Identification of specialist literature in the security field

Analysis and classification of standard literature
and publishing behavior for security management

A master's thesis

presented in the University of Applied Sciences in Brandenburg an der Havel

in partial fulfillment of the requirements for the degree Master of Sciences

By

Roberto Vera

Graduate Program in Security Management

Brandenburg University of Applied Sciences

2010

Thesis Committee

Prof. Dr. Sachar Paulus
Prof. Dr. Friedrich Holl

Table of contents

Abstract

The present work researches the existing publications on security management, assesses the relevance of selected literature in relation to corporate security and its subdisciplines and gives some recommendations for the elaboration of prospective security publications. The addressed publications are specialist books, academic journals and specialist magazines. The first part of the work defines the term security management from the perspective of this study in order to find a homogenous scheme, on which the literature research and analysis will be based. The central part of the work assesses the collected publications and determines their relevance with the security management outline defined in this work. The closing part gathers the results of the research and analysis, in order to determine characteristics and shortcomings of the existing literature, and proposes structural improvements for future publications.

Die vorliegende Arbeit recherchiert die bestehenden Veröffentlichungen zum Sicherheitsmanagement, bewertet die Relevanz der ausgewählten Literatur in Bezug auf Unternehmenssicherheit und ihre Teildisziplinen und gibt einige Empfehlungen für die Ausarbeitung künftiger Sicherheitsveröffentlichungen. Die gezielte Publikationen sind Fachbücher, wissenschaftliche Fachzeitschriften und Fachmagazine. Der erste Teil der Arbeit definiert den Begriff Sicherheitsmanagement aus der Perspektive der vorliegenden Studie, um ein einheitliches Schema, auf dem die Literaturrecherche und Analyse beruhen, festzulegen. Der zentrale Teil der Arbeit bewertet die gesammelten Publikationen und bestimmt deren Bedeutung im Sinne des in dieser Arbeit definierten Sicherheitsmanagementaufbaus. Der abschließende Teil sammelt alle Ergebnisse, um Schwachpunkte und Eigenschaften der Literatur zu bestimmen, und gibt strukturelle Vorschläge für künftige Veröffentlichungen.

1. Introduction

The growing networking and globalization of industries, markets and companies establish new scenarios for the strategic and operational management of any organization. Within a company, the field of corporate security management is a clear example of this developing globalization process. Whereas in earlier times, the solution for many corporate threats was property protection and safety measures in a local level, the multinational shape of small and big enterprises create new challenges for the protection of assets and processes and management of operational risks. The transformation in this terrain entails a demand of education programs and professionals with a holistic background on corporate security. These qualifications require knowledge and qualifications in a multidisciplinary environment ranging between property protection, information security, crisis management and occupational health to name a few. One characteristic feature of establishing a new discipline in the academic world with undergraduate and graduate programs is the appropriate support through literature, research and academic publications. In Germany, the industry demand in this field has been reflected in the creation of bachelor and master programs either focused to the whole thematic of corporate security or concentrating on some key disciplines of security management. Nevertheless, whether there has been an adequate literature supply in German language for the developing discipline was uncertain. The main objectives of the present work is to determine the existence of security literature, evaluate the relevance of the publication in function of a security management outline and define a set of recommendations for future publications in this field. The established sources for scholar research are specialist books and academic journals. Even though the offer of literature can range nowadays to valuable electronic

sources in Internet or other media, the present research set the limits on the printed domain incorporating additionally non-academic regular periodicals, referred to as specialist magazines, which, without the rigorous peer-review editorial process of academic journals, fall into the scope of a proposed security management library. Based on a primary research on the existence of security literature and the bibliographic references of the available media in this field, it is taken for granted that there is some German-speaking literature on the field but the number, quality, scope and relevance of the literature on its current state has not been treated so far on a methodological basis.

The structure of the work follows roughly the development of the overall investigation through an opening chapter and three core chapters for literature research, literature analysis and publishing recommendations. The opening chapter 2 deals exclusively with the definition of security management followed in this research. For definition it should not be understood a mere formal statement defining security management as an academic discipline, but it represents the fundamental outline, on which the research is developed. The definition starts thus with a general framework on the necessity of a security management and the understanding of operational threats a typical organization is confronted to. The analysis recognizes two sets of topics. The fundamental topics deal with the general structure of security management analyses and methodologies, whereas the second set of subdisciplinary topics refer to their actual application on certain fields such as physical or information security. At the end of that chapter, it is stated that a possible perspective is to categorize the fundamental topics in preventive and reactive managerial aspects represented by three main areas namely risk identification, measures identification and implementation and incident handling. The wide range of corporate security applications were accordingly categorized the subdisciplines of physical security, information security, infrastructure resilience and persons safety and security. A special aspect of both fundamentals and subdiscipline areas were given by public and private third party requirements such as legislation and industry standards. Chapter 3 deals simply with the library research of security management material for the three types of publications: specialist books, academic journals and specialist magazines. It will be explained that although the research scope is the German-speaking literature, an exception is done for academic journals. Given that English has become the lingua franca in many fields including the academia and industry, the bibliography research for journals scopes additionally literature published in English and in fact not necessarily restricted to the German-speaking region as publication countries, i.e.

English-speaking journals from any source will be considered. Other than books and journals, which should contain a holistic approach to corporate security, specialist magazines are researched according to the category they belong to; that is, any magazine dealing with any of the four smaller domains of the subdisciplines will be surveyed. In this sense, the magazines investigation returns four sets of publications for the defined subdisciplines. The following chapter 4 deals with the literature analysis of the material found for all three types of publications. The analyses are made based on the definition of security management made in the first chapters through a methodology based on the structure of fundamental and subdisciplinary topics. The purpose of the analysis is not to determine a ranking for the publications in terms of bad or good material, since it is the scholar who would find a specific work more appropriate for his own purposes. Nevertheless, it was necessary to establish a formal methodology, through which the scope and range of particular publications could be measured. This methodology returned some charts that illustrate the sets of most recommended works for a general reader researching on corporate security topics. The final chapter 5 mainly copes with recommendations for the prospective edition of specialist books. It was determined that formal suggestions for academic journals deviates from the scope of this work, since they would require a larger investigation on the universities and institutes making research on corporate security topics and therefore the recommendations concentrate only on specialist books. The closing chapter makes a general summary of the results and presents a couple of future lines of research, that can be based on the present work.

2. Security management scope

Defining the term corporate security could seem difficult given the complexity of companies and organizations in modern economies. The term itself suggests practices related to protect the existence of an organization. Once a business is established, it is exposed to a number of eventualities that could affect its activities. The influence of undesired factors on the business leads to a number of possible scenarios such as production problems, liabilities and the dissolution of the organization.

Given the importance of security related to the protection of the operations and goals of an entity, corporate security turns out to be a task of business management level. The scope of protection is thus not restricted to technical processes but it has a wider field including physical assets such as persons and property and intangible assets like information and market reputation. The analysis of threats and the implementation of measures is the main activity of corporate security management. The decision on the implementation of these measures implemented and its justification is a complex task on which the existence of security as a management organization lays.

There are several reasons why a company has to be committed in the implementation of security processes. Security is one of the most basic needs for any organization and virtually for any individual or collective entity. Without security, entities cannot have some sort of environment, which guarantees its development and growth. The importance as one basic need of any organization does not exclude all those measures that watch over the existence of a company, but also in terms of safety, security has big significance for the employees and persons living of or being related with such organization. The safety and

feeling of security has not only to do with the physical safety of workers, but this is a primary concept that gives the people social stability to those involved with the organization. On the legal aspect, organizations are also obliged to give the members of an organization certain level of personal security in physical terms.

One of the most important reasons why security has become so necessary in an enterprise environment is the financial implications of problems caused by security issues (Flast & Dickstein, 2009, pp. 40-45). The number of consequences leading to financial losses is as extensive as the sources of insecurity. There are events that directly affect the company such as theft and terrorism. This is why there is a difference between several threats compromising in a direct way the assets of a company. In these cases, corporate security acquires the most classical point of view of the term, in which the tasks of security management is the object protection given the ownership and right over such assets by the organization.

Together with the conception of direct threats imposed by criminal intentions, there is also another element of security seen from a classical point of view, in which the term safety becomes relevant since technical problems raised in the company facilities can also be the origin of direct financial loses (Asfahl & Rieske, 2010, pp. 5-6). Example of these cases is the initiation of fires and troubles in a production location. Either being caused by criminal intention or technical failure, the direct financial costs are most likely to be significant, since it is goods, assets, facilities or even personnel loses, which have to be replaced or in extreme cases it is the irreparability of the damages suffered, which have to be coped with. The apparition of events due to security problems bring other series of issues that can cause other indirect financial problems, not only in a quantified monetary cost, but it can be said that the extent and the duration of the effects and damage to the company cannot be foreseen in the short term. Any direct threat affecting the assets of an organization can have any indirect implications causing losses through other means. This is mainly because it is not possible that any given organization covers completely or minimizes the security problems it faced.

Examples of these damages are problems in manufacturing. As illustration, it can be thought that a partner logistics company had issues with workers smoking in the trailer lot and a fire event is produced. The costs of a fire are obvious in the sense that trailers and warehouses would have to be repaired. Nevertheless, the implication that a serving logistics company cannot transport and de-

liver the goods of its clients could be excessively higher than the simple replacing of goods. Together with legal obligations, there are other implications, not only in the form of responsibilities with the clients, but also insurance companies and the government can set penalizations, since such a company is not further able to prove a history with certain level of security and cannot be thus treated as a reliable service deliver. The reputation of the company is also another repercussion in this example given that the public opinion and the media can provoke that potential clients do not want to make contracts with that company. The internal image of the managers can also be damaged, where the grade of confidence of the employees at working for the organization is also one of the undesired outcomes.

As can be seen in this example, the damage and financial costs of a simple direct event can lead to a number of situations where the company confronts an escalating problem at the end of the day. In the worst case, a growing crisis can take to the termination of the company or its conversion into other forms like the change of name or the acquisition by other company, that is, the dissolution of the company in its previous estate.

Based on their responsibilities, security can be observed by different actors within a company in several ways. This is one reason why there is no general accepted definition of security. Moreover, the conception of security can be linked to the proper activities of each company and this fact modifies too the way security is conceived by the organization. The importance of the infrastructure on which a company relies defines the grade of protection of its main processes. In recent years, the increasing significance of information technologies on administrative, logistic and production processes has made the concept of corporate security to be strongly linked with information and computer security. Other partial definitions of corporate security have to do with the use of security personal to control physical access of persons and objects (Purpura, 2008, pp. 47-67).

The main objective of this document is the analysis of content and methodology in publications in the security field. For this purpose is necessary to define what belongs to corporate security as a management discipline in order to appreciate the topics treated by each publication. In order to understand the needs of a corporation in terms of security it is important to distinguish two points of interaction between the activities of a company and the external conditions that could affect its performance. A German global player who has branches all over the world cannot accomplish the same security measures for

expatriates who work in such dissimilar countries like Norway or Pakistan. Those workers, the information and the work they perform require different levels of protection. Not only in terms of personal safety, but also in order to watch over processes, knowledge and other assets.

Not only global players but also any organization of any size is active in an environment shaped by natural, technical and human factors (Gundel & Mülli, 2009, p. 3). Depending on the nature of the company's business, these factors affect in greater or lesser impact its activities. The interrelation between external factors and the nature of the business results in a set of threats relevant for a company. A factor that could be irrelevant for some company could represent a great threat for other company which activities belong to other nature. This is also true for the same company at different times of its history. A virus outbreak can be too less harmful in a production environment in some decades with full automated plants than the damages in the plant workers that such event could have nowadays with collective means of transport and workplaces. The catalogue of threats a company gets from the interaction between the nature of its activities and the external factors is not the only feature that this interaction provides, but also this relation defines the level of security required.

The level of security is not only a product of the combination of factors and activities as exposed above, but also the question of how much security is needed can be determined by the legislation in form of obligations, liabilities and social responsibility.

Security costs money and any effort to increase the security is an investment that shareholders are willing to implement or otherwise they have to cope with the existence of a threat. At this point, the level of security is subject to the question of what are the benefits of having certain level of security and at which price. The decision on how much security a company needs has to be made mainly based on the objectives the company is pursuing. The internet site of a consulting company, that provides general information and the profile of the company, is too less critical than the site of a bank providing online services for its customers such as transactions and balance overview. If the web servers of the first fall down this would not represent a problem, since the internet presence is not one of its main goals. On the other hand, if the information system of the bank cannot provide to its customers with such services, it is possible that the bank presents losses or even risks the existence of the company depending on the downfall duration (Schmidt, 2010, pp. 22-26).

The analysis of the correlation between the business objectives and the environment under which the company moves defines the level of security the organization wants to achieve. This level of security has to be methodically approached through the assumption of threats that the company is exposed to, within a scenario under which the desired security level has been reached.

2.1. Delimitation of security topics

These threats are thus not seen as such anymore, but as measured risks following a proper analysis. In other words, a threat represents some event, to which the company is exposed, but for which there has not been any adequate plan in order to overcome it. In such analysis, there are a number of aspects, which a corporate security management has to deal with. One of these phases of risk analysis is related to the reckoning of the probability of occurrence of such threatening events. The general definition of risk analysis in security management takes not only the probability of threats into account, but also, in order to value the level of risk a threat exposes, is necessary to consider what are the implications that the organization would confront in case of occurrence (Ortmeier, 2009, pp. 234-240).

When a meaningful value has been given to all events present in the threats catalogue according to some adequate scale, the threats ranked most highly are those that have a higher chance to be dealt firstly. Here come again the business goals and other factors such as legislation and financial aspects that have a weight when deciding which measures are to be taken for those threats with high probability of occurrence and higher impact on the organization's operations. The way the measures to be taken is accomplished depends on a number of factors as well such as financial limitations, available resources and politics and strategy of the company.

Once the security management along with the company's direction has analyzed which threats have to be treated by which means, a further step is the planning of all relevant measures in a technical and organizational framework; this is the first step for a security concept of the company (Davies & Hertig, 2007, pp. 129-149).

There are risks resulting from a risk analysis that even if they can have direct impact on the operations of a company, these are not handled by the security management. Due to a number of factors or restrictions, it can be decided in a management level that the efforts taken to minimize the impact of such threats exceed the company's capacity or simply there are no technical or or-

ganizational measures available to attack that kind of threats. In those cases, the company has the option to transfer the risk to third parties like an insurance company or simply cope with their presence.

The existence of threats that are not managed does not mean that the company cannot implement other plans of actions in case of occurrence. This is another aspect of corporate security management, which will be treated later. In order to define what are the limits of corporate security is necessary to differentiate which kind of risk affect directly the normal operation of the activities and which kind of risk are part of the business strategy as part of market or expansion purposes. In this sense, there are several activities, which could seem risky for a company but the management has decided the possible loss of investment and endeavor given to expand the business activities in other fields or markets (Damodaran, 2008, pp. 341-356). In this sense, all strategic risk such as that related with research and finances are out of the scope of the management of corporate security.

Threats against the company can come from several sources and conducted by different reasons, either deliberate or in a random way. The types of threats are related to their sources. A failure in the power supply can seem in some countries as something unpredictable, whereas in other countries such problems could have to do with illegal competition practices or government politics. In general, threats can come from natural sources, operational failures or criminal intentions. These sources of threats can be expresses in different ways along wide aspects of the company's interests. Probably, problems due to operational failures are more common for the vast majority of company types. Moreover, this is one reason why security management is commonly related to computer and network security. Since many companies rely on information systems either for administrative purposes or for controlling environments, information technology plays and important role in the operation of modern companies. This misconception of security management leads to a partial or inexistent corporate security in many companies under the premise that protecting the IT assets the activities can continue smoothly (Hunter & Westerman, 2007, pp. 5-16). As explained above it is through a risk analysis when many threats far from computer technology come out and this have to be treated accordingly.

Operational threats can be posed by human failure as well. The extent of threats in this respect have not to do only with schedules or lack of resources. Any company can confront problems e.g. with general health or even escalating collective societal problems such as the wave of suicides in French compa-

nies recently, where even psychology sciences cannot be disregarded as being strange to security management (The Holmes Report, 2009).

Besides sources of operational threats, there are nature hazards that are not only of the interest of big companies. Natural disaster such as flooding can affect almost any company given the storage of information and physical assets. In worse cases, bigger events like earthquakes and hurricanes can affect and threaten the existence of any company. All this sceneries suggest that such events cannot be managed merely by civil protection plans, but the company has to plan and analyze them in order to overcome and recover its previous situation before the events.

In addition, criminal threats can damage and put an organization in great danger. This kind of menaces are not restricted to violent aspects such as terrorism, sabotage, vandalism and robbery, but also espionage and unauthorized transactions are the scope of corporate security in this sense (Halibozek & Kovacich, 2003, pp. 25-44). In order to define corporate security is consequently necessary to make clear and separate that all this kind of operational risks are far from those risks related to the strategy and finances of the business, which are out of the scope of the subject. Moreover, this distinction does not mean though that corporate security is not involved in this kind of activities where strategic risks are taken.

