80].

There is also a difference on how the protection of the intellectual property of an organization is viewed. In knowledge management related research, the responsibility to protect knowledge is seen as an activity of the organizations managers. For example, “Managers can choose active knowledge protection strategies” (de Fario & Sofka 2010, 957) and in similar manner also Olander, Hurmerinta-Laukkanen & Vanhala (2014;2019) and Husted, Michailova, Olander (2013). When in information and cybersecurity related research the information protection it is pointed towards information security function more than to the responsible managers of an organization (ref. von Solms & von Solms 2004, 372). In research the information and cybersecurity management are strongly oriented towards international standards (ref table 5). The focus and interest on international management standards can certainly foster and harmonize the development of information and cybersecurity management practices (Eloff & von Solms 2000). On one hand the utilization of these standards will also extend the focus outside the technical realm in and include also the users and user awareness on security (von Solms 2000, 616). On the other hand, if the implementation of these standards becomes the purpose, then the information and cybersecurity management may drift apart and lose touch with business management. If the link to the activities and management of an organization is lost, then the management of these organization´s may not be interested or committed to the security and standardization activities (Anttila & Kajava 2010). Other criticism on the unilateral approach on standards relate on the “incompatibility and ambiguousness” of such standards (Anttila & Jussila 2018, 586) and on the lack of business integration and to business processes or quality (Anttila, Jussila, Kajava & Kamaja 2012, Anttila & Jussila 2018).

5.4. Validity, reliability and limitations of the research

The purpose for the thesis was to review the context of intellectual capital in the information and cybersecurity management. The research was conducted as a systematic literature review, and it was focusing to the available research materials available in electronical form in searchable research databases.

The research can be fully repeated as all the prerequisites of the research are presented in the work. The keywords used in the search are presented in paragraph 3.5 and the used databases are publicly available for registered users. The set time window for the selected research articles is from 2010 to April 2022. The research database searches support such selection by default. The acquisition of research articles identified by using the Scopus database search may require license or user access to multiple research article databases. The search can be easily repeated with the information available in the method section. The material intake can be adjusted to fit the particular need of the search.

The validity of the analysis made based on the systematic literature review can be argued as the results provided little or no relationship with the research and theory on intellectual capital and information & cybersecurity management. The zero connection can also be seen as a significant finding, as it indicates that there is a gap both in the knowledge management and information & cybersecurity management related theory on the protection of intellectual capital. On the categorization part in the results part, the classification model is most likely not generally suitable. Meaning that for similar research a case specific categorization needs to be developed, as in this work the categorization was developed only after the material screening and intake phase.

This research focused only on the information and cybersecurity management in the context of intellectual capital as defined in knowledge management theory. The purpose was to study how the protection of intellectual capital appeared in information and cybersecurity management related research. As intellectual capital is considered to be the key resource when creating sustainable competitive advantage, the study focused on enterprises and the protection of their intellectual capital. Because of this, research articles focusing on governmental organizations, healthcare and education institutions was excluded. Similarly, research which focused on the regulated objects like personal data or payment card related information for example was excluded.

5.5. Future research

This research revealed a gap in the concept of protection of intellectual capital. In knowledge management the knowledge protection is one of the key practices (Inkinen, Kianto & Vanhala 2015). Information and cybersecurity focus on protecting the confidentiality, integrity and availability of data and information ((Lundgren & Möller 2019, von Solms & von Solms 2018, Nnolim 2008). But the big question is on the protection of organizations crucial assets -in this context the intellectual capital. There is some research done touching the topic (ref chapter 2.4), but the comprehensive theory and concepts on the protection of intellectual capital are undefined. This area and topic should be approached with multidisciplinary research combining different disciplines like knowledge management, management, social sciences, risk management and security.

Other research area relates to the critical view on information and cybersecurity management. In all research materials the importance of information and cybersecurity is justified with the generic statement on the importance of data and or information. And in addition, most of the research materials relate to the technical aspects or to the protection of information processing systems. The relatively freely used statement on "information security focusing on the protection of organizations critical information assets" should be subject of critical evaluation. This especially when the information and cybersecurity research indicate that the terminology is unclear and vague. And in addition, as it appears that the true focus in information security is on the technical aspects and it the protection of IT systems.

5.6. Closing sentence

Based on the search and number of existing research there appears to be a gap in the research papers on the connection between the "true strategic assets" (Meso & Smith 2000), "firm resources" (Barney 2001) and information & cyber security related research. As the intellectual capital can be proved to be the real crown jewels of the organization, then there should also be activities focusing on safeguarding and protecting these assets. This is a major issue, as the entire concept of information security sets the promise on protecting the valuable information assets of the organization.

The work proves that there is need for research on how the firm resources and intellectual capital can be protected and on what is the role of information and cyber security in it. In addition, the role of information and cyber security should be critically viewed to ensure that the words and deeds match also in an organizational context.

With this new knowledge and view to the existing gap a more holistic view to the protection of intellectual capital and on information and cyber security management can be created. This is important, as modern organizations and societies are dependent on information and knowledge. With the revised view on information and cyber security and on the protection of organizations real key assets, the goal on protecting the organizations long term business success can be achieved.

References

Alavi, M. and Leidner, D.E. 2001. Knowledge Management and Knowledge Management Systems: Conceptual Foundations and Research Issues. MIS Quarterly, 25, 107-136.

Anderson, James M. 2003. Why we need a new definition of information security. Computers & security, 2003, Vol.22 (4), p.308-313

Antoniou, G., S. 2018. A Framework for the Governance of Information Security: Can it be Used in an Organization. SoutheastCon 2018, pp. 1-30.

Anttila, J., Jussila, K. 2018. Challenges for the Comprehensive and Integrated Information Security Management

Arkhipova, A. 2022. Multisociometrical Readiness Characteristics in Information Security Management (2022). CEUR Workshop Proceedings, 3094, pp. 25-34.

Aven, T. 2012. T1 - A conceptual framework for linking risk and the elements of the data–information–knowledge–wisdom (DIKW) hierarchy. Reliability Engineering & System Safety. March 2013 Reliability Engineering. System Safety 111:30–36

Aveyard, H. 2014. Doing a literature review in health and social care: A practical guide (Third edition ed.). Open University Press.

Baskerville, R. Spagnoletti, P. Kim, J. 2014. Incident-centered information security: Managing a strategic balance between prevention and response, Information & Management, Volume 51, Issue 1, 2014, Pages 138-151,

Barney, J. (1991) 'Firm resources and sustained competitive advantage', *Journal of Management*, Vol. 17, pp.99–120.

Borrego, M., Foster, M. & Froyd, J. 2014. Systematic literature reviews in engineering education and other developing interdisciplinary fields. The Research Journal for Engineering Education, 103(1), 45–76.

Cains, M.G., Flora L., Taber D., King, Z., Henshel, D.S. 2021. Defining Cyber Security and Cyber Security Risk within a Multidisciplinary Context using Expert Elicitation. Risk Analysis: An Official Publication of the Society for Risk Analysis.

Chen, M-J. Michel, J., G. Wenchen, L. 2021. Worlds Apart? Connecting Competitive Dynamics and the Resource-Based View of the Firm Journal of management, 2021, Vol.47 (7), p.1820-1840

Choong, K., K. 2008. Intellectual Capital: Definitions, Categorization and Reporting Models October 2008 Journal of Intellectual Capital 9(4):609-638 DOI:10.1108/14691930810913186

US Committee on National Security Systems 2022. [visited 15.4.2022] available at www.cnss.gov/cnss/

Costin, A-M. Ionescu, S.E. Gherghina, A. 2020. Methods for online search of databases with scientific articles. Scientific Bulletin ("Mircea cel Bătrân" Naval Academy), 2020, Vol.23 (2), p.1-5

Craigen, D. Diakun-Thibault, N. Purse, R. 2014. Defining cybersecurity. October 2014. Technology Innovation Management Review 4(10):13-21

Davis, F., G. DeWitt, T. 2021. Organization Theory and the Resource-Based View of the Firm: The Great Divide. Journal of Management Vol. 47 No. 7, September 2021, 1684–1697

de Faria, P. Sofka, W. 2010. Knowledge protection strategies of multinational firms—A cross-country comparison. Research Policy. 39. 956-968.

Drucker, P.F. 1988. 'The coming of the new organization', *Harvard Business Review*, Vol. 66, No. 1, pp.45–54.

Dumay, J. 2016. A critical reflection on the future of intellectual capital: from reporting to disclosure. Journal of Intellectual Capital, Vol. 17 No. 1, pp. 168-184.

Edvinsson, L. and Malone, M. 1997. Intellectual Capital: Realising your Company's True Value by Finding its Hidden Brainpower, New York: Harper Collins.

Ekelhart, A., Fenz, S., Klemen, M., & Weippl, E. 2007. Security ontologies: Improving quantitative risk analysis. In 40th annual Hawaii international conference on system sciences. Piscataway, NJ: IEEE.

Fink, A. 2005. Conducting Research Literature Reviews: From the Internet to Paper (2nd ed.). Thousand Oaks, California: Sage Publications

Gerber, M. von Solms, R. 2005. Management of risk in the information age. February 2005 Computers & Security 24(1):16-30.

Gill, A.K., Zavarsky, P., Swar, B. 2021. Automation of Security and Privacy Controls for Efficient Information Security Management ICSCCC 2021 - International Conference on Secure Cyber Computing and Communications, art. no. 9478126, pp. 371-375.

Harel, Y., Gal, I., B. Elovici, Y. 2017. Cyber Security and the Role of Intelligent Systems in Addressing its Challenges. ACM Transactions on Intelligent Systems and Technology Volume 8 Issue 4 July 2017 Article No.: 49pp 1–12

Hirsjärvi, S., Remes, P., Sajavaara, P. 1997. Tutki ja kirjoita. 6–9. p. Tammi, Helsinki.

Horne, G., A. Ahmad, A. Maynard, S., B. 2016. A Theory on Information Security. December 2016 Conference: The 27th Australasian Conference on Information Systems at: Wollongong, Australia

Hussinki, H., Kianto, A., Vanhala, M. and Ritala, P. 2017. Assessing the universality of knowledge management practices. Journal of Knowledge Management, Vol. 21 No. 6, pp. 1596-1621.

Husted, K., Michailova, S., Olander, H. 2013. Dual allegiance, knowledge sharing, and knowledge protection: An empirical examination. International Journal of Innovation Management, vol. 17, issue 6.

Hurmelinna-Laukkanen, P. 2011. Enabling collaborative innovation - knowledge protection for knowledge sharing. European Journal of Innovation Management, Volume 14, Number 3, 2011, pp. 303-321(19)

Hurmelinna-Laukkanen, P., & Puumalainen, K. 2007. Nature and dynamics of appropriability: strategies for appropriating returns on innovation. R&d Management, 37(2), 95-112.

Inkinen. H. 2016. Review of empirical research on knowledge management practices and firm performance. Journal of Knowledge Management, Vol. 20 Iss 2 pp. 230 – 257

Inkinen, H., Kianto, A., Vanhala, M. 2015. Knowledge Management Practices and Innovation Performance in Finland. Baltic Journal of Management, vol. 10, issue 4. pp. 432-455.

Iqbal, Z. Anwar, Z. 2020. SCERM—A novel framework for automated management of cyber threat response activities, Future Generation Computer Systems, Volume 108, Pages 687-708.

Jones S.L., Muir K., Collins E.I.M., Joinson A., Levordashka A. 2019. What is 'cyber security'? Differential language of cyber security across the lifespan. Conference on Human Factors in Computing Systems - Proceedings, art. no. 3312786

Karangelos, E. & Wehenkel, L. 2022. Cyber–physical risk modeling with imperfect cyber-attackers. Electric Power Systems Research. Volume 211, 2022, 108437.

Kazemi, U. 2018. A Survey: Information Security Management System.

Kianto, A. 2007. What do we really mean by the dynamic dimension of intellectual capital? Int. J. Learning and Intellectual Capital, Vol. 4, No. 4, 2007

Lame, G. 2019. Systematic Literature Reviews: An Introduction', in Proceedings of the 22nd International Conference on Engineering Design (ICED19), Delft, The Netherlands, 5-8 August 2019

Lane, V., P. 1985. Security of computer-based information systems. Macmillan Education ltd.

Łuczak, J. 2014. Information Security Management. Normalized Management Systems: Quality, Environment and Safety (pp.171-190). Wydawnictwo Uniwersytetu Ekonomicznego w Poznaniu.