It can be necessary that security processes and measures be taken by the security management in order to guarantee that the strategic risky initiatives run appropriately with the necessary analysis and protection given by the discipline. This means that security managers get involved in such strategic processes in order to formulate recommendations and find possible issues that could affect the company, when the management decides to take a specific way in the development of the company. The investment, planning of a new plant in a dangerous location or the research of a new product can affect the interest of certain groups, which could attack the company in many ways if their interests are affected (Damodaran, 2008, pp. 89-90).

In these paragraphs, there have been described important definitions that are the matter of study of corporate security management. It was said that threats are the result of the internal and external environment in which the company operates combined with those properties or characteristics of a business operation that could prove to be dangerous. That implies a direct relation between the activities and interest of the company and the set of all dangers relevant for

organizations with special attention of its processes and resources. When a threat comes through a security risk analysis process, this threat becomes measured and rated in order to pass through a set of measures to be taken in order to minimize the affectation in case of occurrence. It was said as well that security management does not deal with strategic risks that a company is willing to take in order to expand its activities into the market. All this considerations give place to a formal definition of corporate security that can be defined as the discipline that deals wit the acceptance, prevention and control of threats and risks that interfere or completely interrupt the normal operation of a company. The way the corporate security works these dangers out, bringing the operations of the company to a more secure controlled status, is by means of internal mechanisms in which a set of measures are taken in order to cover the vulnerabilities or minimize the effects caused by the occurrence of an undesired event. Utterly one of the tasks of corporate security is the study and conception of all relevant measures following a methodical interdisciplinary approach. Internal measure deals not only with all those actions that a company can take in order to reach a more stable control of operations, but that means also the consideration of compliance of partners according to agreements or other mechanisms made to guarantee that the company gets what is needed. There are also some other points of contact where the corporate security interacts too. The presence of security mechanisms is not a concern exclusively for a company and the partner companies which it has operations with, but there are also some other actors such as government and clients that demand the existence of corporate security practices within the company. In this sense, it is important to remark that the company does not stand alone and cannot decide autonomously which are the security practices, assets and processes that need to be protected, but there are a series of regulations, to which the company is subject. This big picture of corporate security gives immediately the idea that the discipline is constituted of a set of heterogeneous subjects and is related to many other fields not only in the technical part, but to other social and natural disciplines such as law, administration, economics, industrial management, informatics and natural sciences.

2.2. Topics to be searched and terminology

A general classification of security management topics can be made if there is a methodological approach that applies in all fields. Such classification should not be made in principle based on specific interests of certain industry, since what applies to a group might not apply to another. This is easily explained by

the fact that every organization has different assets to protect and which are subject to change according to the development of a business through the years. As an example, few decades ago IT security was for sure not as critical as it is nowadays since IT has become the backbone of most organizations. Literature in that frame could lack of IT security topics, which would be regarded as a secondary topic (Halibozek & Kovacich, 2003, pp. 351-354). Based on this consideration, specific interests for the managing of security and protection of assets can be incorporated in the literature research only if it is commonly accepted that such topic is widely valued by heterogeneous present-day sectors.

A first generic classification of security management can be done through the distinction of two main groups: preventive and reactive. Preventive security foresees possible threats and other subjects striving to minimize their effects in advance. Reactive security or incident management deals with threats that could not been controlled in the preventive phase or with unknown threats that were not considered previously (Stucki & Marcella, 2004, pp. 10-25).

The establishment of security management as a discipline demands the conception of methodologies that estimate and control risks. This is because risks are in fact numerical valued threats, being the latter the object of study. Risk management can be conceived as a tool that help the security manager to estimate the importance of risks given an inventory of relevant threats that could damage the organization in several degrees. In this sense risk management is the basis that supports and justifies the efforts and way of dealing these issues.

Another fundamental basis of security management is the active design and implementation of measures taken to control those risks. The implementation and affectivity of those measures are mainly given by methodologies coming from other established disciplines such as project and quality management. Therefore, measures taken to improve security are not restricted to implement security measures but to evaluate and improve the undertaken tasks.

The implementation of measures to minimize risks is related to the preventive aspect of security management. Risk considered worth to be managed during the risk analysis but for which a measure could not be taken due to budget, organizational, technological or other restrictions, can be assigned to the reactive aspect of security management. That is, those threats that cannot be absolutely eliminated and from which an immanent occurrence can be expected with considerable consequences have to be planned by reactive branches namely incident and crisis management (Stucki & Marcella, 2004, pp. 15-17).

Topics	Examples – grouped alphabetically
Fundamentals	
Risk identification	Cost benefit analysis, financing of security, marginal utility of security, reputation, return on Security Investment, risk management, SAP security policy, security governance, security reporting.
Measure identification and implementation	Deming models, guidelines and procedure models, plan do check act models, quality management, security audits, security concept, security level agreement, security organization, security training.
Incident handling (crisis)	Business continuity, catastrophes, corruption, crisis communication, crisis management, disloyalty, embezzlement, emergency organisation, guidelines and procedure models, incident mangament, insurances, investigations, IT forensics, organized crime, protection rackets, public relations, sabotage, situation centers.
Other fundamental issues	
Requirements	Basel II, data protection, enviroment protection, corporate governance, guidelines and procedure models, KonTraG, SOX Act.
Subdisciplines	
Physical security	Access control, authorizations concepts, awareness, employee and candidate profile check, espionage, factory security, guidelines and procedure models, identification, loss prevention, perimeter protection, property protection, security tehcnology, site security, social engineering, surveillance, theft.
Information security	Access control, authorizations concept, awareness, backup, business continuity plan, cryptography, espionage, guidelines and procedure models, identification, information acquisition, information and know-how theft, information privacy, information security management systems, infrastructure redundancy, IT security, IT security scan, knowledge management, least privilege principle, privacy, public key infrastructure, road warriors, social engineering, traffic surveillance, whistleblower, whistleblowers.
Person safety and security	Awareness, event security, expatriates and travellers security, fire protection, guidelines and procedure models, industrial safety, occupational safety and health, persons protection, workplace safety.
Infrastructure resilience	Backup and redundancy, fire prevention, flooding, haulage security, industrial and supply interruption, IT baseline protection, logistics, power supply, raw material supply, security protection, service level agreement, software quality, statics, uninterruptible power supply.
Standards and tools	Accreditation, audits, certification, compliance, guidelines and procedure models, incident reporting systems, ISO 14000, ISO 27001, security service level agreements, service level agreements.

Figure 1 Fundamentals and subdisciplines

Risk identification, measure identification and implementation methodologies and incident handling can be considered as the backbone of security manage-

ment since the combination of these fields strategically play offensive and defensive roles based on a primary dimensioning of the threats scenario pursuing the accomplishment of the organization objectives.

For the purpose of literature assessment, it can be considered that all kind of tasks undertaken by a security management correspond to some undesired event or instance that could damage or affect the organization operationally or financially. This is not precisely the definition of threat, since e.g., legislative instances cannot be considered as threats themselves, but it is the contempt of regulations that give place to a threatening scenario, at least in respect to financial and liability matters. The first division of Figure 1 shows the three different categories of preventive and reactive fundamental topics of security management treated in this work. Along with the three divisions, several keywords are provided in order to exemplify the kind of topics researched in the different publications through this investigation. The topics of risk identification refer to the processes aimed to assess possible threats for the organization. The aspect following the risk identification corresponds to the methodologies taken to establish the strategies to minimize risks and the procedures to implement these measures. The reactive aspect of security management is denominated incident handling, which deals with the organization and preparation aiming to cope with the occurrence of threatening scenarios, mainly with criminal and contingencies background.

The table above depicted and intermediate group for other fundamental issues that contains requirements in the form of regulation and liabilities both from governmental bodies and the legislative. Nevertheless, this is not the perspective followed in the research and analysis parts of this work. In those chapters, the requirements group of the fundamentals and the standards group of the subdisciplines are put together, given that the reviewed security literature did not make a strict and formal differentiation of both fields. Nonetheless, the referred table attempts to stress the fact that the requirements present a more fundamental nature for the establishment and existence of an organization than the secondary aspect of industrial standards and methodological tools for security managers. Below follows a description and justification of the security subdisciplines grouping and the one before the last paragraph of this section treats in advance the requirements and standards together as they will be dealt hereafter.

Security management literature should contain formal methodologies or give a description on how to identify and estimate risks, implement measures and

overcome incidents or crisis in a generic or demonstrative way. Although the present work does not follow a particular shape of an organization, several topics cannot be left apart by the literature in this field. It has to be reminded that security management stems from product and services oriented businesses along with government initiatives to strength private and public structures.

The scope of this study is the analysis of literature in security from a top-level perspective. Works that concentrate exclusively on particular aspects of security are not thus considered. That includes all kinds of books which offer security management applied solely to specific industrial needs such as computer centers and plant security. On the other hand, it should not be expected that a book or an academic journal series cover all aspects of security, as that would imply an extensive encyclopedic study of all industries and possible threats and crisis schemes. Nevertheless, it has to be admitted that certain topics belong to a general concern for the economy of industrialized countries.

Given the different interactions an organization is subject to, there are several groups of interest wanting an organization to undertake security management practices. The legislative emits regulations to enforce transparency and to predict crises that could affect a country´s economy and throw to unemployment masses of workers. Expatriates of global players are interested in their personal safety and of their relatives. End customers want the companies, they are giving personal information to, to protect it and keep it confidential. All internal business areas demand to have a robust information and communication structure that allows them to perform daily business activities smoothly such as production, controlling, logistics and communication with partners. The second division of Figure 1 shows four scopes of security management defined in this work in order to create a standard catalogue of disciplines or fields, namely physical security, information security, persons security and safety, infrastructure resilience and regulation, standards and liabilities an organization is subject to, on which the literature analysis can be based.

The field of physical security refers to the methodology, processes and organization aimed to protect any physical object from unauthorized access. Not permitted access may have two possible causes having to do with criminal efforts or simply so called human failure by which errors in security architecture lead to a violation of access policies with comparable consequences as criminal motivated infringements. The type of secured objects varies from organization to organization; nevertheless, a common start point to deploy a security architecture is the classical concept of property protection with technical and orga-

nizational elements such as surveillance, access control and intervention concepts to name a few (Davies & Hertig, 2007, pp. 27-34).

Another discipline with increasing importance, as industries become more dependent on IT, is information security. Information security is often related with two fields separately. Professionals with background in laws or security officers often understand it as data and knowledge protection whereas computer experts link it mainly with IT security. Both perspectives may be corrects, although an integral definition of what belongs to information security can be given by the nature of organization in question. Information can be considered as an asset to protect, just like some other physical object. Perhaps prior to the storage and transmission of data by digital means, information security could be restricted to classical access control to documents and archives (Müller, IT-Sicherheit mit System, 2003, pp. 20-23)

Persons safety and security is the third set of standard subjects grouped in the literature analysis. This category refers to the conception of persons as elements or assets, which are fundamental for the accomplishment of the organization's objectives. Other than those assets of physical and information nature previously mentioned, the interest of protecting the human capital as a corporate security task comes partially from the legislative and the obligation of any company to provide safe and healthy working conditions and the image of the organization toward the public in general (Asfahl & Rieske, 2010, pp. 45-49). Nevertheless, the most relevant aspect of protecting the human asset in an organization is that the working force is as important as any other resource in any industry. The interest of security management in the safety of workers and facilities is thus the safeguarding of the organizations activities and objectives. Regular associates and workers of a typical company are rarely target of criminal related risks and therefore the involvement of security management in safety and occupational health topics is secondary or delegated, save some cases of organizations with particular security and safety needs towards regular employees, such as news agencies active in journalism threatening countries, or organizations exposed to a pandemic. Security of higher ranked employees such as some expats or chief officer might be under the assignment of corporate security management, since their availability is critical for the organization, and their significance might be irreplaceable in the short term. The type of protection for high ranked associates deals with abduction, bodyguarding, event security and training to name a few (Halibozek & Kovacich, 2003, pp. 387-392).

The group of infrastructure resilience or infrastructure security gathers the facilities needed by an organization to accomplish its tasks. The most representative asset in this category may be buildings and any other kind of construction of the sort. The group infrastructure though holds a larger set of objects, which support the organization's activities. Power supply, communication networks, fire and flooding prevention are some of the topics related with infrastructure security (Herder & Thissen, 2003, pp. 2-9). As it can be seen the resilience of an organization's infrastructure is related to other fields such safety and logistics. The importance and role of a company's infrastructure in corporate security is tightly related with business recovery and safety concepts. Infrastructure resilience typically becomes relevant to the corporate security when escalating incidents in the normal operation might threaten the existence of the organization. A recent example is the 2010 volcanic eruption events in Iceland, where the restriction of air traffic led to a number of problems in the supply and production chain in the automobile industry, where the once typical logistics issues goes over a corporate level leading to the execution of business continuity plans (Disaster Recovery Journal, 2010; Süddeutsche Zeitung, 2010). Another example is construction statics, where failures in the planning of buildings can lead to the collapse of the facilities of an organization. In this case, corporate security is involved in not only the safety and intrinsic crisis of the event, but a process of business recovery has to be started in order to get back to a minimal state that permits in short the resuming of operations.

Regulations and standards come typically from the legislative in observance of the company as a financial entity in relation to possible repercussions in a country's economy or some industrial sectors, and in a lower level in relation to some legal responsibility over the workers and employees for instance. In European and US legislations there has been an increasing interest on corporate governance structures of companies regarding strategic and operational risk of both financial and non-financial nature. Regulations such as the Public Company Accounting Reform and Investor Protection Act (SOX) and the German Law on Monitoring and Transparence (KonTraG), to name a few, are known to the security manager since the identification and handling of operational risks is one of the reasons, why many companies appoint corporate security functions at a managing level (Flast & Dickstein, 2009, pp. 31-35). This group of topics for literature analysis takes into account also industrial level regulations such as ISO standardization industrial norms or service level agreements topics analyzed in the corresponding publications.

The topics categories presented ad hoc here do not pursue to mirror an organizational or established structure of the security management practice. The groups depicted represent rather a way to allocate the topics studied in the publications. In this point, it has to be mention that some topics may belong to two or more groups and therefore any classification can be debatable. As an example, consider access controls, fire protection and power supply. In the given order, these topics could belong to physical security and information security, the second to infrastructure resilience and persons safety and the latter to information security and information security in the sense of availability. On the other hand, the security structure can vary according to the type of activities, and following this considerations the categorization of topics was made accordingly to the main explicit subject of the publication texts or the relevance of the area with the corresponding category. Any organization has very specific interest, which could hardly fit in the scope of a book. As a possible scenario take the situation of the Vatican standing before a series of accusations of child abuse in many countries that will affect the image of the Church and probably a considerable decrease of members (Die Zeit, 2010). Crisis public relations cope with the communication with media and public opinion to protect the image of organizations. Western schools have confronted the rise of amok students that becomes difficult to prevent given the copycat pattern of this phenomenon, the relaxed legislation of weapons particularly in the US trade and the influence of media in the young population. It might be of the interest of this and European countries' schools to have prevention programs and management of amok situations (Der Spiegel, 2010). The control of risks and crisis in these specific examples can possibly be found in academic journals and other periodicals, but, as it has been mentioned previously, the scope of this work includes exclusively the study of generalized security topics concerning a wider public involved and interested in security as an academic discipline.

3. Literature research

Academic investigation can be broadly classified into primary and secondary research. The present work belongs to the secondary type, since the source of analysis material is derived from the synthesis of existing printed publications, and not from conducting tests and analysis of new data (Fink, 2008). The present document divides the investigation in collection, analysis and proposal of security literature.

Computer-aided search of literature is a thorough step given the dynamic of both printed and electronic publishing nowadays, linguistic considerations in the form of equivalent and related terms in addition to language-specific morphology, usual large sets of search results as well as the reliability and quality of specific catalogues. Also relevant to mention is that currently the partial availability of full digital documents for keyword searches obliges to a bibliographic data research rather than content searching. The information technology and the remote availability of catalogues have optimized the work of bibliography research. In the last years the offer of digital catalogues increased continually as many national, state and university libraries in addition to editorials and booksellers made them available through Internet (Mann, 2005, pp. 55-60). Due to cross-search capabilities, there are a number of proprietary and public resources that allow interinstitutional searching of publication keywords and more recently of full publication contents. Interinstitutional catalogue search engines are regularly more appropriate for literature research than isolated catalogues, since they provide a broader overview at national and international levels. For interdisciplinary fields such as security management, the use of interinstitutional cataloguing optimizes the search of literature, rather than querying separate databases, for instance on economics, engineering and law. The

present work concentrates on the publishing of printed books and standard magazines (magazines) in the sprachraum as well as academic journals (journals) in English or German. Although major search engines provide non-periodical and periodical bibliography in English, German and any other language, some of them specialize in determined types of publications, therefore four databases, specifically the Deutsche Nationalbibliothek for German-speaking books, the Zeitschriftendatenbank for German-speaking periodicals and Worldcat and Ulrich's for English-speaking periodicals, have been used for the separate search of books, standard magazines and academic journals respectively as justified in the following sections.

The research scope for books and journals is the same; it aims to find publications specialized in the whole thematic of security management as an independent discipline comprising the key topics mentioned in the previous chapter. An initial informal search showed the lack of a standard magazine integrating the several topics of security management in a dedicated publication. As a result, it was necessary to segregate the discipline in subordinate fields, for instance information technology, crisis management and physical security, in order to provide a library of standard magazines for security management in the sprachraum.

Due to the fact that English and German are composed of hundreds of thousands of words, it is difficult to establish an absolute methodology for the creation of a definite list of keywords appearing on any imaginable publication title within some discipline. That is, it can hardly be proved that discarded words do not appear in possible titles (Mann, 2005, p. 33) of a bibliography for security management. Nevertheless, provided that scientific writing tends to use concise and standard terminology at publishing and cataloguing a title, the accomplishment of some methodological steps leads to a reliable set of contemporary keywords. The initial step in defining a list was the delimitation of security management topics given in Section 2.2. The discrimination on what belongs to security management and what is out of its scope gives a general set of keywords, such as security management, asset protection and corporate risk, which are only a raw basis for searching literature. The segregation of security management in subordinate disciplines led to a wider set of keywords for standard magazines; e.g. information security, person protection and business continuity. Certain influence of English on German terminology is another factor that extends in small degree the set of German keywords in the search of books and magazines. Example of this is the wide integration of terms such as security

and continuity in popular and academic German; in contrast, journals on security management must be searched in both full German and English vocabulary, since the scopes for it are both the sprachraum and English as a lingua franca. Following the delimitation of security management topics, the use of thesauri, taxonomies or ontologies extends the keyword list. For German and English keywords, the Wahrig Synonymwörterbuch (Adolphs, 2008) and the Merriam-Webster Thesaurus (Merriam Webster, 2007) were the primary sources to find related terms. The word formation service in www.canoo.net, German and English Wikipedia.org's redirection "What Links Here" service, Linguee.de's parallel text based dictionary were support tools used to find related designations of concepts. Both English and German have the characteristic that morphemes in compounds can appear together, spaced or hyphenated as for example informationssicherheitsmanagement compared to information security management (Donaker, 2006, p. 2). Word compounding, in addition to word inflection, makes necessary that catalogues have searching capabilities for regular expressions, i.e. string matching, deriving from the defined morphemes. Compounds are constructed by a head and one or more modifiers; the three-stemmed compounds corporate security management and unternehmenssicherheitsmanagement have the word management as their head. Since a separated search of isolated words leads to large result sets, the simultaneous search of two or more keywords becomes mandatory, for it decreases the number of title matches that have to be later manually filtered. The compound corporate security in major Internet search engines returns roughly half million web documents whereas the word security alone gives about half billion, i.e. in this analogy the elimination of the word corporate would increase the manually filtering work by a factor of a thousand. It is important to point out that the allusion to compounding does not mean that actual queries will be made by concatenating heads and modifiers; it is rather the concepts introduced by a compound, which are the source of possible titles where keywords can appear together or separated. Through non-concatenated keyword pairs related to corporate security, matches such as social security or security in social environments, finance security or security in the finance sector and psychology security or security in psychology science are eliminated. It is thus required that all possible keyword pairs are inferred based on the idea introduced by a compound (Mann, 2005, pp. 98-99), since it is not favorable to expect that e.g. corporate security is named as such by all authors and academia uniformly; equivalent used terms could be organization security, business protection, process and assets assurance or simply security management. Since currently full book body

searches are seldom possible, the queries rely on database fields such as title, subtitle, author, description and category. If these fields for a specific publication are not descriptive enough it will not be returned by the queries as characterized above. That is, a book on corporate security is not regarded if it has database plain entries such as security for title, security for description and security for category alone.

3.1. Book research

In sprachraum countries, library research can be done through union catalogues, which allow simultaneous querying of public institutions such as all public and university libraries in regions comprising one or more states. The Austrian Österreichischer Bibliothekverbund and the Swiss Informationsverbund Deutschschweiz are examples of union catalogues that look for physical availability in several types of libraries of those countries (Sesink, 2007, pp. 121-127). In Germany, there is no nationwide engine; the recognized Karlsruher Virtueller Katalog is not a union but a metacatalogue; unions are rather present at regional level with catalogues such as the Gemeinsamer Bibliotheksverbund and the Kooperativer Bibliotheksverbund covering northern Germany. The availability in libraries is an important feature useful for this work to retrieve material; nevertheless, documentation is not necessary. Instead, it is the actual existence of material what is recorded by this work, since a primary step is the state of the art in security literature. For this purpose, results that are more reliable can be provided by the in-house lending Deutsche Nationalbibliothek (DNB) in Leipzig and Frankfurt. Editorials publishing in any language in Germany are obliged to submit copies and bibliographic information of their books to the DNB. In addition, the institution traces, catalogues and collects foreign material written in German including but not restricted to those published in Austria, Switzerland, and Luxembourg making it the primary source for literature research in the European and overseas sprachraum (Ansorge, 2008, p. 19; DNB, 2010). Its electronic catalogue enables researchers to do standard queries by means of multiple right-truncation, logical associativity and advanced catalogue fields such as country, language and serial number.

The definition of security management in chapter 1 distinguishes between fundamental topics and subordinate fields of this discipline. Whereas the belonging and classification of subdisciplines respond to a generalized interest giving shape to a contemporary characterization of security management, for instance in the form of IT security, property protection and counter-intelligence. Whereas the fundamentals refer to models or methodologies aimed to analyze

operational risks and devise measures shielding the processes and assets of an organization and strengthening its contingency capacity. Common designations for this matter of study are corporate security and security management, which together in as corporate security management describe more specifically the goal of conducting protection measures for an organization. In addition to both terms, this work revisits the core concepts of operational risk management, security measure identification and implementation as well as incident handling in order to improve the research quality. Although the scope is corporate security management as a whole, the purpose of segregating the fundamentals topics in separate investigations is due to the possibility that some books, entitled with keywords related to operational risks, security measures or incident handling, might cover mutually the other fundamental topics as well in equal or lesser degree.

In this work, two different methods were tailored for searching literature. The necessity of compounding considerations explained in the last section results from two considerations. The fact that German compound morphemes appear joined rather than spaced or hyphenated as in the case of English compounds, made necessary the querying of compound headers and compound modifiers. The second ground that took to considering word compounding was to restrict the amount of matches since e.g. the search for the word sicherheit alone returns mostly titles related to national security, sociology, several medical sciences and economics.

The compounding method was the first to be tested but at the end of the day it was the second method, the left truncation method, which was proved more reliable though less finer than the compounding method since it is less discriminatory but it requires way too more time for discarding titles manually. It was considered relevant though to document the compounding method in the next paragraphs since it represents a faster alternative for future researches to look for new security literature, nevertheless this work is based on the more reliable left truncation method.

It is important to mention that the two following methods were made from the scratch based on the observation of morphology and research properties studied in the works of Sesink (2007), Mann(2005), Fink(2008) and Donaker(2006). In particular, the so-called compounding method is a straightforward methodology used by almost all researchers. The second single keyword querying is rather a non-optimized method based on retrieving and processing large amounts of titles. Perhaps researchers avoid such large queries since it requires

the use of scripts and long time for manual filtering, which this work did decide to cope with.

3.1.1. Compounding method

Seven key concept scopes were determined, namely unternehmenssicherheit and sicherheitsmanagement; betriebsrisiko and risikomanagement; sicherheitsmaßnahmen; betriebsereignis and ereignismanagement; which are the start point to combine related words; these are shown in Figure 2 along with the number of titles found in the Deutsche Nationalbibliothek through this method. A diversification of compound modifiers and headers by using related words make possible to find books of which titles omit specific terms such as security, risk, security measure and incident but rather use equivalent words to describe the same discipline. On the other hand, appropriate synonyms, but still non-related to the matter of study were arbitrarily discarded; they are though presented next to the valid sets for documentation purposes. For each of the seven concept scopes two keyword sets were defined. Sets A and B contain respectively modifiers and headers in both English and German related to the corresponding concept.

Concepts	Matches
Concept 1 unternehmenssicherheit	3241
Set A = {betrieb, corporat, firm, geschäft, global player, konzern, unternehm} *Set B = {schutz, sicherheit}*	
Ignored related terms: aktiengesellschaft, anlage, association, business, company, enterprise, fabrik, gesellschaft, handelsgesellschaft, handelsunternehmen, kommanditgesellschaft, komplex, multinational, transnational, partnership, security, society, werk, wirtschaftsbetrieb, wirtschaftsunternehmen; abschirmung, bewachung, deckung, geborgenheit, gesichertheit, obhut, safety and sekurität.	
Concept 2 sicherheitsmanagement	383
Set A = {schutz, sicherheit} *Set B = { geschäftsführ, geschäftsleit, management}*	
Ignored related terms: some shown already and aufsicht, direktion, führung, leitung, oberaufsicht and vorsitz.	
Concept 3 betriebsrisiko	1833
Set A = {betrieb, operati; corporat, firm, geschäft, global player, konzern, unternehm} *Set B = { bedroh, gef?hr, risik}*	
Ignored related terms: geschäftlich and risk.	
Concept 4 risikomanagement	1879
Set A = { bedroh, gef?hr, risik, risk} *Set B = { geschäftsführ, geschäftsleit, management}*	
Ignored related terms already shown.	
Concept 5 sicherheitsmaßnahme	1472
Set A = {schutz, sicherheit} *Set B = { maßnahme, vorgehen, vorkehrung}*	

Ignored related terms: some already shown and aktion, anordnung, anstalten, anweisung, bestimmung, entscheidung, handlung, initiative, kampagne, projekt, regelung, richtlinie and vorhaben.

Concept 6 incident 612

Set A = {betrieb, operati; corporat, firm, geschäft, global player, konzern, unternehm}
Set B = { ereignis, incident, krise}

Ignored related terms: some already shown and ablenkung, beeinträchtigung, begebenheit, behinderung, belästigung, geschehen, kritische, not, problemsituation, storfall, störung, unterbrechung, unfall, unglück, vorfall and zwischenfall.

Concept 7 krisenmanagement 406

Set A = { ereignis, incident, krise}
Set B = { geschäftsführ, geschäftsleit, management}

Ignored related term already shown

Special set (concept 8) 3746

Set A = {security}
Set B = {security}

Figure 2 Book search keywords sets.

The purpose of defining two keyword sets is to get all possible word pairs to be queried as $\{(a,b)|a \in A \wedge b \in B\}$, i.e. their Cartesian product. Single word queries based on a set alone would increase the result size by an undetermined factor –as it is actually seen in the left truncation method in the next section– whereas 3-tuple or larger tuple queries would accordingly discriminate relevant titles. The pairs (a,b) are the base for two types of queries: on one hand, the basic compound is queried as the non-spaced concatenationa^*b^*, where * represents a random string for right truncation purposes; on the other hand the stems a and b are queried independently within the same title. As an example consider the ordered pair$(unternehm, sicher)$, which is used for a title query of form$(unternehm^*sicher^*) \vee (unternehm^* \wedge sicher^*)$.

English isolated synonyms with loanwords in sprachraum literature can be included freely as long as the employed search engine differentiates between publication languages. Nevertheless a narrow selection was made for loanwords, since not all catalogues support language fields but primarily because only few English words are actually borrowed by sprachraum academia and industry; large loanwords subsets are not necessary. In this sense, consider the search for global and player returning possible titles such as sicherheitsanforderungen der global player, where the use of a catalogue field for language fixed to German, i.e. conditioned to the sprachraum, would prevent the inclusion of English books. Linguistic stemming is needed for both English and German, for instance due to noun plurals for the former, but particularly relevant for German grammatical genres and cases. Keywords are shown in the referred figure by their shortened stemmed form.

This investigation attested though that bibliographic fields of the DNB catalogue and many other library databases are not reliable parameters; books are not properly allocated to science branches and even basic fields such as publication year and language might be recorded wrong. For this reasons the only field used at the end of the day was the title field itself restricted to the collection of books, i.e. excluding other medium formats. Given that the DNB online catalogue does not allow large sentence queries, that is, the use of more than a couple of operators and wildcards in a single query, roughly two hundred independent queries in this method were executed and imported by script as detailed in the next section. The number of queries here corresponds to the sum for all concepts of two times the product of both set cardinalities or$\sum_{concepts} 2|A||B|$; the factor of two corresponds to concatenated and independent stem querying.

3.1.2. Single keyword querying

The previous method intended to provide a filtering solution to the very large amount of titles returned by single keyword queries. A second reason for set delimitation through keyword pairs was that title filtering by database fields seemed quite unreliable, since it was attested that catalogues often contain wrong or misleading entries such as subject, year and even publication language. It was therefore determined that the most consistent and only field, on which the querying should rely, is the title entry alone. The title field, at least in the catalogues consulted in this work, contains additionally the publication subtitle and, sometimes, other information in a single text string. By this reason, it seemed convenient to use keyword pairs to find relevant publications even when the main title was not clear enough. That is, consider a publication with main title *Security* and subtitle *A Task of Corporate Governance*, which would be indeed fetched thanks to the subtitle detailing. The use of keyword pairs also eliminated the need of left truncation since they represent separated title keywords as well as jointed modifiers and headers by which catalogues start to index from left to right.

The idea of a second querying method came out from finding some publications that were filtered out due to the strict discrimination of keyword pairing either because titles and subtitles were unclear or because some keywords had been mistakenly discarded. That is, it was necessary either to define more sets pairs and more keywords pairs resulting in larger matches or to abandon the keyword pairing idea and to cope with very large results, which at the end of

the day were as large as by increasing the keyword pairing anyways, but more reliable.

Aside from the very significant increase of working time for manual filtering, the actual technical problem of executing single keyword queries is that catalogues commonly index completely German words instead of their components, i.e. modifiers and header. A query for *sicherheit** will never return the title *Unternehmenssicherheit*. The lack of substring indexes can be explained by the fact that indexing words such as *unternehmenssicherheit, nternehmenssicherheit, ternehmenssicherheit, ernehmenssicherheit, rnehmenssicherheit, nehmenssicherheit, ehmenssicherheit, hmenssicherheit, menssicherheit, enssicherheit, nssicherheit, ssicherheit*, *sicherheit*, *icherheit*, *cherheit*, *herheit*, *erheit*, *rheit*, *heit* ,*eit*, *it* and *t* for every single word of every single catalogue entry might not be very useful. Compounding analysis would be though a highly recommendable task in order to index only e.g. *unternehmenssicherheit, unternehmen* and *sicherheit* and to offer an enhanced library service. In addition to these linguistic and database aspects, left wildcarding is also not possible perhaps due to server load issues; this implies that a query for **sicherheit* is either not possible as such or would be simply interpreted as *Sicherheit*.

Despite these drawbacks, multiple right truncation is still possible indeed, which is helpful to emulate some kind of left truncation of the sort **sicherheit*, no matter what precedes, either *unternehmens* or *museums*. This is done by multiplying the number of queries by a factor of 26, corresponding to every letter. A search for *u*sicherheit** returns thus *unternehmenssicherheit*, *unternehmenssicherheitsmanagement* and *ueberseesicherheit* for instance. Some catalogues though do not allow single character prefixed queries of the form *x*keyword**, where *x* represents a single character, but of the form *xy*keyword** or *xyz*keyword** or longer prefix strings, where *y* and *z* represent single characters as well. It is unknown what policy applies the Deutsche Nationalbibliothek, since some times *x*keyword** queries could be successfully executed but other times only *xyz*keyword** queries were possible, in which case a number of 26^3 would be determining. If a factor of *26* in *x*keyword**, multiplier of every single queried keyword, already introduces great difficulties by managing hundreds of web pages of catalogue internet interfaces, the number 26^3 would certainly require greater computational capacity not accessible at first hand by this investigation. Fortunately, *x*keyword** queries could be performed in two different weeks from different locations in order to verify the consistency of the data sets. Two tools were very valuable at query generating

for internet browser and data sets importing into a spreadsheet, in which the querying and the manual filtering could be carried out The first was done by browser scripting, in which a set of keywords were converted into formatted querying URLs tailored to the Deutsche Nationalbibliothek. This was done in three steps. Firstly the keywords were read in plain text by the browser, secondly the browser appended the required URL to each keyword 26 times and finally the browser opened different tabs resulted from parallel querying. Multiple querying was necessary given that the catalogue does not allow complex queries such as chaining tens of logical ands, ors and wildcards due to server load design. The second tool is provided by the Deutsche Nationalbibliothek as a data shopping service, by which large sets of queried records can be downloaded in single files for every query. In contrast, the simple print version and emailing functions only let fetch batch ranges of 200 records at a time.