Lundgren, B., Möller, N. 2019. Defining Information Security. Science and engineering ethics, 2017-11-15, Vol.25 (2), p.419-441

Magnier-Watanabe, R. Benton, C. 2017. Management innovation and firm performance: the mediating effects of tacit and explicit knowledge. Knowledge management research & practice, 2017, Vol.15 (3), p.325-335

Marr, B. (Ed). 2005. Perspectives on Intellectual Capital, Oxford: Elsevier.

Marr, B. 2008. Impacting Future Value: How to Manage your Intellectual Capital. The Society of Management Accountants of Canada (CMA Canada), the American Institute of Certified Public Accountants, Inc. (AICPA) and The Chartered Institute of Management Accountants (CIMA).

Martín-de-Castro, G., Delgado-Verde, M., López-Sáez, P. Navas-López, J. 2011. Towards 'An Intellectual Capital-Based View of the Firm': Origins and Nature. Journal of business ethics, 2011-02-01, Vol.98 (4), p.649-662

Meso, P. and Smith, R. 2000. A Resource-Based View of Organizational Knowledge Management Systems. Journal of Knowledge Management, 4, 224-234.

NIST. 2013. Foundations for innovation in cyber-physical systems: workshop report. National Institute of Standards and Technology, https://www.nist.gov/system/files/documents/el/CPSWorkshopReport-1-30-13-Final.pdf

Nnolim, Anene L. 2007. A Framework and Methodology for Information Security Management. Southfield, MI: Lawrence Technological University.

Nonaka, I. 1994. A Dynamic Theory of Organizational Knowledge Creation. Organization Science, Vol. 5, No. 1 (Feb. 1994), pp. 14-37

Olander, H. 2011. Formal and informal mechanisms for knowledge protection and sharing

Olander, H., Hurmelinna-Laukkanen, P., Vanhala, M. 2014. Mission: possible but sensitive –Knowledge protection mechanisms serving different purposes. International Journal of Innovation Management, vol. 18, iss. 6.

Olander, H., Vanhala, M., Hurmelinna-Laukkanen, P., Blomqvist, K. 2016. Preserving prerequisites for innovation: Employee-related knowledge protection and organizational trust. Baltic Journal of Management, vol. 11, issue 4. pp. 493-515.

Olijnyk, N.V. 2015. A quantitative examination of the intellectual profile and evolution of information security from 1965 to 2015. (2015) Scientometrics, 105 (2), pp. 883-904.

Onwuegbuzie, A. J., Leech, N. L., & Collins, K. M. 2012. Qualitative analysis techniques for the review of the literature. The Qualitative Report, 17(28), 1–28.

Page M., J, McKenzie J.,E, Bossuyt P.,M, Boutron I, Hoffmann TC, Mulrow CD, et al. 20 The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. BMJ 2021

Pérez-González, D. Preciado, S., T. Solana-Gonzalez, P. 2019. Organizational practices as antecedents of the information security management performance: An empirical investigation Information technology & people (West Linn, Or.), 2019, Vol.32 (5), p.1262-1275

Pieters, W. 2011. The (Social) Construction of Information Security. The Information Society - An International Journal Volume 27, 2011 - Issue 5

Ployhart. R., E. 2021. Resources for What? Understanding Performance in the Resource-Based View and Strategic Human Capital Resource Literatures. Journal of Management Vol. 47 No. 7, September 2021, 1771–1786

Polanyi, M. 1966. The Tacit Dimension, London: Routledge & Kegan Paul.

Porter, M., E. 1985. Competitive Advantage: Creating and Sustaining Superior Performance. New York: Free Press, 1985.

Päällysaho, S. and Kuusisto, J. 2008, Intellectual Property Protection in Service Sector. International Chamber of Commerce, Paris.

Päällysaho, S. & Kuusisto, J. 2011. Informal ways to protect intellectual property (IP) in KIBS businesses, Innovation, 13:1, 62-76,

Rajkumar, R. Lee, I. Sha, L. Stankovic, J. 2010. Cyber-physical systems: the next computing revolution. 47th ACM/IEEE design automation conference (DAC).

Ramli, N.A., Aziz, N.A. 2012. Risk identification for an information security management system implementation SECURWARE 2012 - 6th International Conference on Emerging Security Information, Systems and Technologies, pp. 57-61.

Renaud, K., Von Solms, B. and Von Solms, R. 2019. "How does intellectual capital align with cyber security?", Journal of Intellectual Capital, Vol. 20 No. 5, pp. 621-641.

Rothaermel, F. 2012. Strategic Management: Concepts and Cases. McGraw-Hill Education - Europe.

Rowley, J. 2006. What do we need to know about wisdom? Management decision, 2006, Vol.44 (9), p.1246-1257

Salminen, A. 2011. Mikä kirjallisuuskatsaus? Johdatus kirjallisuuskatsauksen tyyppeihin ja hallintotieteellisiin sovelluksiin, Vaasan yliopisto opetusjulkaisu 62.

Schatz, D. Bashroush, R. and Wall, J. 2017. Towards a More Representative Definition of Cyber Security. Journal of Digital Forensics, Security and Law: Vol. 12: No. 2, Article 8.

Silva, L. Hsu, C. Backhouse, J. McDonnell, A. 2016. Resistance and power in a security certification scheme: The case of c:cure, Decision Support Systems, Volume 92, 2016, Pages 68-78,

Singh, A., H. Gupta, MP., Ojha, A. 2014. Identifying factors of "organizational information security management“. September 2014. European Journal of Marketing 27(5).

Singh, V.K., Singh, P., Karmakar, M. Leta, J. & Mayr, P. 2021. The journal coverage of Web of Science, Scopus and Dimensions: A comparative analysis. Scientometrics 126, 5113–5142 (2021).

Siponen, M. T., & Oinas-Kukkonen, H. 2007. A review of information security issues and respective research contributions. SIGMIS Database, 38(1), 60–80.

Siponen, M. Willison, R. 2009. Information security management standards: Problems and solutions, Information & Management, Volume 46, Issue 5, 2009, Pages 267-270.

Soomro, Z., A. Shah., M., H. Ahmed, J. 2016. Information security management needs more holistic approach: A literature review. International Journal of Information Management. Volume 36, Issue 2, April 2016, Pages 215-225

Strupczewski, G. 2020. Defining cyber risk. Safety science, 2021-03, Vol.135

Subramaniam, M. and Youndt, M. 2005. ‘The influence of intellectual capital on types of innovation capabilities’, Academy of Management Journal, Vol. 48, No. 3, pp.450–463.

Taherdoost, H. Understanding Cybersecurity Frameworks and Information Security Standards. A Review and Comprehensive Overview. Electronics 2022, 11, 2181.

Thompson, M., A. Ryan, M., J. Slay, J. McLucas, A., C. 2016. Harmonized taxonomies for security and resilience. Information security journal., 2016-04-04, Vol.25 (1-3), p.54-67

Tu, C.Z., Yuan, Y., Archer, N., Connelly, C.E. 2018. Strategic value alignment for information security management: a critical success factor analysis. Information and Computer Security, 26 (2), pp. 150-170.

Visser, M., van Eck, N. J., & Waltman, L. 2021. Large-scale comparison of bibliographic data sources: Scopus, Web of Science, Dimensions, Crossref, and Microsoft Academic. Quantitative Science Studies, 2(1), 20–41.

Veiga, A., D. Eloff, J., H., P. 2007. An Information Security Governance Framework, Information Systems Management, 24:4, 361-372.

Vermeulen, C., & von Solms, R. 2002. The information security management toolbox – taking the pain out of security management, Information Management and Computer Security, Volume 10, Number 3, 119-125.

von Solms, B. 2000. Information Security — The Third Wave? Computers & security, 2000, Vol.19 (7), p.615-620

von Solms, R. Van Niekerk, J. 2013. From Information Security to Cyber Security. Computers & Security, 38, 97-102.

von Solms, B. Solms, R. 2001. Incremental information security certification, Computers and Security 20 (4), pp. 308 – 310.

von Solms, S., V. von Solms, R., V. 2004. The 10 deadly sins of information security management. Computers & Security (2004) 23, 371-376

von Solms, B. von Solms, R. 2018. Cyber security and information security – what goes where? January 2018 Information and Computer Security 26(1):

Wernerfelt, B. 1984. 'A resource-based view of the firm', Strategic Management Journal, Vol. 5, pp.171–180.

Wellman, J.L. 2009. Organizational learning: How companies and institutions manage and apply knowledge, 1st ed. New York: Palgrave Macmillan Ltd.

Whitman, M., E., Mattord, H., J. 2009. Principles of Information Security. Thomson Course Technology, 2009

Xu, S., Yung, M. & Wang, J. 2021. Seeking Foundations for the Science of Cyber Security. Inf Syst Front 23, 263–267.

APPENDIX 1 - inventory of articles included in the systematic literature review

#	Article data (author, title, key words, summary)	Category
1	Da Silva, J. Cyber security and the Leviathan (2022) Computers and Security, 116, art. no. 102674, . https://www.scopus.com/inward/record.uri?eid=2-s2.0-85125766081&doi=10.1016%2fj.cose.2022.102674&partnerID=40&md5=5e92178bddba940a94184411983b9460 INDEX KEYWORDS: Philosophical aspects, Cybe security practice; Cyber security; Human aspects; Information security managements; Organizational studies; Political perspective; Qualitative research; Security Practice; Security studies; Sociological perspective; Thomas hobbe, Cybersecurity THEME: Role of CISO and comparison on CISO practices in organization with the theories of Thomas Hobbes	CISO
2	Arkhipova, A. Multisociometrical Readiness Characteristics in Information Security Management (2022) CEUR Workshop Proceedings, 3094, pp. 25-34. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85126604620&partnerID=40&md5=1a43a6451627e6b6d179a5d6e7876b5f INDEX KEYWORDS: Cybersecurity; Industrial management; Students, Cyber security; Cybergaming; Cybersecurity level; Education characteristic; Information security managements; Information security risks; Multisociometrical readiness characteristic; Readiness indicator; Security management systems; Social engineering, Information management THEME: Partial maturity model on infosec management readiness based on the education, seniority and advanced training of information security specialist	Maturity/modelling
3	Susukailo, V., Opirsky, I., Yaremko, O. Methodology of ISMS Establishment Against Modern Cybersecurity Threats (2022) Lecture Notes in Electrical Engineering, 831, pp. 257-271. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85121376736&doi=10.1007%2f978-3-030-92435-5_15&partnerID=40&md5=231b711e680c2ab5f245b8d22a2981e8	Standards

INDEX KEYWORDS: Cybersecurity; Industrial management; Risk management; Security systems, CIS top 18; Cyber security; Cybersecurity threat; Education roadmap; Information security management system; Information security managements; ISO 27001/2; NIST 800-53; Roadmap; Security controls; Security management systems, Information management

THEME: Analysis of different ISMS frameworks

4 Onyshchenko, S., Yanko, A., Hlushko, A., Sivitska, S. — Maturity/modelling

Increasing Information Protection in the Information Security Management System of the Enterprise

(2022) Lecture Notes in Civil Engineering, 181, pp. 725-738.

https://www.scopus.com/inward/record.uri?eid=2-s2.0-85116504153&doi=10.1007%2f978-3-030-85043-2_67&partnerID=40&md5=85cedd971bd7a16e2fbcde78edc833c4

INDEX KEYWORDS: Codes (symbols); Competition; Error correction; Industrial management; Information management; Losses, Computer system for processing enterprise data; Conditional alternative set; Data errors; Enterprise data; Errors correction; Information; Information security managements; Linear codes; Security management systems; System of residual class, Security of data

THEME: Modelling the ISM of an enterprise.