Book titles with keywords similar to:	Matches
Concepts: unternehmenssicherheit, sicherheitsmanagement, sicherheitsmaßnahme *Set = {schutz, sicherheit, security}*	139,431
Concepts: betriebsrisiko, unternehmenssicherheit, incident, risikomanagement, *Set = { bedroh, gef?hr, risik}*	60,890
Concepts: incident, krisenmanagement *Set = { ereignis, incident, krise}*	31,969
Total with ~*2%* duplicates	232,290
of which have unclear description (were verified and discarded)	130
ring a bell but have other scope (are described in section 4.1 in spite of it)	7
belong to this work	6

Figure 3 Book query result summary.

Once the data sets were saved in single files, the title entries of all files were merged in a single spreadsheet and removed from duplicates produced by multiple querying that might have fetched the same title two or more times. Figure 3 shows the number of titles containing the keywords strings related to the concepts shown in the same table. A total of 230 thousand books could be fetched from all kind of sciences, for instance medicine, economics and sociology, having books published with titles containing strings such as *sicherh*, *risik* and *krise*. A second step was to code in the spreadsheet application an algorithm for determining the frequency of substrings in order to feed a so-called black list of recurring keywords that definitely are not of the interest of this work. In addition to some expected black list substrings such as *bank* and *national*, the macro helped to find out more unwished substrings such as *krank* and *sozial*, to name a few. Titles in the spreadsheet containing any string in the black list were automatically eliminated reducing the upcoming work time by

about a fifth. A thorough manual filtering led to a set of 143candidate titles, from which 130 books had misleading titles or were discarded by other reasons; prior to their discarding almost all these publications were verified in online libraries and bookshops. Finally, seven books were chosen having titles claiming to belong to the field of this study but following a limited approach; nevertheless, they are documented in this work in section 4 for reference to future research. A final set of six books was identified to be relevant to this study, which are analyzed in the subsections of chapter 4.

3.2. Journal research

The objective of the academic journal research is to document the available periodicals in the field of security management. There are two types of periodicals considered in this work. The type popular magazine refers to specialized periodicals in a set of topics, which are issued by editorials that typically publish other media on different topics and have mostly commercial purposes; the content revision is made by a dedicated editorial board non-active in scientific research. Although the term journal itself, on the other hand, defines any kind of periodical, it refers commonly to a type of magazine published by a scientific editorial, such as nationwide academies or institutes, which serves as communication means for the academia or industry. Prior to publication, journal articles are analyzed and criticized by other individuals with ongoing research or recognized specialization in the topic. Journal articles have the common characteristic that they present the results or state of the art of the authors' proper investigation. In comparison, magazine columnists commonly interpret and report the works of academia, industry and government making them accessible to a wider non-specialized public.

Of the three types of publications considered in this work –books, journals and magazines–, the journal research is not restricted to German-speaking periodicals. Since journal publishing aims an international scientific community, they are published mostly in English as a lingua franca, and as such, the present work searches English-speaking journals within and outside the sprachraum in addition to those published solely in German if available. In comparison to national-level bodies like the Deutsche Nationalbibliothek that can thoroughly survey the German-speaking publication behavior in the smaller sprachraum, there is no inter-government body to watch at and catalogue English-speaking academic journals, since these can be published by any number of institutions in any country despite its national language. Recognized publishing houses, citation-linking services and catalogue unions such as Springer, Ebsco, Jstor and

Proquest commonly concentrate on specific academic branches or gather large bibliography information of any type. These bibliographic services for academic publishing make special consideration in the type and topic of the articles contained on journals, which is just a feature of secondary relevance for this work. Besides Worldcat, the largest most recognized public catalogue union comprising library databases, publishers records and other bibliographic services (Livres Groupe, 2010, pp. 12-15; OCLC, 2009), another private product with over 30 years work on international library collaboration is Ulrich's (Mann, 2005, pp. 133-136; ProQuest LLC, 2009). Worldcat and Ulrich's have been used for journal research in this work. Worldcat and Ulrich keep a record of all ISSN and other periodicals and discriminates them on the basis of belonging to the type academic journal as depicted above. Article or abstract-level classification is not one of their primary objectives; in fact, these services do not keep official records of article tiles. Given that the present work focuses on finding whole publications rather than journal articles on specific topics, Worldcat through Worldcat.org and Ulrich through Ulrichsweb.com are appropriate initial approaches to access only those periodical type titles of interest; that is, all academic journals separated out from tens of thousands of ISSN media.

English concepts	Matches
Concepts: corporate security, security management and security measure *Set = {security, protection}*	250
Concepts: operational risk and risk management *Set = {risk, threat}*	79
Concept 3: incident and crisis management *Set = {incident, catastrophe, crisis}*	19
Total	348
ring a bell but have other scope (are described in section 4.2 in spite of it)	11
of which belong to this work	7

German concepts	Matches
Concepts: unternehmenssicherheit, sicherheitsmanagement, sicherheitsmaßnahme *Set = {schutz, sicherheit, security}*	19
Concepts: betriebsrisiko, unternehmenssicherheit, incident, risikomanagement, *Set = { bedroh, gef?hr, risik}*	2
Concepts: incident, krisenmanagement *Set = { ereignis, incident, krise}*	1
Total	22
ring a bell but have other scope or are not journals (which are surveyed in section 3.3)	10
of which belong to this work	0

Figure 4 Journal search keywords sets and query results

A second investigation is performed by this work in libraries for journal titles that seemed to belong to the security management discipline. Figure 4 show single concepts sets such as security and risk with their corresponding matches. For German speaking publications, the same keywords sets apply as for the books research. The figure shows two tables for both English and German concepts. For both scopes, there are three different sets of keywords, which correspond to the fundamentals of security management as defined in the previous chapter. For the English part there were found 348 different journals containing or related to words such as security, threat and incidents. Most of the titles were immediately discarded after a quick revision of their titles and 40 other with ambiguous titles were deeper researched but finally also dismissed. The remaining set of English journals was 18 titles, which together with the 40 titles were mostly borrowed from European libraries. Out of the 18 candidate journals, it was found out that 11 of them did not fit the scope of this work, nevertheless they are documented at the beginning of chapter 4.2 for reference purpose; the remaining seven journals, which might be part of a security management library, are analyzed in the subsections of that chapter as well. The second table of the referred figure shows the results of German journals research. Similar linguistics characteristics, as in the book investigation were in a first stage also considered for German journal titles; nevertheless, the wider scope of the single keyword querying method, explained above, was followed given that on one hand, the set of German journals is even smaller than of English ones and on the other hand, it was determined that in Worldcat and Ulrich's a left truncation function can also be emulated in the form of *?*keyword*, where *?* represents a fixed single character that takes all different alphabetic values in order to construct 26 different queries. As it can be seen, German journal occupy a smaller fraction in the academic periodical publishing, where 19, 2 and 1 journal titles where founded to contain a keyword related to the fundamentals of security management. The set of 22 journals was reduced to a group of 10 journals that might be part of a security library. Nevertheless, after consulting article copies from some issues obtained from four German and one Austrian library, it was determined that they were out of the scope of security management as a whole and therefore only English journals are documented in chapter 4.2.

3.3. Magazine research

The two previous sections focused on finding literature comprising an integral approach to security. This means that the surveyed publications focused on the

matter of corporate security or security management from a cross-discipline approach, putting together concepts and methodologies from several fields, in order to support and strengthen organizational processes from a holistic perspective, based on the objectives of the organization. The research scopes were German-speaking books as well as either English or German speaking academic periodicals. In this section, the target is again German speaking periodicals of non-academic nature, i.e. magazines not examined in peer-review processes. Actually as it has been pointed before, the whole research concentrates on German speaking literature, and the presence of a English speaking academic periodicals survey was due to the status of English as lingua franca for this kind of publications and for the international communication in general. Besides the academic journals and magazines researched in this work, there are other types of publications listed as periodicals that are not surveyed here; among them there are book series, yearbooks, newsletters, newspapers and internal organs to name a few. Nevertheless, when the relevance of a publication of these other types is such that it makes necessary to comment it, it has been handled and treated as a regular periodical exceptionally.

Books and academic journals are preferred in the academic world given their editorial review process, which increases the reliability of the works in terms of method, sources, clarity and results (Hames, 2007, pp. 1-9). This is not true for all books and periodicals, even when the latter commonly passes through stricter review processes than books. In addition, there are some publications which are not actually reviewed by no one else than the author himself, but are well received in the academia as for instance web blog articles written by recognized authors based on their research curricula and bibliography. Although scholars might not consider some non-academic magazines as reliable resources, by lacking of the authority character that a journal article acquires from its scientific based editing, these periodicals are regarded as key information sources to get an overview of the situation and state of the art on some field, industry or research branch with no further in-depth methodological investigation.

The German speaking magazine research is not focused to analyze these periodicals on the broader field of security management, but instead partial researches were preferred given the initial assumption that there are very few integral security management German speaking magazines, as it was indeed attested. By partial research, it is meant an examination of magazines according to the security fields defined in this work and the regular topics found in

these disciplines. Physical security, infrastructure resilience, information security and persons safety and security is the general structure on which the magazine will be allocated according to the overall or explicit bias of the column and editorial articles as reported in section 4.3.

There are several databases available for periodicals research such as the Karlsruher Virtueller Katalog and the Worldcat discussed in the books research section in this chapter, where it was stated that although these tools are valuable first hand resources for researches, they concentrate on the actual physical availability of publications in German and abroad libraries. Just as if the Deutsche Nationalbibliothek was useful for researching in the largest database of German speaking books, it also keeps the same strict record for periodicals through its Zeitschriftendatenbank (Staatsbibliothek zu Berlin, 2010). This periodicals database is thus the most reliable resources for finding all German magazines and almost all Swiss and Austrian publications as well (Rost, 2010, pp. 150-153). The periodical issues are kept in the Deutsche Nationalbibliothek building in Leipzig and Frankfurt am Main, which are only in-house-lending libraries; the subsequent issue articles fetching was later done through interlibrary loans using the Cooperative Library Union Berlin-Brandenburg, KOBV. The selected research database, the German Zeitschriftendatenbank, allows the search for right truncated words. Nevertheless, similar to other bibliographic databases, the Zeitschriftendatenbank's keyword indexing is made only for whole words beginning from left to right alone, which hinders the search of substrings in multistemmed compounds with header and one or more modifiers. The Zeitschriftendatenbank has neither implemented stemming algorithms to create stemmed indexes. As a solution, the same method for books and journals had to be used to simulate left truncation, where a single word query is the base or produces at least 26 different queries for all the alphabet letters, where one of them would be *u*sicherheit** in order to find possible magazines titles such as *unternehmenssicherheitsmanagement* for example. Overcoming the database compound problem in German, a further step is to define the key words set that can deliver a manageable set size. This means including or discriminating those words whose querying would return a title set that can be filtered manually. Some redundant words might enlarge unnecessarily the size of the result set and therefore probably increasing the manual filtering hours by a considerable factor. A first attempt was to include all word that seemed relevant such as the German terms for incidents, investigation, software, public relations to name a few, besides the basic terms of safety, security and the like. Such a search gave back results corresponding to at least

one ninety hours of manual filtering roughly. It was observed that the marginal benefit of including very specific terms was very low and in many cases, there was no profit at all after including these terms. Another observation was that even though the titles themselves rarely contain the searched word –consider for instance Der Detektiv or Wik magazine titles–, it is the subtitles that at the end contain the simple generic term of security or safety for instance, e.g. Die Fachzeitschrift für Sicherheit in der Wirtschaft.

Stems for all four disciplines	Matches
secur	2,220
sicher	3,804
risik	197
krise	119
safety	1,904
Total with *~2%* duplicates due to parallel querying	8,244
of which have unclear description or are not magazines type periodicals	189
rang a bell but have other scope	15
belong to the scope of this work	51

Figure 5 Magazines search keywords sets and query results

It is important to remind that the only reliable database field is the pair title-subtitle. A research based on publication category fields leads to incomplete or very large results; that is, an e.g. IT security publication can be catalogued to economics sciences in one library whereas in others to mathematics. The reduced keywords set is shown in Figure 5, which also presents the results set size for each term. The overall result size for the terms presented is over eight thousand periodical titles. This figure roughly corresponds to a couple of workdays for manual filtering. Other than in the book research, no script was here necessary to fetch the results from the Zeitschriftendatenbank, since it allows larger download sets to be later managed by a spreadsheet. A short algorithm was indeed coded in this application in order to reduce the set size discarding English speaking titles for a further manual filtering, that subsequently resulted in one 189 titles. Fifteen did not correspond to any security discipline and finally 51 titles were chosen and treated in section 4.3.

4. Literature analysis

The last chapter prepared three collections of publications to be analyzed. The availability check of the media in those sets was done through other databases. The catalogues of the Deutsche Nationalbibliothek for books research, of Ulrich's and Worldcat for journals and of the Zeitschriftendatenbank were used simply to check the existence alone of the searched media as of summer 2010. The present research used the interlibrary loan services of the Cooperative Library Union Berlin-Brandenburg, KOBV. All media was found in libraries throughout Germany with the exception of some journals that were later discarded in addition to some non-analyzed books that were employed for the edition of the initial chapters of this work. Magazines, journals and other types of periodicals are commonly not loanable outside libraries and even within the library buildings, free access is not possible and in-house borrowing requires registration. In some cases, it was necessary to consult physically some magazines in the Humboldt and Berlin Technical Universities in the Berlin-Brandenburg area. Nevertheless, given that only few scoped magazines were available there, at the end of the day it was recurred to the periodical photocopying and sending interlibrary service, which is indeed possible all over Germany through the KOBV or the corresponding state library union. Given that in KOBV photocopying orders the wished page ranges are mandatory, and whole magazines photocopying makes no sense and increases highly the costs for tens of magazines, or in other words hundreds of issues, the processes of article and page range selecting delays the overall working period of this research. This applies particularly for magazines articles, which are not indexed as academic journals are indeed, by e.g. Ulrich's or other providers. In many cases though, it could not be determined, via editorial websites and commercial en-

gines such as Amazon, Google Scholar and Books, Archive.org and the like, which magazines articles and which ranges could be ordered for photocopying, since simply this information can only be determined having an issue on hand or access to an online version of it. In these cases, a random set of pages was chosen based on the known regular page amount of the magazines. This method did work well for the magazines, for which no index could be fetched online beforehand: mostly author content was indeed sent with rarely some advertising. With regard to the selected publication years, recent exemplaries were preferred, nonetheless for long running magazines and journals random old issues were also necessarily considered.

This chapter is divided in three sections for the three types of media each. Their structure is the same beginning with a general analysis and presenting the results for the surveyed publications followed by several sections that describe and comment the publications considered. At the beginning of each section, there is a results table, which for the case of books and journals pretends to evaluate the relevance of each publication according to a simple rating scheme. The rating system is based on a percentage grade obtained by the weighted sum of relevancies with each security subdicipline in order to get a general rate for each publication from the perspective of an integral security management perspective. The weight or share of each subdiscipline differs between each other and differs between books and journals media too, where in the former the basics topics more importance and the secondary topics or actual security subdisciplines have more weight for the latter. Magazines cannot be rated from a global security perspective and instead only individual subdisciplines ratings were determined In order to allocate which subdiscipline bias has each magazine. The purpose of rating is not quite to determine which publication is better than other is, but to establish a scheme that can roughly tell which publications have more resemblance and consistency with the security fields as defined in this work.

Even though it was pursued to stick by the main idea of surveying journals and magazines alone, in some cases it was considered necessary to study and include a couple of other periodicals of different nature. These include one wall newspaper, two yearbooks and a conference proceedings book among few others that did not comply with the security management concepts in the books analysis chapter. In this point is important to mention beforehand that whereas relatively little material was found for journals and books, the chapters and the summary tables provide additional titles that partially fit in the corres-

ponding analyses and also some that might be positively allocated by other researchers.

4.1. Books analysis

In the German sprachraum, there is plenty of literature dealing with all the topics of security management. Nonetheless almost all the books treat security subdisciplines in a separated way and many of them do not restrict to the solely focus of corporate security, but they deepen into each subdiscipline without a holistic perspective of corporate wide management. As example, risk management books might deal with operational and strategic aspects of corporate governance, property protection publications often examine security methodologies with a strong tie to surveillance technology and information security books tend to study the technical fundamentals of computer and network security with almost no relation to other topics of corporate security. In the following paragraphs are presented some books, which deal with some partial aspects of security as a top management responsibility but fail to provide a complete approach to corporate security, some other books in this set may be not quite actual as well but it was considered necessary to document the most relevant material on security management. Sections 4.1.1 to 4.1.5 on the other hand present the books that are considered the most relevant of the security library.