5 Kim, Y., Kim, B. — Other

The effective factors on continuity of corporate information security management: Based on toe framework

(2021) Information (Switzerland), 12 (11), art. no. 446, .

https://www.scopus.com/inward/record.uri?eid=2-s2.0-85118880627&doi=10.3390%2finfo12110446&partnerID=40&md5=e1c0359dd2b839a87e7bf3b309e146fa

INDEX KEYWORDS: Environmental management; Industrial management; Metadata; Security of data; Surveys, Business management; Continuity; Corporate information; Digital transformation; Environment factors; Environmental factors; Information protection; Information security managements; Management activities; TOE framework, Information management

6 Alzahrani, L., Seth, K.P. — HR and organization

The impact of organizational practices on the information security management performance

(2021) Information (Switzerland), 12 (10), art. no. 398, .

https://www.scopus.com/inward/record.uri?eid=2-s2.0-85116446743&doi=10.3390%2finfo12100398&partnerID=40&md5=2f83aec3d5ac530c883346caec152f30

INDEX KEYWORDS: Decision making; Industrial management; Manufacture; Security of data, Business goals; Education trust; Information explosion; Information security managements; Knowledge-sharing; Organizational practices; Security performance; Security training; Small and medium-sized enterprise, Knowledge management

7 Mirtsch, M., Blind, K., Koch, C., Dudek, G. — Standards

Information security management in ICT and non-ICT sector companies: A preventive innovation perspective

(2021) Computers and Security, 109, art. no. 102383, .

https://www.scopus.com/inward/record.uri?eid=2-s2.0-85111569115&doi=10.1016%2fj.cose.2021.102383&partnerID=40&md5=292e5a3daa4757c605d118c75343bbc0

INDEX KEYWORDS: Industrial management; Information management; ISO Standards, Certification; Information security management system; Information security managements; Institutional theory; ISO/IEC; ISO/IEC 27001; Management system standard; Preventive innovation; Resource-based view; Security incident, Security of data

THEME: The implementation of ISO/IEC 27001 standard for ICT and non-ICT company

8 Wu, Y., Wang, L., Cheng, D., Dai, T. — Maturity/modelling

Information security decisions of firms considering security risk interdependency

(2021) Expert Systems with Applications, 178, art. no. 114990, .

https://www.scopus.com/inward/record.uri?eid=2-s2.0-85104665651&doi=10.1016%2fj.eswa.2021.114990&partnerID=40&md5=1d9393ef9dbfb3e0dabc412754246bac

INDEX KEYWORDS: Security of data, Complementation; Different effects; Incentive mechanism; Information assets; Information security managements; Investment incentives; Risk interdependencies; Security risks; Substitution degree; Technical similarity, Investments

THEME: Game theoretic model to investigate two different firms optimal security efforts (in networked environment)

9 Martín, T.R. — Excluded

Automation of an information security management system based on the iso / iec 27001 standard [De un sistema de gestión de seguridad de la información basado en la norma iso/iec 27001]

(2021) Universidad y Sociedad, 13 (5), pp. 495-506.

https://www.scopus.com/inward/record.uri?eid=2-s2.0-85116100308&partnerID=40&md5=a3561b4abfd9b8d11eaef0b28da7ce0a

EXCLUDED as not available in English.

10 Tolah, A., Furnell, S.M., Papadaki, M. — Key activities

An empirical analysis of the information security culture key factors framework

(2021) Computers and Security, 108, art. no. 102354, .

https://www.scopus.com/inward/record.uri?eid=2-s2.0-85109503970&doi=10.1016%2fj.cose.2021.102354&partnerID=40&md5=d15dac8594e110d1b0939519db898b90

INDEX KEYWORDS: Behavioral research; Cell culture; Factor analysis; Human engineering; Personnel; Reliability analysis, Culture framework; Empirical analysis; Empirical studies; Employee behavior; Information assets; Information security cultures; Key factors; Quantitively study; Security breaches; Sensitive informations, Security of data

THEME: Analysis on the key factors in a information security favorable culture

11 Shichkina, Y.A., Fatkieva, R.R. — Maturity/modelling

Intelligent Information Security Management of Cyber-physical Systems

(2021) Proceedings of 2021 2nd International Conference on Neural Networks and Neurotechnologies, NeuroNT 2021, art. no. 9472853, pp. 25-27.

https://www.scopus.com/inward/record.uri?eid=2-s2.0-85112863797&doi=10.1109%2fNeuroNT53022.2021.9472853&partnerID=40&md5=8b6597adec5f536c761365cb16a6f55b

INDEX KEYWORDS: Cyber Physical System; Embedded systems; Industrial management; Information management; Security of data, Information security managements; Intelligent information; Linear aggregates; Parametric synthesis; Technical objects, Neural networks

THEME: The use of modelling and heuristics in the protection of cyber-physical systems.

12 Gill, A.K., Zavarsky, P., Swar, B. — Automation/workflow

Automation of Security and Privacy Controls for Efficient Information Security Management

(2021) ICSCCC 2021 - International Conference on Secure Cyber Computing and Communications, art. no. 9478126, pp. 371-375.

https://www.scopus.com/inward/record.uri?eid=2-s2.0-85114125402&doi=10.1109%2fICSCCC51823.2021.9478126&partnerID=40&md5=b195460e609a14c58b89dabc249a1373

INDEX KEYWORDS: Automation; Industrial management; Privacy by design, Automation process; Compensating control; Information security managements; Personally identifiable information; Security and privacy; Security programs; Technology risks; Tools and applications, Information management

THEME: Identification of controls presented in ISO/IEC 27001 standard which can be automated

13	Naseer, H., Maynard, S.B., Desouza, K.C. Demystifying analytical information processing capability: The case of cybersecurity incident response (2021) Decision Support Systems, 143, art. no. 113476, . https://www.scopus.com/inward/record.uri?eid=2-s2.0-85098519258&doi=10.1016%2fj.dss.2020.113476&partnerID=40&md5=72712bff1fa6fca178790020a75ece24 INDEX KEYWORDS: Advanced Analytics; Decision making; Security of data, Business analytics; Enterprise security; Financial benefits; Information processing capability; Information processing theories; Multiple-case study; Research questions; Theoretical framework, Information use THEME: Study on the use of automation (analytical information processessing) in incident response	Automation/workflow
14	Merchan-Lima, J., Astudillo-Salinas, F., Tello-Oquendo, L., Sanchez, F., Lopez-Fonseca, G., Quiroz, D. Information security management frameworks and strategies in higher education institutions: a systematic review (2021) Annales des Telecommunications/Annals of Telecommunications, 76 (3-4), pp. 255-270. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85088596935&doi=10.1007%2fs12243-020-00783-2&partnerID=40&md5=d6cf7d489bf5b1d76ff626e3853f22ed INDEX KEYWORDS: Digital libraries; Industrial management; Infrastructure as a service (IaaS); Security of data, Higher education institutions; Higher education institutions (HEIs); Implementation phasis; Inclusion and exclusions; Information security managements; Infrastructure services; Systematic literature review; Systematic mapping studies, Information management EXCLUDED as the work focuses only on education sector.	Excluded
15	Culot, G., Nassimbeni, G., Podrecca, M., Sartor, M. The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda (2021) TQM Journal, 33 (7), pp. 76-105. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85103188608&doi=10.1108%2fTQM-09-2020-0202&partnerID=40&md5=fd0116caeba594983fdc1e1cb597af69 INDEX KEYWORDS: Quality management; Security of data, Academic literature; Contextual factors; Design/methodology/approach; Information security managements; Inter-disciplinary studies; Literature reviews; Research opportunities; Systematic literature review, ISO Standards	Standards

16 Sterbak, M., Segec, P., Jurc, J. — Automation/workflow

Automation of risk management processes

(2021) ICETA 2021 - 19th IEEE International Conference on Emerging eLearning Technologies and Applications, Proceedings, pp. 381-386.

https://www.scopus.com/inward/record.uri?eid=2-s2.0-85126881820&doi=10.1109%2fICETA54173.2021.9726596&partnerID=40&md5=c75a5d4f6d8c4db78b83811527306310

INDEX KEYWORDS: Application programs; Cloud security; Complex networks; Industrial management; Information management; Risk assessment; Risk management; Security systems, Automation possibility; Information assets; Information security managements; Information security risk managements; Network devices; Risk management process; Risks management; Storage Clouds, Automation

THEME: Automation of the auditing of risk management process of an organization

17 Zammani, M., Razali, R., Singh, D. — Maturity/modelling

Organisational Information Security Management Maturity Model

(2021) International Journal of Advanced Computer Science and Applications, 12 (9), pp. 668-678.

https://www.scopus.com/inward/record.uri?eid=2-s2.0-85119183506&doi=10.14569%2fIJACSA.2021.0120974&partnerID=40&md5=f77b214049c8810442018c935501a1df

INDEX KEYWORDS: Industrial management; Information management; Surveys, Information security management maturity model; Information security managements; Management IS; Management maturities; Management practises; Maturity levels; Maturity model; Qualitative study, Security of data

THEME: Building of a model to evaluate the maturity of organizations ISM

18 Dotsenko, S., Illiashenko, O., Kamenskyi, S., Kharchenko, V. — Excluded

Knowledge management model based approach to profiling of requirements: Case for information technologies security standards

(2021) Studies in Big Data, 84, pp. 255-277.

https://www.scopus.com/inward/record.uri?eid=2-s2.0-85114165373&doi=10.1007%2f978-3-030-65722-2_16&partnerID=40&md5=b89498490f9b8f513d448b4edd046b77

INDEX KEYWORDS: ISO Standards; Petroleum reservoir evaluation; Security of data; Security systems, Common criteria; Factor model; Information security management systems; Integrated modeling; ISO/IEC; IT security; Knowledge management model; Security standards, Knowledge management

EXCLUDED as original article was not found.

19	Fonseca-Herrera, O.A., Rojas, A.E., Florez, H. A Model of an Information Security Management System Based on NTC-ISO/IEC 27001 Standard (2021) IAENG International Journal of Computer Science, 48 (2), pp. 1-10. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85109172871&partnerID=40&md5=9b32e0c43cd0534c6bfaeb5516fbeaaf INDEX KEYWORDS: Computer viruses; Industrial management; ISO Standards; Personal computing; Security of data; Service industry, Data and information; Information assets; Information security management systems; Information security policies; Infrastructure failures; Management systems; Security structures; Technical vulnerabilities, Information management	Standards
20	Zemtsov, I., Astakhova, L. Object-Oriented Situational Approach to Enterprise Information Security Management (2021) Lecture Notes in Electrical Engineering, 729 LNEE, pp. 591-600. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85104857352&doi=10.1007%2f978-3-030-71119-1_58&partnerID=40&md5=3df7a266f77e835aa667bdbeed3fa94e INDEX KEYWORDS: Application programs; Automation; Classification (of information); Cost reduction; Object oriented programming; Security of data; Semiotics; Software prototyping, Economic feasibilities; Information process; Information protection; Information security management systems; Information security managements; Protection measures; Semiotic approaches; Software applications, Information management THEME: The development of a ISM which focuses to the protection of the most valuable security objects of an organization	Key activities
21	Khan, M.I., Tanwar, S., Rana, A. The need for information security management for SMEs (2020) Proceedings of the 2020 9th International Conference on System Modeling and Advancement in Research Trends, SMART 2020, art. no. 9337108, pp. 328-332. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85101154904&doi=10.1109%2fSMART50582.2020.9337108&partnerID=40&md5=6e5f9a8cb7be8f9b171a4dfeb7c95fc6 INDEX KEYWORDS: Competition; Industrial management, Global economic activity; Information security managements; Large business; Market share; Sensitive informations; Small to medium-sized enterprise, Security of data THEME: Survey on the management of information security in small to medium sized organizations	Depiction/development
22	AlGhamdi, S., Win, K.T., Vlahu-Gjorgievska, E. Information security governance challenges and critical success factors: Systematic review (2020) Computers and Security, 99, art. no. 102030, .	Governance

https://www.scopus.com/inward/record.uri?eid=2-s2.0-85090589289&doi=10.1016%2fj.cose.2020.102030&partnerID=40&md5=5b5a28247d7cd5872426d6510cc818ed

INDEX KEYWORDS: Compliance control, Critical success factor; Holistic frameworks; Information security governance; Information security policies; Systematic literature review; Systematic Review, Security of data

THEME: SLR on the governance model for information security.

23 Douchek, P., Nedomova, L., Luc, L., Novak, L. — Challenges with ISM

Information security: The glory and penury of SMEs in the Czech and Slovak Republics

(2020) 2020 International Conference on Engineering Management of Communication and Technology, EMCTECH 2020 - Proceedings, art. no. 9261506, .

https://www.scopus.com/inward/record.uri?eid=2-s2.0-85098327378&doi=10.1109%2fEMCTECH49634.2020.9261506&partnerID=40&md5=6736e6b3794fd4ce50c62748915ea381

INDEX KEYWORDS: Industrial management; Information management; ISO Standards; Personnel, Company size; Czech and slovak republics; Information security managements; ISMS; ISO/IEC; ISO/IEC 270001:2013; Security; Security audit; Security management systems; Security threats, Security of data

THEME: Identification of the most challenging areas of ISM (based on ISO/IEC 27001) for small and medium sized organizations

24 Genchev, P. — ISR/ISRM

An approach to support information security risk assessment

(2020) Proceedings of the International Conference on Biomedical Innovations and Applications, BIA 2020, art. no. 9244516, pp. 125-128.

https://www.scopus.com/inward/record.uri?eid=2-s2.0-85096776728&doi=10.1109%2fBIA50171.2020.9244516&partnerID=40&md5=e8643554b4d851e57e9d15e11a66d542

INDEX KEYWORDS: Industrial management; Information management; Risk management; Security of data, In-buildings; Information security management systems; Information security risk assessment; Information security risk managements; Software products, Risk assessment

THEME: Development of an model for supporting and developing the ISRM in an organization

25 Tsochev, G., Stankov, I. — Depiction/development

A Study on Information Security Management

(2020) 2020 29th International Scientific Conference Electronics, ET 2020 - Proceedings, art. no. 9238331, .

https://www.scopus.com/inward/record.uri?eid=2-s2.0-85097072457&doi=10.1109%2fET50336.2020.9238331&partnerID=40&md5=ff9b8ac432989108271c2c5c5bee10d9

INDEX KEYWORDS: Industrial management, Cyber security; Fast Processing; Information security managements, Security of data

THEME: The review of the the domains of ISMS.

26 Aleksandrova, S.V., Vasiliev, V.A., Aleksandrov, M.N. — Standards

Problems of implementing information security management systems

(2020) Proceedings of the 2020 IEEE International Conference "Quality Management, Transport and Information Security, Information Technologies", IT and QM and IS 2020, art. no. 9322896, pp. 78-81.

https://www.scopus.com/inward/record.uri?eid=2-s2.0-85100425920&doi=10.1109%2fITQMIS51053.2020.9322896&partnerID=40&md5=fd9940fc3de093420c8081b4444cfa85

INDEX KEYWORDS: Competition; Industrial management; International trade; Network security; Quality management, Competitive advantage; Global informations; Global market; Information security management systems; Information Security Regulations; Management systems; Medium-sized business; Risk based approaches, Information management

THEME: The description of the most challenging areas of the implementation of ISO/IEC 27001 standard

27 Grishaeva, S.A., Borzov, V.I. — Depiction/development

Information security risk management

(2020) Proceedings of the 2020 IEEE International Conference "Quality Management, Transport and Information Security, Information Technologies", IT and QM and IS 2020, art. no. 9322901, pp. 96-98.

https://www.scopus.com/inward/record.uri?eid=2-s2.0-85100403964&doi=10.1109%2fITQMIS51053.2020.9322901&partnerID=40&md5=c01b076ed2a7169f4457d0d69639a128

INDEX KEYWORDS: Quality management; Risk assessment; Security of data, Digital economy; Information assets; Information security managements; Information security risk managements; Information security threats; Preventive measures, Risk management

THEME: A discussion and description of the ISM for an organization.

28 Safonova, O.M., Lontsikh, N.P., Golovina, E.Y., Elshin, V.V., Koniuchov, V.Y. — Standards

Methodology for creating, implementing and system effectiveness evaluation of the business processes' information security system

(2020) Proceedings of the 2020 IEEE International Conference "Quality Management, Transport and Information Security, Information Technologies", IT and QM and IS 2020, art. no. 9322855, pp. 127-131.

https://www.scopus.com/inward/record.uri?eid=2-s2.0-85100379139&doi=10.1109%2fITQMIS51053.2020.9322855&partnerID=40&md5=f74770557e944bc18085998c211e3b98

INDEX KEYWORDS: Industrial management; ISO Standards; Quality management; Risk management; Security of data, Business Process; General methodologies; Information security management systems; ISO/IEC; Iso/iec 27005; Process approach; System effectiveness, Information management

THEME: The development of an ISM based on the ISO/IEC 27001 standard

29 Monev, V. — Maturity/modelling

Organisational Information Security Maturity Assessment Based on ISO 27001 and ISO 27002

(2020) 2020 34th International Conference on Information Technologies, InfoTech 2020 - Proceedings, art. no. 9211066, .

https://www.scopus.com/inward/record.uri?eid=2-s2.0-85093971143&doi=10.1109%2fInfoTech49733.2020.9211066&partnerID=40&md5=94e8e137e088496b3a6956db138b93d1

INDEX KEYWORDS: Decision making; Risk assessment; Risk management; Security of data, Information security management systems; Information security professionals; Information security risk managements; Maturity assessments; Maturity levels; Organisational; Security controls; Strategic decision making, Information management

THEME: The development of a model to evaluate the maturity of an organizations ISMS

30 Diéguez, M., Bustos, J., Cares, C. — Standards

Mapping the variations for implementing information security controls to their operational research solutions

(2020) Information Systems and e-Business Management, 18 (2), pp. 157-186.

https://www.scopus.com/inward/record.uri?eid=2-s2.0-85084149437&doi=10.1007%2fs10257-020-00470-8&partnerID=40&md5=72022aba11b38f70684efb021b024e36

THEME: The description of how to implement the ISM controls described in different ISM standards.

31 Lakhno, V., Malyukov, V., Yerekesheva, M., Kydyralina, L., Sarsimbayeva, S., Zhumadilova, M., Buriachok, V., Sabyrbayeva, G. — Maturity/modelling

Model of cybersecurity means financing with the procedure of additional data obtaining by the protection side

(2020) Journal of Theoretical and Applied Information Technology, 98 (1), pp. 1-14.

https://www.scopus.com/inward/record.uri?eid=2-s2.0-85079645261&partnerID=40&md5=5c82d26cbaad6e717ae2b09931a7db09

THEME: To present a model for calculating and evaluating the cost of preventing the cyber security attacks

32	Filatov, V.V., Mshakov, V.Yu., Rodinova, N.P., Ostroukhov, V.M., Polozhentseva, I.V., Akhmedova, Kh.G. Organizational and economic risks of introduction of information security systems of the enterprise (2020) Izvestiya Vysshikh Uchebnykh Zavedenii, Seriya Teknologiya Tekstil'noi Promyshlennosti, 386 (2), pp. 60-68. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85104466636&partnerID=40&md5=2806ba99b9fc4ea01be484dfcf6293df EXCLUDED as not available in English	Excluded
33	Sulistyowati, D., Handayani, F., Suryanto, Y. Comparative analysis and design of cybersecurity maturity assessment methodology using nist csf, cobit, iso/iec 27002 and pci dss (2020) International Journal on Informatics Visualization, 4 (4), pp. 225-230. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85099029846&doi=10.30630%2fjoiv.4.4.482&partnerID=40&md5=d404b77a7a91e85ce46f61f82ccb41a9 THEME: To present an integrated model for evaluating the maturity of organizations cyber security (by using different ISM standards)	Maturity/modelling
34	Wang, L., An, X., Xu, J., Huang, J., Guo, M., Hu, J. Collaborative innovation community capacity building for electronic records security management (2020) Proceedings of the International Conference on Intellectual Capital, Knowledge Management and Organisational Learning, ICICKM, 2020-October, pp. 391-399. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85097847746&doi=10.34190%2fIKM.20.027&partnerID=40&md5=afbd5a8844861b1108c3ac801f21cd20 INDEX KEYWORDS: Cognitive systems; Electronics industry; Historic preservation; Industrial management; ISO Standards; Knowledge management; Security of data, Business continuity management; Collaborative innovation; Conceptual frameworks; Effectiveness and efficiencies; Information security managements; International standards; Long-term preservation; Process collaboration, Records management EXCLUDED as article focuses only on governmental data in electronical form.	Excluded
35	Bergström, E., Karlsson, F., Åhlfeldt, R.-M. Developing an information classification method (2020) Information and Computer Security, 29 (2), pp. 209-239. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85097088962&doi=10.1108%2fICS-07-2020-0110&partnerID=40&md5=4ebfb27a67a9663b9ef1f553e9a7bc7d INDEX KEYWORDS: ISO Standards; Security of data, Design Principles; Design-science researches; Design/methodology/approach; Information assets; Information classification; Long-term goals; Organisational; Subjective judgement, Classification (of information) THEME: Creating a model for creating a model for the classification of information for an organization.	Information classfication

36	Akinyemi, I., Schatz, D., Bashroush, R. SWOT analysis of information security management system ISO 27001 (2020) International Journal of Services Operations and Informatics, 10 (4), pp. 269-287. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85096581948&doi=10.1504%2fIJSOI.2020.111297&partnerID=40&md5=b0745a91555f66c20c07cc3abed06912 THEME: SWOT analysis performed against the ISO/IEC 27001 standard to evaluate the strenghts, weaknesses, opportunities and threats of the use of it.	Standards
37	Müller, N. Information security management: It need not be complicated [Informationssicherheitsmanagement: Es muss nicht kompliziert sein] (2020) Technische Sicherheit, 10 (3), pp. 16-18. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85083830060&partnerID=40&md5=518b86eead25a718f83edbba6c39f30b EXCLUDED as not available in English.	Excluded
38	Kangle, Z. Design Information Security Management System Based on Cryptography (2020) Advances in Intelligent Systems and Computing, 1146 AISC, pp. 187-193. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85082989219&doi=10.1007%2f978-3-030-43306-2_27&partnerID=40&md5=147fd1bd91cf53d0ed6179d2ead234ee INDEX KEYWORDS: Access control; Design; Industrial management; Information management; Network security; Security of data, Cryptographic techniques; Design information; Encryption function; Encryption technologies; Information security management systems; Information support; Networked design; Networked security, Cryptography EXCLUDED as focuses only on technical aspects.	Excluded
39	Govender, S.G., Kritzinger, E., Loock, M. Information security cost reduction through social means (2020) Communications in Computer and Information Science, 1166 CCIS, pp. 1-14. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85082305928&doi=10.1007%2f978-3-030-43276-8_1&partnerID=40&md5=d4b0fae43048cd134756ba349e210655 INDEX KEYWORDS: Security of data, Behavioral changes; Information security managements; Large organizations; Paper costs; Technical human resource; Technological solution, Cost reduction THEME: Description of the use of social means in the control of the costs relating to the ISM of an organization.	HR and organization

40	Diefenbach, T., Lucke, C., Lechner, U. Towards an integration of information security management, risk management and enterprise architecture management - A literature review (2019) Proceedings of the International Conference on Cloud Computing Technology and Science, CloudCom, 2019-December, art. no. 8968909, pp. 326-333. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85079050240&doi=10.1109%2fCloudCom.2019.00057&partnerID=40&md5=7f92c99386c87e8e7f323f3d7b41579a INDEX KEYWORDS: Blockchain; Cloud computing; Industrial management; Risk management; Security of data, Conceptual model; Enterprise Architecture; Enterprise architecture managements; Information assets; Information security managements; IT security; Literature reviews; Research interests, Information management THEME: Combining two different standards from risk management (ISO 31000) and from enterprize architecture (ISO/IEC 27001 to support the development of an ISMS for an organization.	Standards
41	Pérez-González, D., Preciado, S.T., Solana-Gonzalez, P. Organizational practices as antecedents of the information security management performance: An empirical investigation (2019) Information Technology and People, 32 (5), pp. 1262-1275. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85067284350&doi=10.1108%2fITP-06-2018-0261&partnerID=40&md5=b60e0387dfd725ecf746b05c37d08196 THEME: A study of the impact of organizational practises like training, knowledge sharing etc. in the ISM of an organization	HR and organization
42	Bongiovanni, I. Kala Kamdjoug, J.R., Nguegang Tewamba, H.J., Fosso Wamba, S. IT capabilities, firm performance and the mediating role of ISRM: A case study from a developing country (2019) Business Process Management Journal, 25 (3), pp. 476-494. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85049133541&doi=10.1108%2fBPMJ-11-2017-0297&partnerID=40&md5=bf240b3e81580385e8f08a4da867c35b THEME: To build a model for evaluating the IT capabilities of an organization and on the mediating effects ISMS has in this relationship	Maturity/modelling
43	Luma, A., Abazi, B. The importance of integration of information security management systems (ISMS) to the organization's Enterprise Information Systems (EIS) (2019) 2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2019 - Proceedings, art. no. 8756645, pp. 1205-1208. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85070321202&doi=10.23919%2fMIPRO.2019.8756645&partnerID=40&md5=5fcf213eaca8764948f72d486c96ea46	HR and organization

INDEX KEYWORDS: Competition; Digital storage; Industrial management; Information systems; Information use; Integration; Management information systems; Microelectronics; Security of data, Amount of information; Business competition; Business management; Business value; Dataprotection; Enterprise information system; Information protection; Information security management systems, Information management
THEME: To study the impact of organizational practises like training and knowledge sharing on information security

44 Accerboni, F., Sartor, M. — Standards

ISO/IEC 27001

(2019) Quality Management: Tools, Methods and Standards, pp. 245-264.

https://www.scopus.com/inward/record.uri?eid=2-s2.0-85079316844&doi=10.1108%2f978-1-78769-801-720191015&partnerID=40&md5=75e225d1d917683468e5064f256be396
THEME: A review and introduction of ISO/IEC 27001 standard and its content.