There are some books related with operational risk such as the **Unternehmerisches Risikomanagement** (Adams H. W., 1992) which is a band belonging to a series edited under the title Das zukunftsichere Unternehmen by the Technischer Überwachungs-Verein Rheinland. The series were published after the congress Bessere Organisation – mehr Sicherheit in 1992. Although the congress proceedings and the profile of the TÜV are commonly associated with technical safety, the referred book deals with a broader scope of risk. The book pictures several scenarios for introducing several threats on the operative and strategic risk components in order to concentrates on the former from a safety, security, environment and logistics point of view. Although the book might be out of date on some technical aspects, the author attains to settle the fundamentals of corporate risks and its analysis giving an insight into measure identification and other topics of security management in a lesser extent.) Another relatively recent collaborative book dealing with risk management and incident handling was published by Behr Verlag with focus on the food segment with title **Risiken vermeiden, Krisen bewältigen** (Elles, 2008). Although the present work avoids concentrating on specific industries, only two authors and chapters of the book pay strong attention on particularities of that branch. The work has

a deep understanding of security management on its preventive and reactive elements. A special remark is the extensive study of crisis management and the analysis of contingencies with scope on reputation, communication with public authorities and know-how and data protection in crises not found on other publications. Another book on the same line of risk management is **Praxisleitfaden des operativen Risikomanagements** (Meier, 2007) published in 2007 approaches the field of security management from the perspective of standardization. The highlights of the books concentrate on recommendations, certification and obligations of organizations on risk management and business continuity practices. The book intends to study the implications of several standards on risk management, which affect compliance, audit and PDCA aspects when assessing operative risks, and implementing measures on both preventive and reactive phases in security management.

A very complete work not dealing only with risk management and incident handling and worth to consider is the **Vernetztes Betriebssicherheitsmanagement** (Tenckhoff & Siegmann, 2009) published last year by Haefner. The book covers most of the topics of security management on the start point of process quality. The authors study the responsibilities in a corporate environment on several fields of operational risks, how to manage them and analyze several roles and processes on crisis scenarios. Security management literature has commonly a tendency to cope with the criminal aspect in the fields of physical security and information technology. The book instead emphasizes the collaboration between several areas such as safety, occupational health, environmental safety, infrastructure safety, property protection and information security in the frame of quality, compliance and business resiliency. Being written in Germany, the authors provide a deep description on norms and regulations on this matter relevant for European and German organizations. Another publication dealing with most corporate security topic is the **Praxishandbuch Unternehmensschutz** (Ohder, 1999-), a looseleaf service updated regularly by Boorberg. These kind of media is not commonly catalogued neither can be referenced as regular books, nonetheless the relevance of the topics covered makes necessary to mention the publication. The Praxishandbuch is authored by several persons dedicated to security, safety and crisis industries. The work concentrates on up to date material and methodologies on topics such as property protection, security technologies, corporate security management and crisis and contingency planning. The authors focus and revise the articles of the Praxishandbuch based on industry or standards releases or major events such as pandemics and major events bringing up and summarizing methodologies and

experiences on risk management, threats and crisis management. A special remark of the work is its corporate focus pursuing to analyze threats and concerns to global players such as information technologies, product criminality, logistics and security analyses from a global perspective.

A book clearly related with property protection but relevant for security managers is **Security als Managementaufgabe** (Lindner, 2007) published by the Steinbeis University which is a work focused mostly on physical security and its role in industrial process chains related to quality management and consumption plans for instance. Although the book is not quite related to other fields of corporate security such as information technologies, risk management and safety, the importance of the work lies on the deep understanding of integrating classical safety topics such as property protection and access controls in the corporate security practices with the scope of pursuing the organization's objectives. The book **Sicherheitsmanagement** (Ibing, 1996), on the other part hand, of the series Die Bibliotheca der Wirtschaft focuses also on particular aspects of corporate security such as property protection and industrial safety. The series was edited until some years ago by the same group of the Süddeutsche Zeitung and reviewed by the insurer HDI. Although the book lacks of other security topics such as IT and crisis management, its relevance lies on portraying the topic of insurance within the framework of security management. In general, security literature concentrates either on methodologies coping with threats, the realization of contingences and enterprise risk management or else with sharing financially risk transfer and risk sharing among other topics; in this sense, the book on its own studies the connection between security, safety and insurance from a non quantitative perspective. Sicherheitsmanagement is divided on safety and security chapters for which threat analyses and risk management methodologies are given. Some recurrent topics are loss prevention, property protection, fire prevention and environmental safety for which risk analyses and measure identification are examined from a general industrial context.

To finalize, there as a book by Von zur Mühlen difficult to catalogue given that it is based on data centre security but actually provides, as the author states, general principles and methodologies for managing corporate security and physical security. Indeed, deriving methodologies from other established fields is common in technical sciences, for instance, risk management schemes for several industries are modeled from economic science originally and also Müller's Unternehmenssicherheit covered later in this chapter is based on IT se-

curity models. **Sicherheits-Management** (von zur Mühlen, 2006) describes a set of 10 principles for security planning based on an example for data centers. The systematic explained by the author consists on precepts such as availability, uniformity, consistence and anticipation related to assets, security measures and threats. The book should be considered as a systematic approach to security planning rather than an information source for other topics of security management such as specific risks in corporate security.

The present work does not pursue to find a relative best publication on security management but to collect the most significant title on this field. Nevertheless, a rating scale might be useful to orient readers and researchers on the relevance of the books and their material. Figure 6 shows the result of the analysis in a rating scheme. The table is vertically divided on two sections, namely significant and other titles. The books of the second section correspond to the eight titles summarized earlier in this chapter, which hold only a partial relation with the discipline security management. The other five books comprised in the first section of the table are extensively studied in chapters 4.1.1 to 4.1.5.

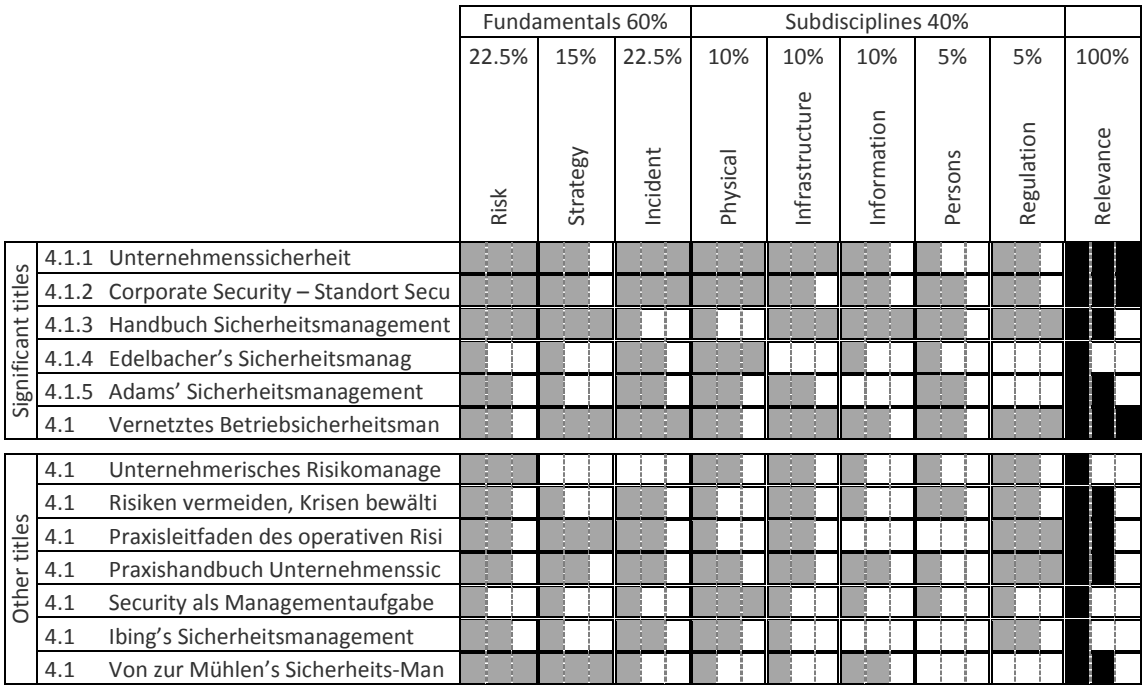


Figure 6 Books rating

The table has a further slighter vertical division that separates fundamentals topics of security management from the accompanying subdisciplines. The former is composed by risk analysis, measure identification and implementation topics as well as by incident handling. The subdisciplines correspond to those grouped or considered so far, namely physical security, infrastructure se-

curity, information security, person safety and security as well as regulation, standards and liability. The method to measure the relevance of the publication was to assign a discrete value to the topics covered in the book from 0 to 3; these discrete values are represented by shaded rectangles for each publication. That is, each publication was measured by eight parameters: risk, measures, incident, physical, infrastructure, information, persons and regulation topics. For each parameter, a shaded brick is provided by a 0-1-2-3 scale, which measures the relevance of the book with the corresponding topic. 0-shadings and 3-shadings represent respectively absence of material or a strong relation of the publication with the given topic, whereas 1 and 2-shadings symbolize an equal spaced rank between both poles, i.e. values that imply partially related material in the publication. In order to comprise the eight single ratings in a general value assigned to the publication relevance showed in the last column with a darker shade, relative percentaged weights were assigned to each of the eight topics. The assignment of weights was a subjective step in which several consideration were made. The first factor was that a book on security management covering all the fundamentals might provide general methodologies that can be applied to any subdiscipline. That is, a book that provides an accurate understanding of threats and risks, general methodologies to successfully apply measures for risks minimization and a systematic approach to contingencies handling, is a book that might be useful for all security subdisciplines. Such publication might help to understand the risks, measures implementation and incident handling in the physical, infrastructure, information, persons, regulation and any other dimensions relevant to security management without deepening or even covering any particular subdiscipline at all. Given this consideration, the fundamental must have a minimum weight of 60 percent, corresponding to a 22.5 percent for both risk and incident topics and a lower 15 percent for measures where specific implementation practices can be very heterogeneous depending on the industry or organization type. At this point is important to remark that no strict numerical rating is pursued by this process, but such percentage values are the result of the considerations mentioned above and trying to assign evenly balanced values for topics with equal importance. Most of the remaining 40 percent correspond equally to physical, infrastructure and information topics with 10 percent each, whereas persons and regulation was considered as the lowest level of importance in corporate security, given that persons are rarely the target of criminal efforts. Regulation topics, although highly important for liability matters, can be considered aside if all the other process and topics were successfully treated by the security management. The last Co-

lum of the table contains the overall weighted rating for both groups of books, for which an analysis argument follows in the next section for the most significant titles group.

4.1.1. Unternehmenssicherheit

Unternehmenssicherheit (Gundel & Mülli, 2009) is a concise work making a holistic examination of operational risks and security measures within the general interest frame of present-day industry and trade. Gundel and Mülli achieve an unusual balance in comprising such a complex and extensive discipline in a concise manner by setting clear objectives from the beginning and putting aside broad technical explanations, which might belong to other subordinate fields. The book is organized in a consistent way, by following a logical thread to the question of creating a robust organization against internal and external threats. In this sense, the authors explain the problem of what means secure for an organization and what has to be protected followed by the question of implementing efficient and durable measures. The book closes with a comprehensive study of incidents and crises, their organization, recovery process and relations with third parties such as public bodies and media. Written in 2009, Unternehmenssicherheit is the most recent corporate security book in German, hence it represents an up to date state of the field including reliable reference currently.

According to the book, the identification of risks begins with two iterative steps, which yield the set of threats relevant to the organization's activities and the definition of protection objectives according to both the organization's goals and external requirements. The threat analysis deals with the identification of threats related to the organization through the review of threats groups, specific threats and possible scenarios. On the other hand, the book explains that an analysis of external requirements for the definition of a desired security level comprises regulatory, liability, criminal and stock companies laws, property, liability and person insurances on the grounds of responsibility and asset protection, investor stipulations as well as the public interest. Several factors of influence are also an essential element in the definition of the security level pursued by the organization. The criticality of services from the point of view of the general community, business continuity management and corporate social responsibility are mentioned examples of relevant factors of influence in the definition of an organization's security level. The book explains that the grouping of external requirements and factors of influence results in the target dimension of the security concepts, for which the former have to be prioritized.

Each target is related to a protection objective, for which qualitative and quantitative definitions are made (Gundel & Mülli, 2009, pp. 17-73). As final step of risk identification, the authors describe the classical risk assessment schema, in which a short-range discrete scale is used to map risk values on probability of occurrence and damage extent coordinates. More elaborated risk assessment methodologies take into consideration the failure mode and effects analysis, legislative requirements for quantitative risk analysis and formal financial impact analyses.

The authors explain further that the analyses of risks, protection objectives are the basis of measures identification, and that the categorization classification of protection objectives is related to the classification of measures. In this sense, the book differentiate between safety and security for a first general classification of measures, including earthquakes, fires, property protection and information security, for which normative, technical and organizational aspects are given. The assortment of all measures to be implemented is the basis for a security concept documentation, which contains the entire security procedures taken by the organization as a single body. An evaluation of cost and benefit of identified measures accompanies the process of measures identification, which is particularly important for budgeting (Gundel & Mülli, 2009, pp. 75-76, 144-152). The methodological strategies proposed in the book are the German Scale of Fees for Services by Architects and Engineers, or HOAI, and the Swiss SIA 112, which in the book are described in the frame of corporate security and include the strategic planning, preliminary study, project planning, tender, implementation and control of security measures. The structures in charge of implementation and maintenance as well as the one responsible of reactive security issues are the security and incidents organizational structures. The authors distinguish three types for the former, namely adjunct, centralized and hybrid models. After the organizational security structure is established and the security procedures implemented, the up keeping of measures is done for both technical and organizational aspects through the conception of maintenance plans, control intervals, training, audits and exercises (Gundel & Mülli, 2009, pp. 154-167, 181-203). In closing the security process, the book identifies a series of stages leading to occurrences of incidents and crises and their planning. The authors characterize the latter as the preparation of all organizational procedures aimed to minimize injuries, deaths and damage and loss of property as well as the control of further damages to the organization and the return to the normal state. In terms of organizational architecture, the book defines the functions and structure for both incident and crisis management paying atten-

tion to communication with auxiliary services such as rescue corps and police as well as with media and public relations agencies (Gundel & Mülli, 2009, pp. 211-239).

The physical security topics studied by the authors deal mainly with property protection as described along these lines. Break-in protection is partially described as the sum of procedures that shield and monitors property perimeters through electronic, mechanic and personal means. Access control within and between the property and the exterior consists of electromechanical and electronic devices, for which Europeans norms are provided together with a study of several access identification technologies. As third point of physical security, the authors explain both break-in alarm and video surveillance systems and types as part of monitoring techniques. The book recommends a periodical examination of all security related mechanism and permissions through the physical inspection of security devices and the deployment of a functional access management system (Gundel & Mülli, 2009, pp. 110-131, 185-187).

The authors characterize information security in both its technological and human aspects as possible factors of information drain. Failing to appreciate the importance of IT and information security for operational purposes, the authors approach this field primarily from the perspective that electronic systems are in fact knowledge containers, which have to be protected against criminal practices. In this sense, the book defines IT security goals such as confidentiality, availability, integrity and authenticity and gives a number of recommendations to improve IT security related to software, access, cryptography, networks and backing up. The authors mention that the maintenance and control of IT security implementations is typically done through security scans, security software, intrusion detection tools and penetration tests. On the other hand, the authors identify that one issue with internal perpetrators, e.g. a company's own associates, is the misuse of the organization's know-how and other sensible information among other types of criminal activities. Accordingly, the book revises several measures such as preemployment screening, guidelines and codices of conduit, openness in payroll and promotions, sensitization and coercion (Gundel & Mülli, 2009, pp. 132-139, 187-188).

Some German and Austrian work safety norms together with standards emitted by the International Labour Organisation are mentioned in order to explain that corporations are responsible of implementing work safety and occupational health measures, for which a regulatory offense generates particularly high sanctions in industrialized countries. The variety of possible measures differs in

function of the size and type of organization. The authors hence concentrate on general types of safety measures such as physical and technical configuration, utilization of adequate working clothing and organizational measures such as training and instruction (Gundel & Mülli, 2009, pp. 108-110).

Although other infrastructure security terms like flood protection, blackouts and other failures are mentioned throughout the book, the authors elaborate on the safety topics of building statics and fire protection. They remark that in highly legislated countries the adherence to existing norms gives beforehand a valuable level of protection in this matter. The book refers to a series of European norms such as the Eurocode 0-9 for statics and earthquake protection, in explaining building planning issues in this field for instance support capacity, conversion of buildings to a new use, trafficability and ground plan types. Fire protection is analyzed from its normative, planning and executive aspects. The book provides a number of architectural considerations such as, fire resistance and statics, creation of fire compartments, distance between buildings and escape routes. Among the technical fire measures, the book explains diverse criteria in the design of fire alarm, gas detection, and fire extinguishing and smoke extraction systems. As final point of fire protection, the book examines the process of preparation of fire control models, for which fire protection, security and operational concepts are the basis of a sequence of implementation and testing steps leading to the endorsement of the fire plan (Gundel & Mülli, 2009, pp. 76-105).

Apart from technical standards cited in the safety and security measures section, the book is not particularly strong in legal and other kind of normative references. Nevertheless, the authors included liability considerations, which is a recurring deficiency in the literature. Accordingly, the book covers topics like environmental protection and prevention of hazards, as for example scenarios of logistics and transport of dangerous material (Gundel & Mülli, 2009, pp. 105-108).

4.1.2. Corporate Security – Standort Security

The global character of large-scale organizations, such as conglomerates and multinationals, implies particular security challenges given the diverse scenarios and environments in which this type of companies is present. The title **Corporate Security – Standort Security** (Sack, 2007) suggests beforehand the orientation of the book to global players and the conception of security at both international and local levels. The book makes an initial differentiation of the

concepts security and safety by stating that they deal with deliberate acts and technical and human failure respectively. In this sense, the author uses the term sicherheit as broader term, in order to describe operational risks encompassing the security and safety subordinate areas. The book concentrates entirely on security defined as a discipline that copes with unauthorized and criminal actions, for instance efforts to the detriment of property, information and associates. In line with the author's definition of safety as a state of controlled technical failure and managed reckless conduct, only occupational health related topics in addition to infrastructure security are actually left apart. The work is published by and is oriented primarily to the academia; as such, most of the concepts are presented together with a couple of illustrative examples, which makes the book suitable for a wide public including security professionals. However, taking into consideration that the work is intended to graduate studies, the inclusion of direct literature references, the elaboration of additional figures and the incorporation of an index would contribute to an enhanced composition. The book follows a logical thread beginning with the study of risks and possible solutions together with the handling of incidents and crises as analyzed as follows.

Physical security is related mainly with control and surveillance of the movement of persons and objects as well as the perimeter protection round a property within the context of site security. The author explains that access control is determined by the complexity of the property in terms of the number of ways physical penetration is possible, the evaluation of material and human assets inside the property together with the response capacity of security and emergency teams. Further considerations examined in the book deal with legal and internal requirements such as controlling of hazardous material and vehicle traffic within and outside the property. Both access control and perimeter protection functions are accomplished through the conception of technical, organizational and personal measures. Since the higher cost of security employees is often minimized by an appropriate planning of technical and organizational measures, the book provides a description for several electronic and mechatronic passive and active technologies, in addition to the conception of organizational considerations, including the anticipated planning of buildings and the reduction of vulnerable physical accesses. The author goes deeper in explaining that areas and rooms with higher security requirements, such as executive offices and warehouses with high-valued assets can be protected by specific technical and personal measures. As final point, the book delineates the organizational and hierarchical features of a response and operations centre for site

and corporate security, for which the book introduces concepts of permanent availability, patrolling and the intervention process during access violation incidents (Sack, 2007, pp. 117-132).

The view of the book on information security goes a step further the typical association of the topic with information technologies. The author regards information as the collection of public and confidential knowledge of the organization's assets, processes and resources, which, although might be mainly stored in electronic networked media, is also kept as diagrams or data physically in paper or archives and refers likewise to the information flow for instance in meetings and telephone conversations. The book explains that information leakage can take place due to negligence or as a result of targeted criminal efforts. There are several risks and measures related with the former such as dealing with information handled by associates and external employees, for which training and several guidelines must be accomplished in order the reduce the number of leakage incidents. The range of criminal practices extends from perpetrators working internally for the organization to the acquisition of information through high-end resources such as parabolic microphones, satellite imagery and informatics. The author introduces concepts of industrial espionage in order to explain a set of criminal motives leading to the illegal acquisition of information. Among the causes, count state intelligence and competitive intelligence (Sack, 2007, pp. 87-107).

The topics related with protection of persons are handled from the perspective of corporate personal security by describing both individuals and event security. On the former, the book explains the basics of a person protection concept ranging from the private house to the working location and the route between both. The author identifies a set of proceedings so as to increase the security of individuals such as technical, organizational and personal measures. It is pointed out that escorted security is not a privilege, but the result of a risk analysis targeted to a specific associate or the organization's hierarchical position itself he or she occupies. In this sense the author highlights a series of considerations that are involved in the creation of a security concept for individuals such as the working environment, business trips and events, family members and health issues, which results in the grade of vulnerability of a person and protection needs. A similar approach is taken when reckoning the risks associates are subject to in collective events. The book explains that the arrangement of large-scale events outside and within the property demands particular protection measures. The organizer team must involve the security management

throughout the event coordination in order to estimate measures related for instance to the number and type of participants, access policy, escape routes and emergency services among others (Sack, 2007, pp. 73-82).

The central legal reference for a German global player for the accomplishment of security management is the Supervision, Openness and Accountability Act (KonTraG), which demands the board of management to assure the continuity of the organization through the anticipated identification of threatening events. Although the author makes clear that the KonTraG applies to German stock corporations, he points out that this reflects the European legislative interest in financial and operational risk management along with matters related to crisis management. The topics of information protection present two principal legal aspects: the Federal Data Protection Act that requires saving personal information from exposure, injury or misuse along with industrial espionage aspects, being the latter particularly relevant for global players. As a final point, the book presents a remarkable discussion on the limits between the competence of security provided by both the state and privately by the organization. In this sense, the book mentions that, according to the German Civil Code (BGB), the Industrial Constitution Act (BetrVG) and the Penal Code, the organization is committed with several purposes in a site security level. Example of it is the protection of the organization's assets, the prevention of crimes and the protection of employees in the sense of safety and occupational health (Sack, 2007, pp. 35-37, 62-65, 87-89, 97-99, 110-115).

4.1.3. Handbuch Sicherheitsmanagement

Security is a state, in which a level of freedom of dangers is present beforehand or is achieved through a process. The way to accomplish this state in an organization is something that is commonly not formally, comprehensively and above all systematically studied in the literature. The **Handbuch Sicherheitsmanagement** (Müller, 2005) provides its own perspective to the question of analyzing and implementing the security needs in an organization based on a hierarchical and cyclical security management methodology. The approach of Müller is based on a general-purpose, pyramidal-shape architecture of his own, tailored to the problematic of corporate security. The seven-leveled pyramid was though conceived, and originally made public as such, to solve managerial aspects in the field of information technologies, where the author himself comes professionally from. Nevertheless in IT-Sicherheit mit System(Müller, 2003), when the view of universality of the pyramid developed, the author explains how his management design can be applied to business administration,

environmental safety, plant safety, quality, project management and corporate security, to name a few.

The versatility of the pyramid lies on the fact that management is a series of hierarchical tasks and changes in a cyclical fashion. The top defines the direction of the organization whereas the underlying levels hierarchically delegate responsibilities becoming more complex and geometrically wider on operational levels. Seen from the top downwards to the base, the first to the seventh levels of the security management pyramid are security and risk policy, security objectives, security function deployment, security architecture, security guidelines, security specifications and security measures. There is a continuous interaction between upper and lower levels that underlies a periodical transformation and improvement of the management organization.

The starting point of risk identification is the definition of security objectives based on the security and risk policy of the organization. The book explains that the security policy is the most important step in the security management process, since it comprises the objectives of the organization and the completion of products and services. Furthermore, the security policy represents the weight that the topic security has for the organization's strategy. The latter considers requirements from third parties equally in the conception of policies, essentially the legislative and industry norms. The book describes that the security objectives, in accordance with the security policy, encompass the definition of a business impact analysis, which yields the protection requirement for core processes and their resources (Müller, 2005, pp. 71-130). The third level of the pyramid transforms processes and objects in measurable elements in order to fulfill the security requirements in the implementing phases. As closing stage of the risk identification, the security architecture provides the basis of a threat analysis and the security strategy. Based on the priority processes and objects derived in the previous phases, and with the help of a classical probability of occurrence-damage extent map, the security architecture emits the organization's security principles, which are supported by several disciplines such as management of conformity, data privacy, occupational health and safety, financials, projects, capacity and continuity (Müller, 2005, pp. 131-304).

The latter level of security architecture previously described actually comprises three sublevels, which represent the transition between the topics of risk identification and measure identification. The analyzing character of the pyramid becomes operational after the definition of security strategies and the roles supported by the subordinate disciplines mentioned above within the security

architecture. The three lower levels of the pyramid cope with the definition of security guidelines, concepts and measures for each process and object derived from the risk identification phase. The guidelines represent a general basis for the systematic security management, which is oriented to the security level required in the pyramid's upper levels such as the security policy. The remaining levels of security concept and measures represent but the totality of instructions and verification protocols of the corresponding processes and objects (Müller, 2005, pp. 305-348). The final part of the book deals with the continuous improvement of security, in both its analytical and implementation aspects, through the integration of security management in the lifecycle of processes, resources, products and services. An organization is subject to constant transformations. The security management should go together with these changes in order to guarantee the proper recognition of new vulnerabilities and threats. The security controlling and the Deming cycles support the structure and adjustment of the security management to the continuous transformations inside and outside the organization (Müller, 2005, pp. 349-400).

Although the book does not contain an extensive study of incident handling, it explains concisely the topics of business continuity related to information availability along with measures for provision of general incidents and catastrophes. The subordinate discipline of continuity management explained in the security architecture part approaches the problem of technical breakdowns with the help of information security examples. For this purpose, the author explains concepts as document securing and data protection, suggesting the execution of similar approaches for dissimilar topics such as failures and incidents of personnel, properties and assets. The incident and catastrophe management outlines the composition and the tasks of the crisis teams together with crises simulations (Müller, 2005, pp. 221-240). Moreover, the security concept part provides a couple of models to establish incident and catastrophe guidelines. The author broadens at this point the revision of continuity management by explaining the life cycle of incidents introducing the concepts of incident discovery, immediate measures and recovery process. The security concept provides in addition a brief guideline and layouts for bomb threats scenarios (Müller, 2005, pp. 319-329).

The book presents the topic of physical security with the designation security management by presenting concepts of property protection and entity rights management. The influence of IT security makes the book tend to the subject of information protection. In this sense, the topics of protection of driving

access, admission, personal access and physical access are explained within the setting of information protection. Nevertheless, the author presents an interesting subject-object model with the scope of rights management for each four layers of access type. From the technical side, a series of solutions for access control such as biometry devices, USB tokens and X-ray scanning (Müller, 2005, pp. 240-274).

Information security is present throughout the entire book. Even though the back and front matter suggests that the work handles an integral concept of security, it is difficult to deny that the continual examples and scenarios reveal the recurrent focus on information security rather than physical security, person safety and security, incident handling or other aspects of security.

The work handles the problematic of corporate security with the aid of the management pyramid; it can be said that the book is about the security pyramid. During the course of the work, the area of information security acquires more attention, whereas other aspects become gradually excluded. One possible explanation is that a work such as the Handbuch, that provides a formal methodology for corporate security as a whole, has the dilemma of presenting the discipline in a very abstract way following a thread such as information technology, or else expanding the extent of the book in order to cover as many security aspects as possible.

The person safety topics concentrate on occupational health. The author touches the topic from the fact that German organizations are obliged to protect their employees against dangers and provide healthy work conditions (Müller, 2005, pp. 181-183).

The author refers to infrastructure as a classification of resources together with assets such as information and personnel. Within the frame of continuity management, the book describes a number of security elements such as fire and flood prevention that have to be considered in the security architecture. In addition to this, the level of security concept provides several guidelines for redundancy of power and communications resources. Although the book shows for these topics also a tendency to information security –concretely in this case for computer centers– the basics of infrastructure are reasonable explained in order to apply them to other environments beyond IT security within the corporation e.g. manufacture or logistics (Müller, 2005, pp. 252-257, 319-327).

The Handbuch has a remarkable background of laws and regulations. In this sense throughout the book, the organization's competitiveness principles sup-

ported by the security management goes together with remarks and highlights of external requirements from German and international laws, partners and the industrial landscape. Worth mentioning are two sections where the book defends the necessity of a corporate security management by compiling and citing the Trading Code (HGB), the Federal Data Protection Act (BDSG), the Public Companies Act (AktG), the Supervision, Openness and Accountability Act (KonTraG), the Sarbanes-Oxley Act and the Basel II regulations among others (Müller, 2005, pp. 43-49, 89-118).

4.1.4. Edelbacher's Sicherheitsmanagement

Sicherheitsmanagement (Edelbacher, Reither, & Preining, 2000) of Edelbacher, Reither and Preining describes the fundaments and tasks of security management with a strong practical orientation. The book, written from a criminal starting basis by experts in investigations, gives also methodological guides about how corporate threats can be managed. Throughout the book published in Vienna, the authors describe a number of examples and scenarios such as information leakage, terrorism, technical safety and security, IT security and touch other topics related to police-like tasks within corporations such as coping with extortion, rape and murder scenarios.

Together with a wide compendium of threats, the authors concentrate on giving systematic solutions to risks that can be present in an enterprise environment. In this sense, they give a detailed description from the identification of security issues, through the security analysis of such problems, to the implementation of measures. For this purpose, it is described the procedures that the management can take in order to make a so called current situation analysis in order to deliver a general picture of the organization properties and security issues. In this sense, the authors begin with statistical insights with the purpose of telling what is relevant for organizations.

The risk identification is approached through three bases in which the economic justification of security management is given along a methodology for threat analysis and some basics regarding the cost/benefit analysis of security. It is explained that the lack of an established security competence in organizations is due to the opinion that security management represents a non-profitable cost center. In this sense when an incident is presented the organizations react according to basic measures without analytical background or they overreact spending more efforts and budget than required. A so-called danger portfolio with classifications is presented by the authors to give way to the threat analy-

sis, putting special attention in criminal considerations by studying the attractiveness and resistance of both assets and security (Edelbacher, Reither, & Preining, 2000, pp. 72-85). In connection with the threat analysis, three methods for cost-benefit analysis are briefly explained; these are based respectively on a probability matrix, risk expectance values and a risk simulation process (Edelbacher, Reither, & Preining, 2000, pp. 86-95).

The work does not give a main thread, by which the security can be improved methodically and continuously and its measures systematically identified and implemented. Instead of this, a number of isolated recommendations for several threats are given through the entire book on how to attack specific threats and commonly pointing out to specific solutions such as those for access control and information security.

The topics related to incident handling consider possible problematic situations for which a guideline is given on how to manage and to be organized for incidents and crisis. The incident management is detailed through the organizational features of coping with these events for which the task, internal communication and work methodology of a crisis team is explained (Edelbacher, Reither, & Preining, 2000, pp. 299-302). Going further into specific crises, the authors give some guidelines for the preparation of evacuation of buildings under emergency circumstance and types and properties of bomb threats (Edelbacher, Reither, & Preining, 2000, pp. 302-315). An informal consideration of risk transfer concludes the incident handling topics by mentioning the possibility of insurance contracts. At this point it is worth to mention that the whole last book chapter is dedicated to the legal framework and police support in Austria on which security managers can base investigations tasks for criminal acts in cooperation with services and bureaus of the criminal police of this country.

The physical security is approached by a property security perspective. Beginning with maxims of protection such as security from the outside inwards and the interplay of organizational and technical efforts (Edelbacher, Reither, & Preining, 2000, p. 101), the book dedicates an extensive chapter on illustrating technical mechanisms and devices for protecting properties from unauthorized access. A third of the book body, in a sole subsection (Edelbacher, Reither, & Preining, 2000, pp. 102-195), is dedicated to the description of access control devices, alarm systems and video surveillance. Together with the general focus of the book on criminalistics, suggest that this work is not oriented to the prob-

lematic of security management as a whole as the front matter of the book claims.

Organizational and technical factors compose the topics of information security. Given the fact that the book was edited ten years ago, it is comprehensible that much of the content presented lacks of actuality. Example of this is the millennium problem of two and four digits representation of years in old informatics systems and the dilemma of choosing isolated or networked computer solutions at the beginning of the worldwide web era (Edelbacher, Reither, & Preining, 2000, pp. 232-298). The publishing year cannot be though a restriction for the book to omit IT security concepts or present IT security basics such as those based on the confidentiality, integrity and authenticity principles of information. A better approached topic and one of the less treated in the literature is the organizational aspects of information security that has to do only partially with IT security. Special attention is given to espionage, for which internal perpetrators as well as external persons can be used as tools for information leakage. This can be counteracted with organizational measures and security awareness (Edelbacher, Reither, & Preining, 2000, pp. 196-231).

Several person security topics are treated from the assumption that criminal efforts have been conducted in order to extort, commit robbery or blackmail an organization. In this sense, there is little distinction between incident handling and person security since most of the topics deal with person security in violent criminal scenarios such as robbery, kidnapping and hostages (Edelbacher, Reither, & Preining, 2000, pp. 21-45). These subjects are not discussed from a preventive point of view and little is said about crisis organization in these scenarios.

After revisions of the book, no topic could be found connected with infrastructure security. Only in the part of incident management, there were some passages dealing with fires, but not based or oriented in fire prevention, contingency planning or continuity management.

4.1.5. Adams' Sicherheitsmanagement

The book **Sicherheitsmanagement** edited by Heinz W. Adams is one of the first books in Germany that treat the concept of corporate security as a whole discipline. The authors handle security management from the perspective of risk and crisis prevention and control showing particular interests in aspects of security such as data processing, physical security and safety.

Although the book has the value of putting together and systemizing many of the security topics with growing importance at the beginning of a global oriented economic age years ago, the book does not show an academic methodology. The work, published by a remarkable media corporation, but neither specialized in economy matters nor scientific publishing, the Frankfurter Allgemeine Zeitung, is structurally based on a collection of articles that appeared periodically in an economy supplement of the FAZ and was subsequently published as book in 1990.