45 Minzov, A.S., Tokareva, N.A., Cheremisina, E.N. — Excluded

Integration of various information security control systems

(2019) Journal of Advanced Research in Dynamical and Control Systems, 11 (8 Special Issue), pp. 323-328.

https://www.scopus.com/inward/record.uri?eid=2-s2.0-85070869765&partnerID=40&md5=661bfd48846e73432ab2fe7482036009

EXCLUDED as original article was not found.

46 Carcary, M., Doherty, E., Conway, G. — Excluded

A capability approach to managing organisational information security

(2019) European Conference on Information Warfare and Security, ECCWS, 2019-July, pp. 97-105.

https://www.scopus.com/inward/record.uri?eid=2-s2.0-85070011657&partnerID=40&md5=23d0941f6ac8e264404171a1c1777108

INDEX KEYWORDS: Competition; Computer crime; Crime; Digital storage; Industrial management; Public relations; Security of data; Security systems, Collaborative research; Electronic transaction; Information security incidents; Information security management systems; Information security risks; Inventory and monitoring; Management and controls, Information management
EXCLUDED as article does not meet the requirements of scientific release.

47 Brunner, M., Mussmann, A., Breu, R. — Automation/workflow

Enabling change-driven workflows in continuous information security management

(2019) Proceedings of the ACM Symposium on Applied Computing, Part F147772, pp. 1924-1933.

https://www.scopus.com/inward/record.uri?eid=2-s2.0-85065644765&doi=10.1145%2f3297280.3297468&partnerID=40&md5=84936a03105be769bf66b277313b432d

INDEX KEYWORDS: Automation; Industrial management; Risk management; Security of data, Continuous risk management; Information processing systems; Information security management systems; Information security managements; Information security risk managements; Process Improvement; Prototypical implementation; Threats and vulnerabilities, Information management
THEME: To present a workflow which focuses and takes into consideration of the ISM aspect

48 Muthaiyah, S., Zaw, T.O.K. Excluded

ISO/IEC 27001 implementation in SMEs: Investigation on management of information assets

(2018) Indian Journal of Public Health Research and Development, 9 (12), pp. 2631-2637.

https://www.scopus.com/inward/record.uri?eid=2-s2.0-85062981112&doi=10.5958%2f0976-5506.2018.02112.5&partnerID=40&md5=d8c4ef0b6d370fc219aef966e8c7aad8
INDEX KEYWORDS: adult; article; confidentiality; female; human; human experiment; major clinical study; male; organization; physician; practice guideline; quantitative analysis; questionnaire; software; telecommunication
EXCLUDED as the scope of article does not meet the research scope.

49 Choi, S., Martins, J.T., Bernik, I. Excluded

Information security: Listening to the perspective of organisational insiders

(2018) Journal of Information Science, 44 (6), pp. 752-767.

https://www.scopus.com/inward/record.uri?eid=2-s2.0-85042361253&doi=10.1177%2f0165551517748288&partnerID=40&md5=40b0c56ae7edf5a13986b95fba7e0472
INDEX KEYWORDS: Personnel training; Information security awareness; Information security managements; Information security practice; Mission statement; Organizational; Qualitative case studies; Strategy as practices, Security of data
EXCLUDED as the scope of article does not meet the research scope.

50 Shamala, P., Chinniah, M., Foozy, C.F.M., Wen, C.C., Mustapha, A., Ahmad, R. Excluded

Information structure framework for ISMS planning and certification: Malaysian data

(2018) Indonesian Journal of Electrical Engineering and Computer Science, 12 (2), pp. 634-640.

https://www.scopus.com/inward/record.uri?eid=2-s2.0-85051831302&doi=10.11591%2fijeecs.v12.i2.pp634-640&partnerID=40&md5=6228910f73ee1b23a7f27b9a355622a6
INDEX KEYWORDS: Certification; Information Security Management System (ISMS); Information structure; Malaysia practitioners
EXCLUDED as the article is single country specific.

51	Kiedrowicz, M., Stanik, J. Method for assessing efficiency of the information security management system (2018) MATEC Web of Conferences, 210, art. no. 04011, . https://www.scopus.com/inward/record.uri?eid=2-s2.0-85055578528&doi=10.1051%2fmatecconf%2f201821004011&partnerID=40&md5=6381e5e8adb5a0ade820bbc1ec8b28f7 INDEX KEYWORDS: Computer circuits; Efficiency; Information systems; Information use; Management information systems; Security of data; Security systems, Efficiency assessment; Functional properties; Information security management systems; Loss of efficiencies; Security; Security configurations; Security measure; Security organizations, Information management THEME: Presentation of an formula on how to evaluate the efficiency of ISMS	Maturity/modelling
52	Antoniou, G.S. A Framework for the Governance of Information Security: Can it be Used in an Organization (2018) Conference Proceedings - IEEE SOUTHEASTCON, 2018-April, art. no. 8479032, . https://www.scopus.com/inward/record.uri?eid=2-s2.0-85056202630&doi=10.1109%2fSECON.2018.8479032&partnerID=40&md5=06ef5ac79e65e4b814d0a52987cae966 INDEX KEYWORDS: Health insurance; Knowledge based systems; Laws and legislation, Chief executive officer; Enterprise governance; Face-to-face interview; Health insurance portability and accountability acts; Information security governance; Information security managements; Information technology departments; Organizational transparency, Security of data THEME: Presentation of an ISM governance model based on the the framework by Posthumus & von Solms	Governance
53	Qusef, A., Arafat, M., Al-Taher, S. Organizational management role in information security management system (2018) ACM International Conference Proceeding Series, art. no. 11, . https://www.scopus.com/inward/record.uri?eid=2-s2.0-85055413264&doi=10.1145%2f3231053.3231064&partnerID=40&md5=aae960a6ba31e1e1c6210a3aec3e3822 INDEX KEYWORDS: Industrial management; Managers; Network security; Project management, Information assets; Information security management systems; Loosely coupled; Management level; Management structure; Organization structures; PDCA cycles, Information management THEME: Reviewing the aspects of organization and organizing in ISM	Governance
54	Tu, C.Z., Yuan, Y., Archer, N., Connelly, C.E. Strategic value alignment for information security management: a critical success factor analysis (2018) Information and Computer Security, 26 (2), pp. 150-170.	Maturity/modelling

https://www.scopus.com/inward/record.uri?eid=2-s2.0-85049908585&doi=10.1108%2fICS-06-2017-0042&partnerID=40&md5=77d43b9ba382231e2e28b5c80fb60af1
INDEX KEYWORDS: Decision making; Factor analysis; Industrial management; Least squares approximations; Security of data, Critical success factor; Design/methodology/approach; Information security controls; Information security managements; Organizational awareness; Partial least square (PLS); Structural equation modeling; Top management support, Information management
THEME: Evaluation of the efficiency and relevance of the ISMS of an organization

55 Ilvonen, I., Thalmann, S., Manhart, M., Sillaber, C. — Excluded

Reconciling digital transformation and knowledge protection: A research agenda

(2018) Knowledge Management Research and Practice, 16 (2), pp. 235-244.

https://www.scopus.com/inward/record.uri?eid=2-s2.0-85046538923&doi=10.1080%2f14778238.2018.1445427&partnerID=40&md5=0fc741c4c0bedd9f4497597d5723e5ca
INDEX KEYWORDS: computer-integrated manufacturing; digital transformation; industry 4.0; knowledge management; Knowledge protection; knowledge sharing; literature review; networks
EXCLUDED as article is not available in research article database (available in a fee based commercial service).

56 Schatz, D., Bashroush, R. — Other

Corporate information security investment decisions: A qualitative data analysis approach

(2018) International Journal of Enterprise Information Systems, 14 (2), pp. 1-20.

https://www.scopus.com/inward/record.uri?eid=2-s2.0-85044759413&doi=10.4018%2fIJEIS.2018040101&partnerID=40&md5=0b94e3e318dfcd6e97eb81f54683f6db
INDEX KEYWORDS: Economics; Information analysis; Security of data, Grounded theory; Information security managements; Problem structuring methods; Qualitative research; Security Economics, Investments
THEME: Presentation of an model on how to evaluate the investments made to ISM by using qualitative data analysis

57 Anttila, J., Jussila, K. — Challenges with ISM

Challenges for the Comprehensive and Integrated Information Security Management

(2018) Proceedings - 13th International Conference on Computational Intelligence and Security, CIS 2017, 2018-January, pp. 586-589.

https://www.scopus.com/inward/record.uri?eid=2-s2.0-85046622641&doi=10.1109%2fCIS.2017.00136&partnerID=40&md5=340aa9bb32e0b9b2485cadbebb5456f9
INDEX KEYWORDS: Artificial intelligence; Data privacy; Industrial management; Management; Managers; Security of data, Business environments; Business integration; Cyber security; Information security managements; Integrated informations; Research and development; Research frameworks; Research initiatives, Information management
THEME: To identify the challenges when implementing an ISMS for an organization

58 Kosutic, D., Pigni, F. — Excluded

Exploring the impact of information security practices on competitive advantage

(2018) Americas Conference on Information Systems 2018: Digital Disruption, AMCIS 2018, .

https://www.scopus.com/inward/record.uri?eid=2-s2.0-85054199502&partnerID=40&md5=96b8bc1318fed1a84dc49d1a6d902d66

INDEX KEYWORDS: Competition; Industrial management; Information systems; Information use, Competitive advantage; Cyber security; Holistic approach; Information security investment; Information security managements; Information security practice; Integrative modeling; Security technology, Security of data
EXCLUDED as article was not found.

59 Wang, P., Ratchford, M. — IRM/ISRM

Integrated methodology for information security risk assessment

(2018) Advances in Intelligent Systems and Computing, 558, pp. 147-150.

https://www.scopus.com/inward/record.uri?eid=2-s2.0-85048516886&doi=10.1007%2f978-3-319-54978-1_20&partnerID=40&md5=0decb8eba1cb57e1befd2a6cc3cd7c3f
INDEX KEYWORDS: Risks; Security of data, Assessment; Information security managements; Information security risk assessment; Information security risks; Qualitative; Qualitative and quantitative approaches; Quantitative; Security, Risk assessment
THEME: To present an integrated model for ISR assessment which uses both quantitative calculation and qualitative evaluation

60 Stewart, A. — Maturity/modelling

A utilitarian re-examination of enterprise-scale information security management

(2018) Information and Computer Security, 26 (1), pp. 39-57.

https://www.scopus.com/inward/record.uri?eid=2-s2.0-85044283978&doi=10.1108%2fICS-03-2017-0012&partnerID=40&md5=42f56b2f20903658ff9bbff95245fa0a
INDEX KEYWORDS: Economics; Investments; Management; Security of data, BS7799; Design/methodology/approach; Diminishing marginal utilities; Information security managements; ISO/IEC; Security management; Spending, Industrial management
THEME: To evaluate the usefullness and practicality of information security practises (based on BS7799)

61 Mendoza, I.E. — Excluded

Information security management as a business strategy and its financial impact

(2017) Economic Growth in Latin America and the Impact of the Global Financial Crisis, pp. 73-91.

https://www.scopus.com/inward/record.uri?eid=2-s2.0-85046052718&doi=10.4018%2f978-1-5225-4981-9.ch005&partnerID=40&md5=1e5f2ede13f336c81162d1edf91a777a
EXCLUDED as article was not found