Along with the editor and principal contributor –founder of the Dr. Adams und Partner consulting firm–, most of the thirteen authors were associates of this company, what probably explains that many of the chapters seem rather to follow a white book format lacking of citations and references.

Risk identification is outlined through the presentation of risk analysis and risk policy, where the work defines the necessity and methodology of dealing risks in a corporative environment. Remarking that an organization has the principal objectives of planning and producing goods or services the book describes a methodology for the identification and minimization of risks based on a so-called Failure Mode and Effects Analysis. In this sense, the risk identification is based on the drawing up of the study of potential errors, potential consequences and potential causes and their measures in project management (Adams H. W., 1990, pp. 77-84). It is however not clearly explained how this methodology can be applied a step away from project management in the direction of security management. Nevertheless it is explained how the FMEA analysis leads to the rating of risks and the corresponding ranking of measures.

Connected with the risk identification is the security policy in which the book describes the importance of a top-level perspective when defining, modifying or redefining an organization's security policy. It mentions the use and characteristics of a security policy by explaining the delineation of objectives and tasks, the settlement of responsibilities and the methodologies as well as the process of risk assessment and finally requirements for external partners, i.e. suppliers (Adams H. W., 1990, pp. 129-131). The implementation of measures is a process done after the risk analysis. In this phase the security concept is implemented, for which the authors give a general methodology to implement the security guidelines through a model of pyramidal deployment of delegate functions and security responsibilities (Adams H. W., 1990, pp. 39-68). For the continual improvement and upkeep of the implemented security concept, the authors present a process based on quality modeling, with which a manufactur-

ing oriented security perspective is introduced in order to minimize threats that jeopardize the production and its environment (Adams H. W., 1990, pp. 107-124). The latter related to partners and infrastructure. Connected with security control there is a section of the book dedicated to the realization of audits by both internal and public instances. It is said that audit is an essential tool that guarantees the security of an organization. Based as well in quality models, the book presents the general aspects of an audit process from the checklist, planning and reporting (Adams H. W., 1990, pp. 135-152).

Emergency scenarios and early warning are topics introduced to cover the reactive aspect of security. In this sense, the book presents two perspectives in coping with emergencies. The first for a production oriented business continuity, in which it is tried to minimize the causes and effects of interruptions. The second perspective copes with the protection of people and legal obligations for organizations. For the managing of incidents, the regular tasks and organization architectures of a crisis team are presented in which training and practice of contingencies are in the front line (Adams H. W., 1990, pp. 307-339). Connected with this area the authors give a formal description and analysis of insurance when residual risks cannot be controlled to an optimal level or when a potential damage demands the existence of this kind of protection. The authors explain the costs, policy basics and financials of insurances and give some guidelines on deciding the benefits and disadvantages of transferring the risk to a third party (Adams H. W., 1990, pp. 202-218).

The property protection section covers both physical and infrastructure security topics. Although without major details on implementing access control systems (technical or organizational) or prevention of fires, the work gives a solid knowledge by explaining the property threat profile and the corresponding protection conception. For this purpose several kind of threats are classified on external passive factors (lightning, flood), internal passive factors (fire, explosion, power and machine failures) and active factors from third parties (bomb threat, sabotage, espionage, robbery). For the prevention of these risks, the property concept is explained by the introduction of technical, organizational, and personal measures (Adams H. W., 1990, pp. 185-201).

Person safety is explained from the perspective of security of workers inside the property of the company. For this purpose the books is only strongly based on the German legislation regarding the protection of employees and the legal obligation an organization has to this respect. After some explanation of this framework the authors briefly indicates that a current situation analysis and a

concept for work safety has to be done to comply with regulations (Adams H. W., 1990, pp. 170-184).

Throughout all the book references for laws such as the German Civil Code and the Penal Code are found. No references are made to other industrial standards and compliance as well as good practices for companies. At the beginning of the book there is a complete legal framework based on German laws that explains the obligations for German corporations such as the prevention of criminal and risky practices that an organization could take (Adams H. W., 1990, pp. 21-38).

4.2. Journals analysis

Security Management is an interdisciplinary field composed by topics such as risk management, criminal sciences, informatics, industrial engineering and operation research to name a few. As such, many journals focus on covering areas commonly related partially to security management. During this research, a lot of material has been found related to specific topics separately. Academic journals and other scientific publications are not the exception, since they cover research being done on particular areas of security management. This section pursues to document some periodicals that are not completely related with security management as a whole discipline but are not actually part of the proposed publications for a security management library. In these paragraphs are also included some publications which could fit in the general concept of security management though some of them are not published anymore. At the end of this section, a summary and introductory analysis is made of those publications that are indeed recommended and studied from sections 4.2.1 to 4.2.7.

Some periodicals are closely related to IT security but include many other topics on security management such as the discontinued trimonthly **SIG Security, Audit & Control Review** (1982-1997), which focused on IT security. The journal published until 1997 had highlights that apply very well for nowadays information and physical security principles on other topics out from IT for security managers on the ground of information protection. In this sense, many articles are dedicated to physical security, safety and data centre security. A journal less related to IT and a valuable periodical on security management was the ceased **Assets Protection** (1975-1981) which covered the established topics on security, safety, investigations and security measures and implementations. The journal was not IT biased like its also ceased successor Data Processing &

Communications Security; although it is not published anymore, the back issues could help on highlights for the fundamentals on corporate security. Another ceased journal documented here for research purposes and one of the first journals on security management was the **Australian Security Journal** (1968-1973). The publication contained papers on risk management and security measures mainly focused to retailing and loss prevention with insights on industrial security and occupational safety. The journal had also a strong profile on incident handling and crisis management although no information security was yet considered on that time. The journal was followed by the **Security and Property Protection** (1973-1980) which followed a similar line with a stronger focus on surveillance systems. Although the final or last current issue of this journal is unknown, there are no records of it after 1985; indeed the publisher, the Australian Institute of Commercial and Industrial Security Executives, does not exist anymore and has been followed by the non-publishing association Security Providers Association of Australia Limited based in Sydney.

The **Security Management Bulletin** (1985-2000), retitled later simply as **Security Management**, was another ceased valuable publication on the topic, which was a monthly publication edited during the 1990's by the National Foremen's Institute based in Connecticut, which focused on industrial security and property protection. From some exemplaries obtained, it could not be attested whether this can be considered an academic journal since no information on the editors was found; it can be said though that it does not belong to the regular magazine type. The publication was continued from the late 1990's till 2003 under the title **Security Watch** (1990-2003) with a wider perspective on assets protection, including information and document protection with some highlights on networks, software and other IT infrastructure.

There are some publication recently ceased that can be useful for non strictly actual research and some other which are very close to corporate security but fail on covering important topics. The **Security Insider** (1995-) is a current publication by the Australian Security Industry Association. The periodical is mostly a regular magazine, nevertheless many articles published are written by the academia, especially in the Universities of Sydney, Canberra, the Osaka Institute of Technology and other Australian, Japanese and English schools. The journal-magazine covers most aspects of corporate security with the exception of IT security, nevertheless in the early 2000s the supplement Crime Watch published papers on information and knowledge protection with regard to access control, social engineering and espionage. The biweekly **Corporate Se-**

curity (1981-2008), which from 1981 continued the prior periodical **Protection Management** is not a journal itself but rather a magazine for professionals and scholars. It is mentioned in this work, since this is a kind of periodical that approaches at best the concepts of security management treated in this document. The magazine published by the Business Research Publishing was recently ceased in 2008.

On another area of risk and security publishing are journals that make extensive research either on risk analysis or crisis management topics. Although these are actually side disciplines, it was considered that the documentation of these journals could help on covering the areas of risk and crisis, which are commonly ignored by other publications at least from the deep, scientific and methodological approach that they require. The **International Journal of Risk Assessment and Management** (2000-) is an ongoing peer-reviewed publication, which is not properly related to the wider field of corporate security. It was decided though to document this quarterly given the lack of security literature with focus on scientific or numerical risk assessment, which is a central start point in risk management to execute security measures efficiently, particularly in large corporations. The journal covers many topics on risk from the insurance industry to natural sciences. Many papers are focused though concretely on safety and security as seen from the perspective of this document. A ceased journal was the **International Journal of Risk Security and Crime Prevention** (1996~2005). The bimonthly was published 10 years approximately around 2000. This journal provided a complete perspective on security management topics ranging from safety to security and IT security. The range of public was several public and private institutions with some interest on citizen and government scope, which gave the journal an interesting perspective keeping some distance from pure corporate security. The UK based publisher, Perpetuity Group, is still active and has other publications in book and other media for several security areas. An interesting ongoing periodical is the **IOMA's Security Director's Report** (1993-). This is also not an academic journal but it can be regarded as a monthly newsletter worth to consider published by experts on corporate security active in the field. The New York based Institute of Management & Administration publishes since fifteen years this periodical, in the beginning as an internal bulletin, covering aspects such as disaster, executive protection, crisis management and safety. More recently, the Report focuses on IT topics as well.

The previously reviewed publications compose a set of periodicals that do not quietly fit in a proposed library for security management. As it was seen, these journals lack from certain characteristics such as actuality, editorial review aspects or topic scope. These journals have been though included in a rating schema in Figure 7 similar to the one used for the book counterpart. The section of the table labeled as other titles refers to the journals reviewed previously in this chapter, whereas most significant titles analyzed from sections 4.2.1 to 4.2.7 compose the first group of the table.

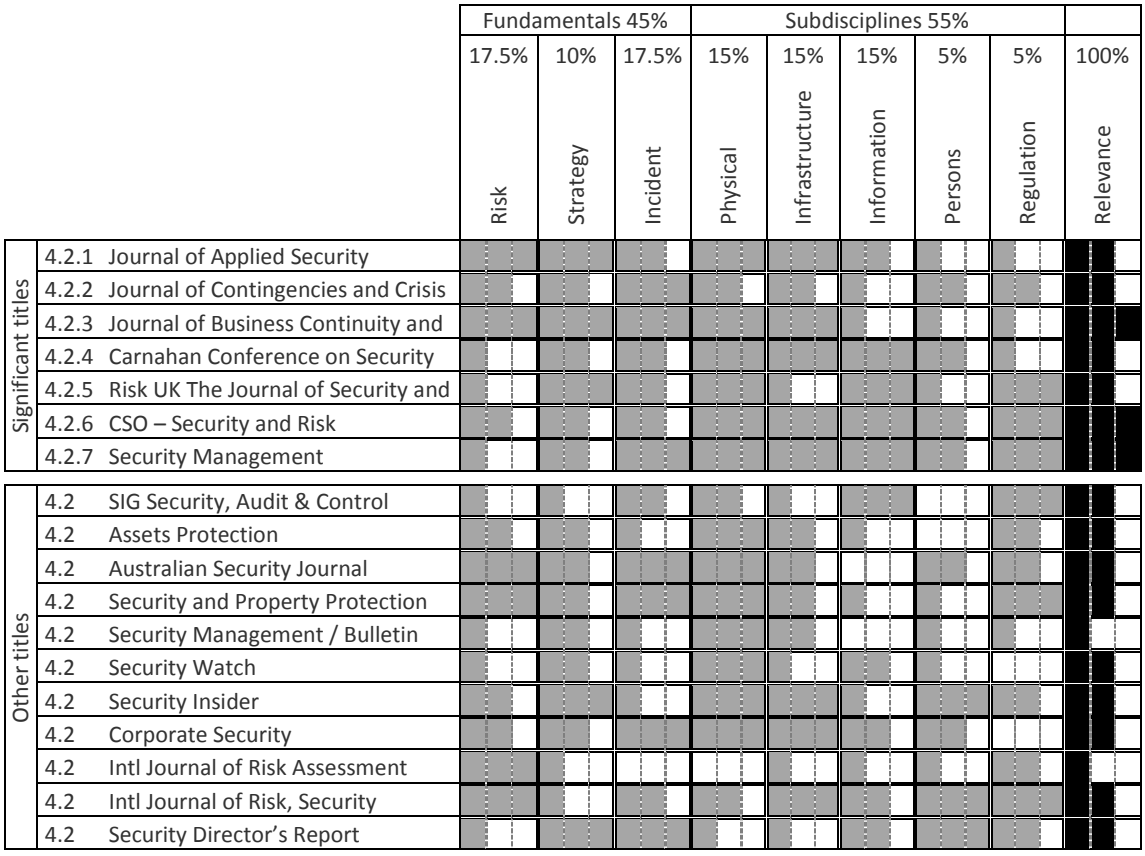


Figure 7 Journals rating

Each journal has eight different categories to which their articles' topics where assigned. For each category a discrete value from 0 to 3 was assigned based on the journal relevance associated with each fundamental topic and subdisciplines, where 0 represents no or very few articles about the topic in question and 3 represents recurrent articles on the same topic in each issue. 1 and 2 represent middle values in-between. The scale from 0 to 3 has been graphically pictured as four grades shaded bricks going respectively from no shading through mid-shadings to full shading states. In order to provide a rating of the journals the same measurement method was used as in the books chapters by assigning relative weights to each topic based on subjective consideration rather than on

a formal numerical method. Academic periodicals can be seen as publications dedicated to the research on fundamentals topics, nonetheless the stress on particular applications in the security field such as physical, infrastructure and information security may also play an important role in journal publishing, since periodicals are characterized by presenting actual research on scientific disciplines and their applications. The weight given to the subdisciplines should be slightly greater than of the fundamentals; percentages of 55 and 45 were respectively chosen. In the fundamentals, the topics of risk analysis and incident handling have a weight of 17.5 percent, greater than the topic of measurement identification and implementation with a 10 percent following the same reasoning as in the books chapter. Accordingly, the subdisciplines of physical, infrastructure and information security share an equal importance of 15 percent weight each, in contrast to the side disciplines of persons safety and security and regulations, standards and liability with only a 5 percent for each both categories. The last column contains the weighted overall relevance of the publication for both the other titles group and the significant titles, which are analyzed in the following sections.

4.2.1. Journal of Applied Security Research

The **Journal of Applied Security Research** (2007-) is a peer-reviewed quarterly published by Taylor & Francis in New York. The publication is relatively new and was created from the collaboration between the University of New York and the Academy of Criminal Justice Sciences. The periodical existed previous to 2007 as a bulletin of the Academy, which concentrated mostly on crime prevention and law from a governmental and educational perspective. After the formalization as an academic journal, the periodical contains a number of security studies not restricted to corporate security but it is able to incorporate a wider public such as institutional, international or private bodies as well having some orientation to public administration.

Most of the articles contained in the Journal present actual research on risk management, experiences on security and safety cases and report incident and catastrophe proceedings of recent studied cases. The areas of investigation comprehend primarily asset protection from a global perspective: on one hand a part of the articles focus on the classical concept of physical and public security paying special attention to industrial loss prevention, criminality and terrorism. On the other hand some articles concentrate on information protection as an asset, which does not mean a bias to computer security but rather a holistic perspective including organizational aspects for mobile security and property

access control to name a few. A remarkable feature, not found on other publication, is the recurring editorial interest on security management education from a university perspective. This leads into some papers discussing the interaction, responsibility and behavior on corporate and public security education.

4.2.2. Journal of Contingencies and Crisis Management

The present research differentiated preventive and reactive aspects of security. The former is a focus extensively treated by many periodicals and books. Nevertheless, the literature fails on joining evenly both passive and response natures of corporate security. The **Journal of Contingencies and Crisis Management** (1993-) is a three monthly periodical which focuses on coping with crisis situations in the public and private sector; an important editorial feature and line of many articles is that research is made on how a crisis state could be prevented, that is through adequate preventive measures and risk management. The journal has been edited and published for fifteen years by Blackwell, Wiley and an academic network of European institutes for crisis research. Some of these institutes belong to universities but other are directly related to national security bodies, which explains that the journal has some tendency for large-scale crisis of public interest, which in the sense of corporate security can be particularly relevant for global players.

This was not the case before 2001; after the events in New York, the Journal presents many articles related with terrorism-related contingencies, coping with media and reputation in international contexts and the role of IT security as backbone of contemporary organizations. In this sense the articles can be categorized firstly as public and global player crisis organization and recovery, secondly threat analysis and scenarios faced by public and private bodies and lastly preventive measures in the level of physical security and infrastructure safety. Current events are covered by the journal with major events having certain editorial priority, since it can be attested that some articles dates correspond with infamous incidents occurrence, which provides to security officers with a scientific information source about implications for the public and private sectors out of the popular media highlighting.

4.2.3. Journal of Business Continuity and Risk Management

The **International Journal of Business Continuity and Risk Management** (2009-) is a new periodical released last year. So far, there is not too much material to analyze but from editorials and the articles published for the first vo-

lume so far, it seems that the journal fits the topics for corporate security in its preventive and reactive aspects. The quarterly published by Inderscience in Milton Keynes, UK is independent from any particular organization; the editorial board is composed by almost twenty members of several European, U.S. and Japanese public and private institutions. The range of topics is risk management applied to enterprise and public environments. In this sense, the journal focuses on risk management methodology research not only applied to operational risks but also some topics of financial risks relevant to corporate security.