62	Sidi, F., Daud, M., Ahmad, S., Zainuddin, N., Anneisa Abdullah, S., Jabar, M.A., Suriani Affendey, L., Ishak, I., Mohd Sharef, N., Zolkepli, M., Nur Majdina Nordin, F., Amat Sejani, H., Ramadzan Hairani, S. Towards an Enhancement of Organizational Information Security through Threat Factor Profiling (TFP) Model (2017) Journal of Physics: Conference Series, 892 (1), art. no. 012011, . https://www.scopus.com/inward/record.uri?eid=2-s2.0-85030183862&doi=10.1088%2f1742-6596%2f892%2f1%2f012011&partnerID=40&md5=486d441b26a7eab3e60bf683060f9ae4 INDEX KEYWORDS: Electronic crime countermeasures, Comparative analysis; Incident Management; Information security managements; Intelligent information; Internal operations; Organizational information; Pro-active approach; Security challenges, Security of data THEME: To develop and present a threat actor profiling model for identifying key risks for information security	Key risks
63	Goldes, S., Schneider, R., Schweda, C.M., Zamani, J. Building a viable information security management system (2017) 2017 3rd IEEE International Conference on Cybernetics, CYBCONF 2017 - Proceedings, art. no. 7985763, . https://www.scopus.com/inward/record.uri?eid=2-s2.0-85027885618&doi=10.1109%2fCYBConf.2017.7985763&partnerID=40&md5=f8b67a6713ddf5c7cf37e9aadf2f53c6 INDEX KEYWORDS: Cybernetics; Industrial management; Security of data, Best practices; Business models; Cyber-crimes; De facto standard; Information security management systems; Regulatory focus; System approach, Information management THEME: Building a viable ISMS by comparing and using the commonly known ISM standards	Depiction/development
64	Eloff, M.M., von Solms, S.H. Information security: Process evaluation and product evaluation (2017) IFIP Advances in Information and Communication Technology, 47, pp. 11-18. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85066119953&doi=10.1007%2f978-0-387-35515-3_2&partnerID=40&md5=254dc47d1dd00bad64cdf7e9cdbd0513 INDEX KEYWORDS: Control engineering; Sandwich structures; Standards; Technology transfer, Certification; Code of practice; Evaluation criteria; Guideline; Process Evaluation; Product evaluation, Security of data EXCLUDED as the original article is from year 2000	Excluded
65	Miloslavskaya, N.G., Tolstoy, A.I. Visualization of information security management processes (2017) Scientific Visualization, 9 (5), pp. 117-136. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85039863878&doi=10.26583%2fsv.9.5.10&partnerID=40&md5=57e25bfce4c5f42cfa29cd5d225c50d2	Maturity/modelling

INDEX KEYWORDS: Industrial management; Risk assessment; Risk management; Security of data; Visualization, Information infrastructures; Information security managements; Management process; Management systems; Security maintenance; Visualization of information, Information management
THEME: To present a model where both the technical aspects and the management process are included in the concideration when measuring and evaluating the efficiency of the ISMS of an organization.

66 Zammani, M., Razali, R. — Excluded

Information security management success factors

(2016) Advanced Science Letters, 22 (8), pp. 1924-1929.

https://www.scopus.com/inward/record.uri?eid=2-s2.0-84985015746&doi=10.1166%2fasl.2016.7746&partnerID=40&md5=198a8bbcf02f844197baa8662e70f6fd
INDEX KEYWORDS: Information Security; Information Security Management; Success factors
EXCLUDED as article is not found

67 Park, Y., Teiken, W., Rao, J.R., Chari, S.N. — Excluded

Data classification and sensitivity estimation for critical asset discovery

(2016) IBM Journal of Research and Development, 60 (4), art. no. 7523364, .

https://www.scopus.com/inward/record.uri?eid=2-s2.0-84982733762&doi=10.1147%2fJRD.2016.2557638&partnerID=40&md5=0b1b7f65919be128c1a020a9682a6253
INDEX KEYWORDS: Information retrieval systems; Security of data, Automatic sensitivity; Business documents; Classification scheme; Data classification; External informations; Information security managements; Perimeter protection; Sensitivity estimation, Classification (of information)
EXCLUDED as published by a commercial operator

68 Soomro, Z.A., Shah, M.H., Ahmed, J. — Depiction/development

Information security management needs more holistic approach: A literature review

(2016) International Journal of Information Management, 36 (2), pp. 215-225.

https://www.scopus.com/inward/record.uri?eid=2-s2.0-84948426486&doi=10.1016%2fj.ijinfomgt.2015.11.009&partnerID=40&md5=24b30a7f2cc64cce29fdb933a470011f
INDEX KEYWORDS: Cloud computing; Distributed computer systems; Industrial management; Information retrieval; Management; Managers; Security of data; Security systems, Business - IT alignments; Business information; Information architectures; Information security policies; Managerial practices; Systematic, Information management
THEME: A SLR on which arguments on the need for an holistic ISMS

69	Shameli-Sendi, A., Aghababaei-Barzegar, R., Cheriet, M. Taxonomy of information security risk assessment (ISRA) (2016) Computers and Security, 57, pp. 14-30. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84948421951&doi=10.1016%2fj.cose.2015.11.001&partnerID=40&md5=0bfbf0af64385c4132f0a83279a5655b INDEX KEYWORDS: Information management; Knowledge management; Risk analysis; Risk management; Security of data; Societies and institutions; Taxonomies, Information assets; Information security management systems; Information security risk assessment; Risk assessment methods; Risk based approaches; Security risk assessments; Threat; Vulnerability, Risk assessment THEME: To establish and to present a taxonomy for the terms used in ISRM	IRM/ISRM
70	Naseer, H., Shanks, G., Ahmad, A., Maynard, S. Enhancing information security risk management with security analytics: A dynamic capabilities perspective (2016) Proceedings of the 27th Australasian Conference on Information Systems, ACIS 2016, . https://www.scopus.com/inward/record.uri?eid=2-s2.0-85058057787&partnerID=40&md5=2ebf6f2cb6a74a95f0618ac65a953b50 INDEX KEYWORDS: Competition; Decision making; Enterprise resource management; Information systems; Information use; Law enforcement; Security of data; Turbulence, Competitive advantage; Dynamic capabilities; Environmental turbulences; Information security managements; Information security risk managements; Organizational information; Security Analytics; Risk management THEME: A study on how the use of security analytics capabilities can be used to benefit the organizations ISRM and to benefit the organization to gain competitive advantage	Other
71	Haufe, K., Colomo-Palacios, R., Dzombeta, S., Brandis, K., Stantchev, V. A process framework for information security management (2016) International Journal of Information Systems and Project Management, 4 (4), pp. 27-47. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85007568894&doi=10.12821%2fijispm040402&partnerID=40&md5=1e2d0d7977eb9e3d9d90cd05f84ae5cf INDEX KEYWORDS: Information security management systems; ISMS; ISO 27000; IT resources; IT security; Resource management process; Security standards THEME: Work focusing to idenfify those core processes which are needed and the foundation for organizations ISMS	Depiction/development
72	Haufe, K., Colomo-Palacios, R., Dzombeta, S., Brandis, K., Stantchev, V. Security Management Standards: A Mapping (2016) Procedia Computer Science, 100, pp. 755-761. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85006894223&doi=10.1016%2fj.procs.2016.09.221&partnerID=40&md5=b5227cde9f4b3528f19e3bee53d2e02e	Key activities

INDEX KEYWORDS: Cost effectiveness; Industrial management; Information systems; Management information systems; Mapping; Processing; Project management; Security of data, Information security management systems; Information security managements; International standards; ISMS; IT governance; Process framework; Process mapping; Security management, Information management
THEME: Work focusing on the mapping of core ISMS processes. The article states that there is no such as ISMS process framework and attempts to map such based on certain security standards

73 Haufe, K., Colomo-Palacios, R., Dzombeta, S., Brandis, K., Stantchev, V. — Key activities

ISMS Core Processes: A Study

(2016) Procedia Computer Science, 100, pp. 339-346.

https://www.scopus.com/inward/record.uri?eid=2-s2.0-85006867358&doi=10.1016%2fj.procs.2016.09.167&partnerID=40&md5=1058e4fe8aee268ca27f198ee73ebc6f
INDEX KEYWORDS: Cost effectiveness; Information systems; Management information systems; Processing; Project management; Security of data, Basic elements; Information security management systems; ISMS; IT governance; Key elements; Process framework; Security measure; Study, Information management
THEME: The article attempts to identify the core processes incremental for a viable ISMS

74 Cárdenas-Solano, L.-J., Martínez-Ardila, H., Becerra-Ardila, L.-E. — Excluded

Information security management: A bibliographic review [Gestión de seguridad de la información: Revisión bibliográfica]

(2016) Profesional de la Informacion, 25 (6), pp. 931-948.

https://www.scopus.com/inward/record.uri?eid=2-s2.0-85003561569&doi=10.3145%2fepi.2016.nov.10&partnerID=40&md5=7ab2c6f952bf8f13a53976dee27bc9d4
INDEX KEYWORDS: Best practices; Bibliography; Frameworks; Information security; Information security culture; Information security management; Knowledge management; Literature review; State of the art
EXCLUDED as not available in English.

75 Shamala, P., Ahmad, R. — IRM/ISRM

Generic taxonomy of assets identification during risk assessment in information security management

(2016) International Business Management, 10 (17), pp. 3982-3991.

https://www.scopus.com/inward/record.uri?eid=2-s2.0-84988917274&partnerID=40&md5=b5de67491ea5471e545d0b8d699a0068
INDEX KEYWORDS: Asset identification; Information leakage; Non-technical assets; Taxonomy; Technical assets; Traditional ISRA
THEME: Identification and creation of taxonomy used in ISRM activities

76 Brunner, M. — Automation/workflow

RiskFlows - Continuous risk-driven workflows and decision support in Information Security Management Systems

(2016) CEUR Workshop Proceedings, 1603, .

https://www.scopus.com/inward/record.uri?eid=2-s2.0-84977524849&partnerID=40&md5=0af818d654eabf453ecf40dbbf1794e9

INDEX KEYWORDS: Decision making; Decision support systems; Industrial management; Information systems; Management information systems; Risk management; Security of data; Systems engineering, Decision supports; Information security management systems; Information security risk managements; Process automation; Risk model, Information management

THEME: Description of workflows where information security centric information and actions will be included

77 Olijnyk, N.V. — Other

A quantitative examination of the intellectual profile and evolution of information security from 1965 to 2015

(2015) Scientometrics, 105 (2), pp. 883-904.

https://www.scopus.com/inward/record.uri?eid=2-s2.0-84945479833&doi=10.1007%2fs11192-015-1708-1&partnerID=40&md5=d9b61e17d7eb8cbbd1f9e9b00ad58631

INDEX KEYWORDS: Co-word analysis; Computer security; Cyber security; Network security; Specialty development

THEME: Study on the development of ISM related literature between years 1965 and 2015

78 Mattos, M.M., Heckmann, J.R., Da Silva, P.F. — Taxonomy

An Ontology to the Information Security Management

(2015) Proceedings - 2015 9th International Conference on Complex, Intelligent, and Software Intensive Systems, CISIS 2015, art. no. 7185206, pp. 326-329.

https://www.scopus.com/inward/record.uri?eid=2-s2.0-84959455121&doi=10.1109%2fCISIS.2015.46&partnerID=40&md5=ad9a847769a52fb696ebc5e0bc2845b7

INDEX KEYWORDS: Industrial management; Knowledge management; Ontology; Security of data, Information security managements; Ontology construction, Information use

THEME: Attempt to develop the ontology for ISM which could allow the knowledge management within ISM in organizations working with elements of explicit knowledge and with the tacit knowledge of ISM related consultants

79 Holik, F., Horalek, J., Neradova, S., Zitta, S., Novak, M. — Standards

Methods of deploying security standards in a business environment

(2015) Proceedings of 25th International Conference Radioelektronika, RADIOELEKTRONIKA 2015, art. no. 7128984, pp. 411-414.

https://www.scopus.com/inward/record.uri?eid=2-s2.0-84942810459&doi=10.1109%2fRADIOELEK.2015.7128984&partnerID=40&md5=4a69103f3965a3e11fc1d133a63addb0
INDEX KEYWORDS: Risk analysis; Risk assessment; Security of data; Technology transfer, Automotive companies; Building blockes; Business environments; Financial transactions; Information protection; Information security management systems; ISMS implementation; Security standards, Information management
THEME: Implementing the ISO/IEC 27001 standard for the target organization

80 Ilvonen, I., Jussila, J., Karkkainen, H., Paivarinta, T. — Knowledge

Knowledge security risk management in contemporary companies - Toward a proactive approach

(2015) Proceedings of the Annual Hawaii International Conference on System Sciences, 2015-March, art. no. 7070291, pp. 3941-3950.

https://www.scopus.com/inward/record.uri?eid=2-s2.0-84944191417&doi=10.1109%2fHICSS.2015.472&partnerID=40&md5=f175a171b736ade3e952f2797d04fcfc
INDEX KEYWORDS: Security of data, External knowledge; Information assets; Information security managements; Knowledge creations; Knowledge securities; Organizational knowledge; Pro-active approach; Proactive management, Risk management
THEME: Presenting a model on proactive process for managing knowledge management risk

81 Nancylia, M., Mudjtabar, E.K., Sutikno, S., Rosmansyah, Y. — Standards

The measurement design of information security management system

(2015) Proceedings of 2014 8th International Conference on Telecommunication Systems Services and Applications, TSSA 2014, art. no. 7065914, .
https://www.scopus.com/inward/record.uri?eid=2-s2.0-84937232135&doi=10.1109%2fTSSA.2014.7065914&partnerID=40&md5=7b3b9c298d9719e429e693bc25722eab
INDEX KEYWORDS: Industrial management; Information use; Measurement; Security of data; Telecommunication services, effectiveness; Information security management systems; Measurement designs; Security management; Information management
THEME: Development of a method to measure the effectiveness of ISMS based on ISO27001 standard.

82 Baras, D.S.A., Othman, S.H., Ahmad, M.N., Ithnin, N. — Taxonomy

Towards managing information security knowledge through metamodelling approach

(2015) Proceedings - 2014 International Symposium on Biometrics and Security Technologies, ISBAST 2014, art. no. 7013140, pp. 310-315.
https://www.scopus.com/inward/record.uri?eid=2-s2.0-84922784543&doi=10.1109%2fISBAST.2014.7013140&partnerID=40&md5=74e55254ac9d4b9204ea780a9d874c5e
INDEX KEYWORDS: Industrial management; Models, Conceptual model; Current situation; Information assets; Information security managements; knowledge; Knowledge domains; Knowledge-sharing; Meta model, Security of data
THEME: Development and presentation of a metamodel for terminology used in ISM.

83 Ahmad, A., Tscherning, H., Bosua, R., Scheepers, R.
Guarding against the erosion of competitive advantage: A knowledge leakage mitigation model
(2015) 2015 International Conference on Information Systems: Exploring the Information Frontier, ICIS 2015, .
https://www.scopus.com/inward/record.uri?eid=2-s2.0-85126607540&partnerID=40&md5=ce436c23e5e6561cc6574e0c03b04ca3
INDEX KEYWORDS: Competition; Economic and social effects; Erosion; Information use; Knowledge based systems; Risk management; Security of data, Competitive advantage; Information security managements; Knowledge management capabilities; Knowledge-intensive organizations; Organizational strategy; Resource-based theory; Security risk managements, Knowledge management
THEME: Presentation of a model to prevent knowledge leakage to protect the knowledge assets of an organization.
Knowledge

84 Alshaikh, M., Maynard, S.B., Ahmad, A., Chang, S.
Information security policy: A management practice perspective
(2015) ACIS 2015 Proceedings - 26th Australasian Conference on Information Systems, .
https://www.scopus.com/inward/record.uri?eid=2-s2.0-85049589391&partnerID=40&md5=7e78a9c53378c66fac6ac81c4c2870df
INDEX KEYWORDS: Information security policy; Policy development; Security policy management practice
THEME: Study focusing on how the information security policy should be developed from management activity perspective.
Key activities

85 Agudelo, C.A., Bosua, R., Ahmad, A., Maynard, S.B.
Understanding knowledge leakage & BYOD (bring your own device): A mobile worker perspective
(2015) ACIS 2015 Proceedings - 26th Australasian Conference on Information Systems, .
https://www.scopus.com/inward/record.uri?eid=2-s2.0-85041732057&partnerID=40&md5=0bd5af593611ac4a161ef623d7d4f383
INDEX KEYWORDS: Bring Your Own Device; BYOD; Information Security Management; Knowledge leakage; Mobile Computing
THEME: Study on the phenomenon of Bring Your Own Device (BYOD) from the context of knowledge leakages where the purpose is to understand why it happens and on how organizations can protect them self's against these proceedings.
Key risks

86 Delak, B., Damij, N.
Knowledge risk assessments
(2015) Proceedings of the European Conference on Knowledge Management, ECKM, 0, pp. 997-1004.
https://www.scopus.com/inward/record.uri?eid=2-s2.0-85006827127&partnerID=40&md5=23ce218f1e1f2f275321f8b6ccd7aeb9
Knowledge

INDEX KEYWORDS: Knowledge management; Project management; Risk management; Security of data, Assessment approaches; Critical knowledge; Information security management systems; International standard organizations; Knowledge; Knowledge capture; Knowledge-sharing; Literature reviews, Risk assessment
THEME: Work attempting to combine two different activities which are; the identification of organizations knowledge assets and the risk assessment process to map the knowledge risks (here knowledge management risk assessement).

87 Pirnea, I.C., Hohan, A.I., Olaru, M. — Excluded

Development of a business relevant information security management system using the Balanced Scorecard and the EFQM Excellence Model
(2015) Proceedings of the 25th International Business Information Management Association Conference - Innovation Vision 2020: From Regional Development Sustainability to Global Economic Growth, IBIMA 2015, pp. 1075-1084.
https://www.scopus.com/inward/record.uri?eid=2-s2.0-84947545738&partnerID=40&md5=38e2e227151b73418330db1bb0f93aee

INDEX KEYWORDS: Competition; Economics; Industrial management; Information use; Planning; Regional planning; Regulatory compliance; Security of data; Strategic planning; Sustainable development, Balanced scorecards; Balancedl scorecard; Business administration; Business excellence; Competitive advantage; Doctoral research; Information security management systems; Information security managements, Information management
EXCLUDED as article was not found.

88 Nazareth, D.L., Choi, J. — Maturity/modelling

A system dynamics model for information security management

(2015) Information and Management, 52 (1), pp. 123-134.

https://www.scopus.com/inward/record.uri?eid=2-s2.0-84919791641&doi=10.1016%2fj.im.2014.10.009&partnerID=40&md5=247062dbac72d3900ae85f8e13da2e95
INDEX KEYWORDS: Decision making; Industrial management; Information management; Investments; System theory, Information security managements; Security detection; Security investments; Security management strategy; Simulation; System Dynamics; System dynamics model; Vulnerability reductions, Security of data
THEME: Development of a model for ISM where the financial investements and costs are incorporated to allow the more holistic understanding of the impact of investments in ISM.

89 Warkentin, M., Mutchler, L. — Other

Behavioral information security management

(2014) Computing Handbook, Third Edition: Information Systems and Information Technology, pp. 54-1-54-20.

https://www.scopus.com/inward/record.uri?eid=2-s2.0-85054714834&doi=10.1201%2fb16768&partnerID=40&md5=64828fd8ad912251ef3063abf92ba69f

INDEX KEYWORDS: Behavioral research; Computer crime; Computer system firewalls; Intrusion detection; Malware; Security systems, Academic research; Behavioral control; Behavioral information security; Information assets; Intrusion Detection Systems; Protect information; Security practitioners; Technical control, Computer viruses
THEME: Article focusing on to desribe the inside threat for organizations. The insider threat and related human behavioural theories and linked to the prevention of the described insider threats.

90 Ng, Z.X., Ahmad, A., Maynard, S.B. — IRM/ISRM

Information security management: Factors that influence security investments in SMES

(2014) Proceedings of the 11th Australian Information Security Management Conference, ISM 2013, pp. 60-74.

https://www.scopus.com/inward/record.uri?eid=2-s2.0-84917673059&partnerID=40&md5=b1ce57b5fcff4083c09eeec3e9c29c32

INDEX KEYWORDS: Decision making; Decision theory; Economics; Industrial management; Risk assessment; Risk management; Security systems; Societies and institutions, Information security investment; Information security managements; Information security practice; Medium sized organizations; Security expenditures; Security risk assessments; Small to medium enterprise; SME, Security of data
THEME: Study on security investments in Small and Medium sized enterprices and on the role of ISR in the ISM related decission making (survey included 5 SME organizations).

91 Bergström, E., Åhlfeldt, R.-M. — Information classification

Information classification issues

(2014) Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 8788, pp. 27-41.
https://www.scopus.com/inward/record.uri?eid=2-s2.0-84910065925&doi=10.1007%2f978-3-319-11599-3_2&partnerID=40&md5=88ba41700740f543c7ae694673c3666b
INDEX KEYWORDS: Information classification; Information security management systems; Systematic literature review

THEME: Information classification has seen as a key activity in information protection. There are many challenges influensing on the effectiveness of information classification. The article tries to answer to these challenges by using a SLR.

92 Hassan, N.H., Ismail, Z., Maarop, N. — Knowledge

Understanding Relationship Between Security Culture and Knowledge Management

(2014) Lecture Notes in Business Information Processing, 185 LNBIP, pp. 397-402.

https://www.scopus.com/inward/record.uri?eid=2-s2.0-84907324548&doi=10.1007%2f978-3-319-08618-7_38&partnerID=40&md5=a435585e22fce1d20530c0699003f4ff
INDEX KEYWORDS: Health care; Human engineering; Industrial management; Security of data; Societies and institutions, Health care informatics; Healthcare industry; Healthcare organizations; Information security incidents; Information security managements; Knowledge creations; Knowledge use; Knowledge-sharing, Knowledge management

THEME: The article attempts to explain the relationship with knowledge managment and security culture in health care sector. The leading thought is, that the sharing of relevant knowledge will also benefit the security culture of an organization. This as the knowledge creation, sharing and usage will influence on security behaviour and thus impact the security culture of an organization.

93 Asosheh, A., Hajinazari, P., Khodkari, H. — Standards

A practical implementation of ISMS

(2013) International Journal of Information Science and Management, 11 (SPL.ISS.), pp. 111-126.

https://www.scopus.com/inward/record.uri?eid=2-s2.0-84891086125&partnerID=40&md5=7e5753ad4568ce77686b596aedd79ef0

THEME: Review of the most common ISM standards and a practical guidance on how an ISM standard should be implemented to an organization.

94 Mir, M.S., Wani, S., Ibrahim, J. — Challenges with ISM

Critical information security challenges: An appraisal

(2013) 2013 5th International Conference on Information and Communication Technology for the Muslim World, ICT4M 2013, art. no. 6518890, .
https://www.scopus.com/inward/record.uri?eid=2-s2.0-84879065860&doi=10.1109%2fICT4M.2013.6518890&partnerID=40&md5=2a8e619f5a6415cbba94acb0a4a31ca1
INDEX KEYWORDS: Credentials; Critical challenges; Identity theft; Information leakage; Security issues; Security policy, Information dissemination; Information technology; Security of data; Societies and institutions, Crime
THEME: A study aiming to identify the most critical security issues relating to information security. The study was performed by performing a interview with different IT and ISM experts.

95 Hugl, U. — Challenges with ISM

Crying for the moon? current challenges in corporate information security management

(2013) IC3K 2013; KDIR 2013 - 5th International Conference on Knowledge Discovery and Information Retrieval and KMIS 2013 - 5th International Conference on Knowledge Management and Information Sharing, Proc., pp. 579-586.
https://www.scopus.com/inward/record.uri?eid=2-s2.0-84887692181&doi=10.5220%2f0004700605790586&partnerID=40&md5=d442756de6e4716a7bf0288bea63e5ea
INDEX KEYWORDS: Big data; Cloud computing; Industrial management; Information retrieval; Knowledge management; Personal computing; Security of data, Corporate assets; Corporate information; Industrial espionage; Intelligence gathering; Organisational; Prevention measures; Social business; Social engineering, Information dissemination

96 Stoll, M., Felderer, M., Breu, R. — Depiction/development

Information management for holistic, collaborative information security management

(2013) Lecture Notes in Electrical Engineering, 151 LNEE, pp. 211-224.

https://www.scopus.com/inward/record.uri?eid=2-s2.0-84865959283&doi=10.1007%2f978-1-4614-3558-7_17&partnerID=40&md5=439506774e093bf628950cf98d97880f
INDEX KEYWORDS: Collaborative information; Control objectives for information and related technologies; Critical success factor; Differentiators; Information security management systems; Information system integration; Information technology infrastructure library (ITIL); ISO/IEC; Oriented direction; Research approach, Data processing; Industrial management; Information technology; Security of data; Taxonomies, Information management
THEME: A work focusing to develop a framework which would address both the IM (Information Management) and ISM needs and thus offer a holistic model for different organizations for their IT and information security needs.

97 Korhonen, K.J., Hiekkanen, K., Mykkänen, J. — Governance

Information security governance

(2012) Strategic and Practical Approaches for Information Security Governance: Technologies and Applied Solutions, pp. 53-66.

https://www.scopus.com/inward/record.uri?eid=2-s2.0-84898275073&doi=10.4018%2f978-1-4666-0197-0.ch004&partnerID=40&md5=6a7d130a15ebe38574b6ac9e66c2deec
THEME: to desribe the role and need for governance in ISM and to present a reference model for ISM related governance.

98 Ramli, N.A., Aziz, N.A. — IRM/ISRM

Risk identification for an information security management system implementation

(2012) SECURWARE 2012 - 6th International Conference on Emerging Security Information, Systems and Technologies, pp. 57-61.

https://www.scopus.com/inward/record.uri?eid=2-s2.0-84881450672&partnerID=40&md5=841d7d08cf80ad58a9bd92b17ca6adbc
INDEX KEYWORDS: Asset identification; Information security management systems; Information security risks; International standards; ISMS; Risk Identification; Threat; Threat identification, Industrial management; Regulatory compliance; Risk assessment; Security of data, Information management
THEME: A work attenpting to develop a concept on how key asset identification and related threat identification could be used in the ISMS implementation.

99 Anttila, J., Jussila, K., Kajava, J., Kamaja, I. — Standards

Integrating ISO/IEC 27001 and other managerial discipline standards with processes of management in organizations

(2012) Proceedings - 2012 7th International Conference on Availability, Reliability and Security, ARES 2012, art. no. 6329214, pp. 425-436.
https://www.scopus.com/inward/record.uri?eid=2-s2.0-84869450574&doi=10.1109%2fARES.2012.93&partnerID=40&md5=249c01a7edb110232fdf356612573acb
INDEX KEYWORDS: Business environments; Business integration; Business leaders; Business performance; Business Process; Information security management systems; Information security managements; International management; ISO/IEC; Management systems;

managerial disciplines; Organizational practices; Research approach; Social communities; Theoretical foundations, Industrial management; Managers; Security of data; Standardization, Information management
THEME: Review and presentation of key ISM standards and on how these can be utilized in the context of business management.

100 Tatar, Ü., Karabacak, B. — IRM/ISRM

An hierarchical asset valuation method for information security risk analysis

(2012) International Conference on Information Society, i-Society 2012, art. no. 6284977, pp. 286-291.

https://www.scopus.com/inward/record.uri?eid=2-s2.0-84867391102&partnerID=40&md5=f4eec6f5f6d470835f71dfcbac548737

INDEX KEYWORDS: Asset identification; Asset valuation; Business Process; Cyber threats; Information security managements; Security risk analysis, Industrial management; Information science; Information technology; Security of data, Risk analysis
THEME: Attempt to develope a model for including the valuation of the assets as a part if ISRM.

101 Dagorn, N. — Excluded

Information security management: A state of the art [Le management de la sécurité de l'information: Un état de l'art]

(2012) 17th Symposium of the Association Information and Management 2012, AIM 2012, pp. 101-110.

https://www.scopus.com/inward/record.uri?eid=2-s2.0-84995677846&partnerID=40&md5=b5449a9f8a9b4d868f2c79e5e9bf34bb

INDEX KEYWORDS: Industrial management; Security of data, Academic journal; Academic research; Information security managements; Literature reviews; Research focus; State of the art, Information management
EXCLUDED as article is not available in English

102 Da Silva, P.F., Otte, H., Todesco, J.L., Gauthier, F.A.O. — Excluded

An ontology for information security management [Uma ontologia para gestão de segurança da informaç ão]

(2011) CEUR Workshop Proceedings, 776, pp. 141-146.

https://www.scopus.com/inward/record.uri?eid=2-s2.0-84891610678&partnerID=40&md5=fdb7bddc0beb45f9e4e5e844132ab741

INDEX KEYWORDS: Information security managements; Management information; Security environments, Knowledge management; Semantic Web; Semantics, Security of data
EXCLUDED as article is not available in English

103 Modiri, N., Sobhanzadeh, Y.M. — Standards

Information security management

(2011) Proceedings - 2011 International Conference on Computational Intelligence and Communication Systems, CICN 2011, art. no. 6112913, pp. 481-484. Cited 1 time.

https://www.scopus.com/inward/record.uri?eid=2-s2.0-84856159555&doi=10.1109%2fCICN.2011.100&partnerID=40&md5=19422f4c73ea9a4c886cb340852863f9
INDEX KEYWORDS: COBIT; Information security management; ISO/IEC 27001; Mapping; Organization; PDCA cycle

THEME: Presentation of the different ISM standards belonging to the ISO/IEC 27000 series

104 Yazdanifard, R., Musa, M.G., Molalmu, T. — Depiction/development

The basics issues on the security information management practices in organizational environment

(2011) International Conference on Management and Service Science, MASS 2011, art. no. 5999086, .

https://www.scopus.com/inward/record.uri?eid=2-s2.0-80052903235&doi=10.1109%2fICMSS.2011.5999086&partnerID=40&md5=b0e4fe3c2e8ab3c8bf0416a2853744bd
INDEX KEYWORDS: Facility security; Information management; Information Security and management

THEME: Attempt to identify the key components of an ISM and on how these should be used (establish information management and information security - develop strategy and plan - implement security controls - monitor & review - improve)

105 Aksentijevi?, S., Tijan, E., Agati?, A. — Standards

Information security as utilization tool of enterprise information capital

(2011) MIPRO 2011 - 34th International Convention on Information and Communication Technology, Electronics and Microelectronics - Proceedings, art. no. 5967277, pp. 1391-1395. Cited 4 times.
https://www.scopus.com/inward/record.uri?eid=2-s2.0-80052300303&partnerID=40&md5=3abf46ff0f17e4c3ec2bf26a6decba5e

THEME: Combination of an applied model of information hierarchy in combination with different ISM standards. The approach for the work is to demonstrate on how information security can be used as a method or a tool to map the information assets of an organisation.

106 Ray, A.W. — Excluded

Rethinking Information Systems Security

(2011) The Oxford Handbook of Management Information Systems: Critical Perspectives and New Directions.

https://www.scopus.com/inward/record.uri?eid=2-s2.0-84924872605&doi=10.1093%2foxfordhb%2f9780199580583.003.0020&partnerID=40&md5=dfb5e1cc83c4daaf371ce518254dfa9e
INDEX KEYWORDS: High-level policy; Information security management; Responsibilities; Risks; Security risk

EXCLUDED as article was not found.

107 Abbas, H., Magnusson, C., Yngstrom, L., Hemani, A. — Other

Addressing dynamic issues in information security management

(2011) Information Management & Computer Security, 19 (1), pp. 5-24. Cited 19 times.

https://www.scopus.com/inward/record.uri?eid=2-s2.0-79955624015&doi=10.1108%2f09685221111115836&partnerID=40&md5=d45a57bc4732e560d906b125710a7d73

INDEX KEYWORDS: Data security; Generation and dissemination of information; Information systems
THEME: Study of a one technological solution relating to authentication as a part of ISM.

108 Kuokkanen, P. — Depiction/development
Operations management of information security at enterprise levels
(2010) 9th European Conference on Information Warfare and Security 2010, ECIW 2010, pp. 160-167.
https://www.scopus.com/inward/record.uri?eid=2-s2.0-84873158007&partnerID=40&md5=e48da9cef08bc97fd267c4f8a670dd11
INDEX KEYWORDS: Information security governance and management; Security management for enterprises; Strategic leadership
THEME: Article presents a framework on how to build the operations management as a part of ISMS.

109 Wipawayangkool, K. — Excluded
Strategic role of human resource management in information security management
(2010) 16th Americas Conference on Information Systems 2010, AMCIS 2010, 7, pp. 5300-5306.
https://www.scopus.com/inward/record.uri?eid=2-s2.0-84870281464&partnerID=40&md5=f80b046fbb0c1eb04bfcb904ba4dc59d
INDEX KEYWORDS: Collaboration; Human resources; Information security; Sustainable competitive advantage; Transactive memory systems
EXCLUDED as article was not found.

110 Huang, C.D. — Maturity/modelling
Optimal investment in information security: A business value approach
(2010) PACIS 2010 - 14th Pacific Asia Conference on Information Systems, pp. 444-451. Cited 1 time.
https://www.scopus.com/inward/record.uri?eid=2-s2.0-84862964150&partnerID=40&md5=f1940b7eb50e29f63c14e79e527c9183
INDEX KEYWORDS: Business value; Information security investment; IT security; Optimal investment
THEME: Work addressing the gap in the capabilities to evaluate the optimal investments in ISM. The work presents a business value calculation for managing information security in an organizational context.

111 Whitman, M.E., Mattord, H.J. — Key risks
The enemy is still at the gates: Threats to information security revisited
(2010) Proceedings of the 2010 Information Security Curriculum Development Annual Conference, InfoSecCD'10, pp. 95-96. Cited 4 times.

https://www.scopus.com/inward/record.uri?eid=2-s2.0-79952502906&doi=10.1145%2f1940941.1940963&partnerID=40&md5=7bfdf81d3341faeed352834e46202d76
INDEX KEYWORDS: Information security management; Information security metrics; Information security standards; Information security threats
THEME: Work focusing to identify and to describe the relevant and topical information security related threats.

112 Fruehwirth, C., Biffl, S., Tabatabai, M., Weippl, E. — Other

Addressing misalignment between information security metrics and business-driven security objectives

(2010) 6th International Workshop on Security Measurements and Metrics, MetriSec 2010, art. no. 1853927, . Cited 7 times.

https://www.scopus.com/inward/record.uri?eid=2-s2.0-78649431229&doi=10.1145%2f1853919.1853927&partnerID=40&md5=304f94f8d99cf42e7e2221527c9c6fa7
INDEX KEYWORDS: business-driven ITSM; security management; security metrics

THEME: Works presents a method with a tool on how to develop such security metrics which can be aligned with business management. supports matching security metrics with the objectives and capabilities of a company.

113 Broser, C., Fritsch, C., Gmelch, O. — Other

Towards information security management in collaborative networks

(2010) Proceedings - 21st International Workshop on Database and Expert Systems Applications, DEXA 2010, art. no. 5591102, pp. 359-363. Cited 3 times.
https://www.scopus.com/inward/record.uri?eid=2-s2.0-78449312856&doi=10.1109%2fDEXA.2010.76&partnerID=40&md5=aceb63fd3aef5e8d7b96dfe5a84eeef9
INDEX KEYWORDS: Collaborative network; Compliance; Privacy; Security

THEME: Article addresses the needs and challenges relating to the work done in collaborative networks. It also presents a solution "SPIKE platform" which can be used in short- and medium-term collaborative projects.

114 Sánchez, L.E., Santos-Olmo, A., Fernández-Medina, E., Piattini, M. — Depiction/development

Building ISMS through the reuse of knowledge

(2010) Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 6264 LNCS, pp. 190-201. Cited 4 times.
https://www.scopus.com/inward/record.uri?eid=2-s2.0-78049357355&doi=10.1007%2f978-3-642-15152-1_17&partnerID=40&md5=78e926e82dd848dd2c1dc5302af47151
INDEX KEYWORDS: ISMS; ISO27001; Pattern; Security Knowledge Reuse; SME

THEME: To present a model on how Small and Medium Sized organizations can build their ISMS by re-using knowledge created from other occasions and projects (or by other organizations) and therefore allowing a implementation of an ISMS for and SME in a cost and resource effective way.

115 Anttila, J., Kajava, J. Standards

Challenging IS and ISM standardization for business benefits

(2010) ARES 2010 - 5th International Conference on Availability, Reliability, and Security, art. no. 5438059, pp. 416-421. Cited 2 times.

https://www.scopus.com/inward/record.uri?eid=2-s2.0-77952378628&doi=10.1109%2fARES.2010.113&partnerID=40&md5=cd37fa871b7f34e9b56b62e1d3218810
INDEX KEYWORDS: Business integration; Haste; Human aspects and behavior; Information security management
THEME: Critical view on the use, benefits, and implementation of international information security standards on an organization.

116 Jo, H., Kim, S., Won, D. Standards

A study on comparative analysis of the information security management systems

(2010) Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 6019 LNCS (PART 4), pp. 510-519. Cited 3 times.
https://www.scopus.com/inward/record.uri?eid=2-s2.0-77952314021&doi=10.1007%2f978-3-642-12189-0_44&partnerID=40&md5=b935a303f64870b2783c66ff3e761c85
INDEX KEYWORDS: Information Security Check; Information Security Evaluation; Information Security Evaluation Process; Information Security Management System (ISMS)
THEME: Presentation and comparison of different international standards used in ISM.