Reactive aspects of corporate security are well covered by business continuity and crisis management. In this respect, contingencies are studied and described in their planning, testing and developing aspects regarding the crisis coordination internally and with external parties. For both contingency and threat assessment fields, the journal pays attention not only in methodology research but also in tools and software to handle risk and continuity plans. Perhaps due to the fact that many board members come from the operation research area, the journal accents the importance of infrastructure security and logistics for corporate and public resiliency. Critical infrastructure such as power networks, transport, goods supply and communications are studied at national and corporate levels. It is thus expected that homeland and border security have some weight among other infrastructure topics. IT security is treated as part of communications in private and public environments, for which networks, data security and computer security present certain weight too. Physical security in the form of property protection is handled in connection with information security for access control and social engineering among others.

4.2.4. Carnahan Conference on Security Technology

The Carnahan is the longest running academic conference of any type. Organized by the IEEE the conference primarily covers mostly technological aspects of security, nevertheless the published annual papers are found to be of angular importance for the whole of corporate and public security since they represent the technical baseline of any risk and continuity organization in the interdisciplinary area of security management. Compared to regular conference collections, the **Proceedings of the Carnahan Conference on Security Technology** (1982-) can be considered as having similar academic journal quality, since it is widely known the thorough process by which both presentations and papers are scanned and peer-reviewed.

The topics of papers can be grouped in three categories, namely property protection, homeland and information security. Traditional security has been the backbone of the papers since the 1950's. In this field, about a third of the articles found in the proceeding have to do with the technological state of the art for physical access control and surveillance among others. As theoretical aspects, the proceedings present mainly research on optimization problems on security such as monitoring and identification. Since two decades or more, the Conference has been shaped by many presentations on information security. In this field, the proceedings present virtually all the range of communications and informatics security research from the mathematical aspects, through transmission and media aspects to the use secure computer infrastructure. Eventually the proceedings publish some links to risk analysis linked to best and optimal solution problems but in general, the conference does not focus on risk assessment topics, at least not on quantitative methodologies. Reactive aspects of security are not seen from the crisis management perspective but on business continuity and infrastructures resiliency, nonetheless typically the conference provides big-scenario business cases, which give a picture of contingency planning and the role of security technology on coping with crises in complex environments such as the oil, aviation and bank industries.

4.2.5. Risk UK, the Journal of Security and Loss Prevention

Besides English speaking journals, there is a considerable set of publications of other type of periodicals related with security management. This supply ranges from renowned blogs and newsletter such as Bruce Schneier's Crypto-Gram, free printed monthly magazines strongly focused to the security market, as well as popular magazines such as those researched for the German-speaking world at the end of this chapter. The following three sections record some non peer-reviewed English speaking popular magazines for the sake of documenting adequate literature for security managers. These cannot be classified as academic journals; nonetheless, their content and quality can in fact be compared to the journals presented previously.

Risk UK (2003-) is a monthly magazine published by Pro-Activ in Kent since about 8 years. Pro-active is not a peer review based editorial, nevertheless Risk UK and other security related publications from the editorial seem to provide accurate information about the security industry whereas some articles try to provide the state of the art on security research by covering academia and conference developments around the world. As the publication title might imply some articles picture the security industry within the United Kingdom, which

actually does not seem to allocate the magazine on a national level. The greater part of the articles actually apply to any kind of organization, and only the security news section and the valuable advertising are actually tied to the local industry.

The articles of the magazine can be classified firstly as belonging to physical security in the sense of property protection and loss prevention. In this context, the authors focus on technologies and methodologies implemented in private and public infrastructure. Also towards physical security, the magazine tries to attract general public attention by reporting major events on public security such as terrorism or security efforts taken by the government. On other category, the periodical focuses on IT security, not technically, such as reports on data protection and IT infrastructure availability. A common perception of the authors is that corporate security is to prevent criminality either on the lost prevention level or hacking activities, in this sense the magazine does give some value to risk analysis but leaves somehow apart infrastructure security as part of operational resiliency and crisis management topic are rather marginal.

4.2.6. CSO – Security and Risk

CSO (1999-) is a magazine oriented to security and information security managers edited monthly by IDG in Connecticut. IDG publishes since 6 years the periodical among other computer publications. In fact, this is the first magazine published from the group that does not cope merely with informatics; nevertheless, the editorial board is composed by former or active Chief Security Officers and other scholars from US universities. The articles is focused to a more executive public than oriented to academic research, nonetheless the review and quality of the articles follow certain uniformity in content and form which suggests an adequate editorial process. The line of the magazine is balanced between physical, IT security, risk and business continuity in public and private scenarios.

Physical security and risk management is the main line of the articles, in this context there is an important focus of the articles on data protection from network security and mobile security for e.g. road warriors, i.e. information security, data leakage to name a few. Physical security derives also from IT topics, but in the last years, most of the articles barely mention information protection when studying access control, identification methodologies and loss prevention, which is favorable for a wider public interested on classical safety topics. For reactive topics of security the magazine is well positioned in infrastructure

security and business continuity topics, there are even some articles focusing on investigations and forensics, but fails on coping with crisis management and crisis organization. An important feature is that this is one of the few media founded that publishes topics on supply chain and other logistics and operation research topics as part of business continuity, which is particularly important for the global economy and markets.

4.2.7. Security Management

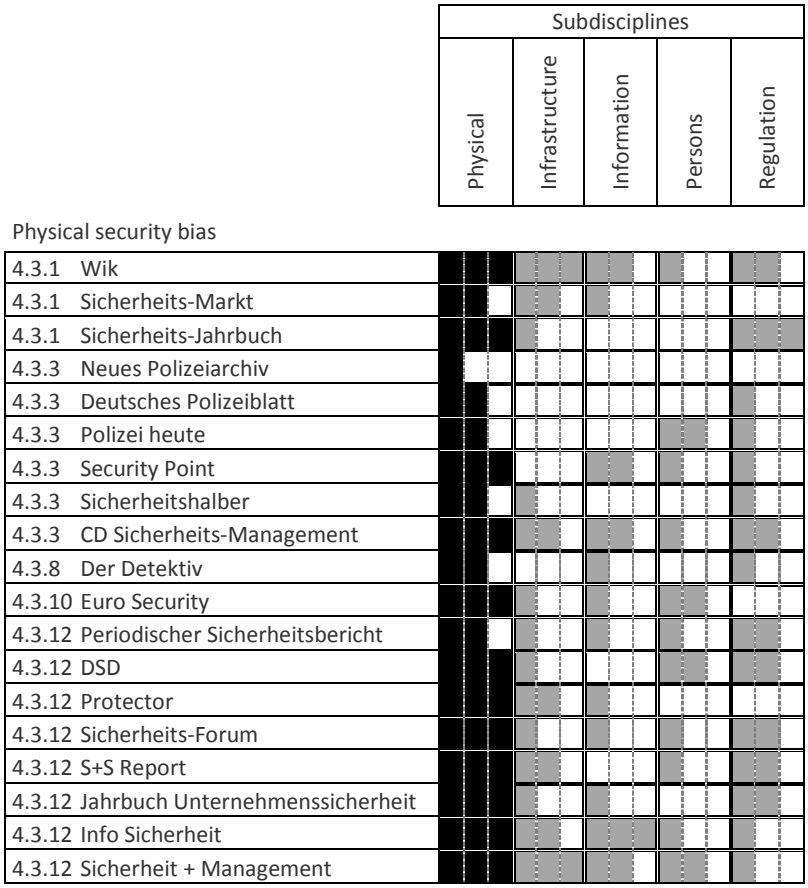
ASIS International, formerly American Society for Industrial Security, publishes since 1972 the monthly periodical **Security Management** (1972-). It couldn't be attested which kind of publication was the periodical prior to 2000, since only indexes for the volumes could be obtained, but recent exemplaries show that is a peer reviewed type publication with some commercial focus aiming US and European industries. The organization is a professional's organization with 200 chapters dedicated to all topics of security management. The magazine is well known by publishing security research standard practices later adopted by the American National Standards Institutes. Nonetheless, in general the periodical lacks a scholarly tendency, which makes it suitable for a wider public aimed to security professionals.

The range of topics has gradually changed since the beginning. Being originally a publication oriented to physical security and property protection, the magazine has evolved through the years presenting since the last few years a great interest on information technologies and data protection. Nevertheless the main focus stays being infrastructure security whether IT or not and security protection against criminal efforts on private organization as well as for public bodies. The topics could be then classified on classical security topics such as access control, surveillance and security technology together with IT topics. Risk management is not a spotlight of the magazine, nevertheless several issues on terrorism, theft and disasters get commonly tied with articles on threat analysis on different scenarios. The publication contains some contingency planning topics and crisis organization mainly related or reported on known current incidents or scandals. A special remark of the periodical is the stress on legislative and compliance matter, mostly US regulations.

4.3. Magazines analysis

The magazine research section in last chapter described the resources, procedure and results of periodicals survey for the sprachraum through the Zeit-

schriftendatenbank. A number of titles greater than the magazines surveyed here were physically fetched but some of them were discarded as it was shown in the summary table in that chapter section. It was determined that the set of 51 periodicals presented here may fit into the security subdisciplines structure established in this work for the fields of physical security, infrastructure resilience, information security and persons safety and security. At this point, it is important to comment that the fifth subdivision of regulations, standards and liabilities, taken into account for the books and journals ratings is not considered for the magazines analysis. Although a regulations' grading is indeed given for magazines, there is no subset of recommended magazines for the particular subject of regulations, since this topic is something a regularly accompanying feature in greater or lesser degree to all publications. That is, there is no scope for such a security management law and no grouping of security management law magazines, and in fact, no sprachraum magazines are available on this particular subject alone.



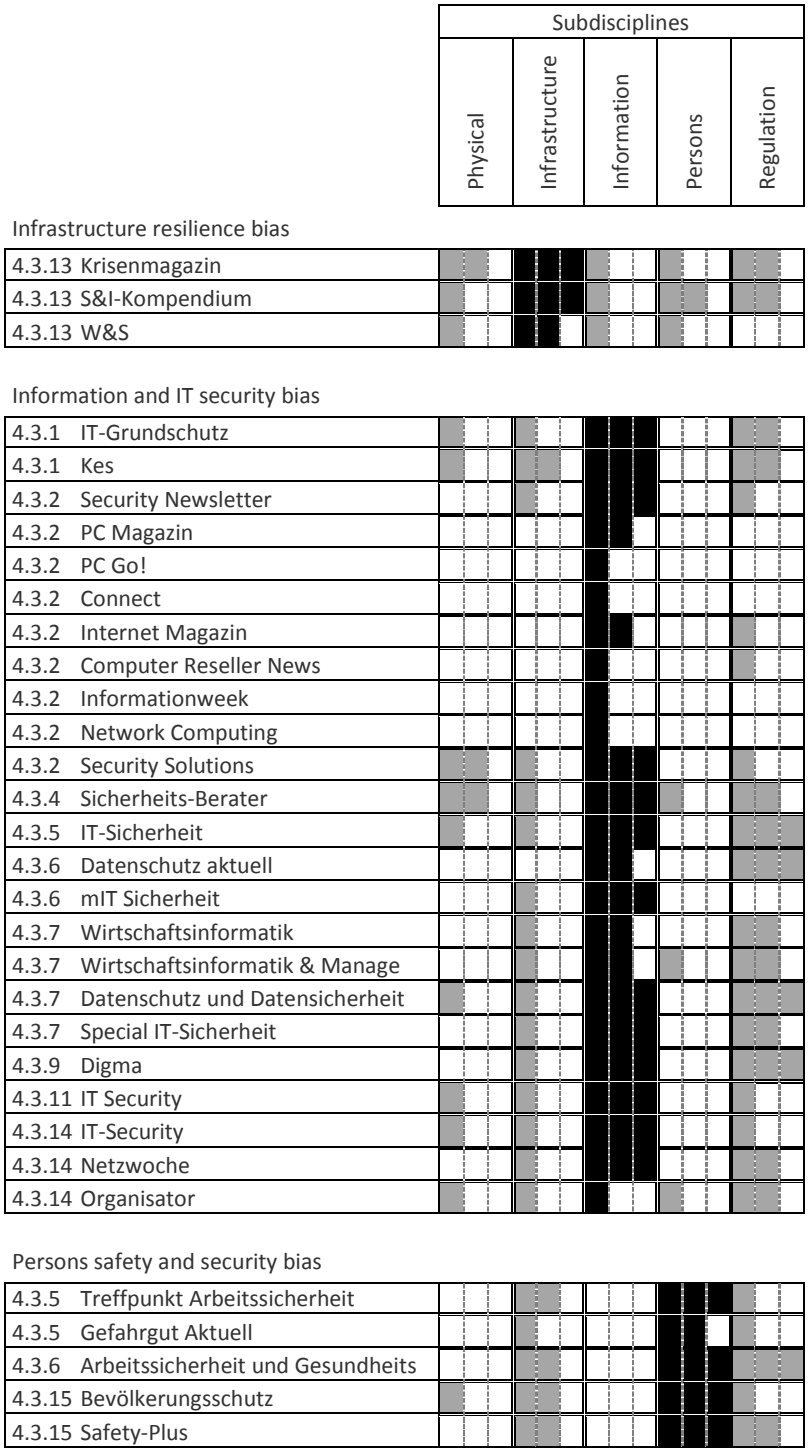


Figure 8 Journals rating sorted by topic

Following the scheme applied in the books and journal analyses, it was first intended to review each magazine independently as they were appearing and with no connection between them. It was nevertheless soon realized that editorials commonly publish more than one periodical on safety, security and related topics for instance –as well as on any branch namely medicine, social sciences and the like–, and therefore an editorial based grouping is also present through

the following sections. This naturally is also a characteristic of books and journals publishers; nevertheless, an editorial based classification was not possible there, since the interdisciplinary principle of security management produces a quite concrete and specialized focus of security management. Therefore the books and journals supply in this field becomes limited within the editorial and the market in general, whose demand is in turn covered by the more general security subdisciplines publications. Other than the structure depicted in the table above, the eleven following sections correspond to the editorials presented more than one security publication. One-off periodicals or one-off editorials are in turn classified in the four remaining four section from 4.3.12 to 4.3.15 corresponding to physical, infrastructure, information and persons subdivisions. All periodicals were afterwards brought back to the table depicted in Figure 8 in order to provide a general overview according to their classification and bias. The figure is composed by four subtables matching the mentioned subdisciplines. The periodicals were allocated on one of the four subtables based on the bias that the regular articles showed. The darker shading for each of the four columns does not represent an overall rating, like it was given in the books and journals researches, but it is simply an aid indicating why was a particular magazine allocated to a determined subdiscipline; the presence of secondary topics in the same magazine are thus represented by the normal gray shading. No subtable was created for regulations topics and therefore the regulation column neither presents darker shading following the last considerations of the previous paragraph. The vertical columns present the grading or rating given on every topic based on the usual bottom-top 0-1-2-3 scale, where 0 or lack of shaded squares means no connection with the topic and 3 or full shade represents a strong presence of one or several subjects on that topic. An overall rating column would make no sense, since no holistic security approach is being scoped, but a subdiscipline research is the purpose here; moreover, no weighted sum could be performed since no quotients can be assigned to any of the four subdisciplines, given that, for the magazine research, they represent heterogeneous elements.

4.3.1. Secumedia

Secumedia is an editorial based in Gau-Algesheim publishing several printed and electronic media since almost three decades. The editorial sponsors and is strategically present in several security fairs and conferences, and hence it is well positioned in the security literature industry and widely known by security professionals in German-speaking countries. Besides magazines, the editorial

has a small library of books on several topics of security management including IT security, conflict management and data protection. Other media published by the editorial are training and learning material useful for companies engaged in security awareness programs for instance. Some of this material is published in cooperation with Springer's imprints. The editorial has three periodicals, all relevant for security managers, which are described as follows.

Wik (1987-) is the longest running magazine of Secumedia and one of the few security management periodicals keeping being published for over three decades. The editors and columnist of the magazine are in general well known in the security market, some of them coming from the academia or the industry. Indeed this publication is classified as journal in some sources, although no reference to the editorial review process could be found. Although the magazine is referred as a security management magazine, most of its content has a bias to physical security and is not particularly strong in topics such as information security, safety or crisis management. Nevertheless, the authors do show integral security concepts in all aspects of security in the modern industry. Regular topics of the magazine include access control, locking technologies, identification technologies, transmissions technology, facility management, property protection including surveillance and perimeter security, security consulting, training and education, information security and some topics related to safety besides fire protection which is treated commonly by many columnists through the about hundred pages of the bimonthly. Wik is also characterized by in-depth criminality analysis as background for a security management, this is also attested in some occasional supplements accompanying the issues such as Special Sicherheitsdienstleistung, Special Zutrittkskontrolle and CCTV and the more regular **Sicherheits-Markt** (1993-), which can be ordered separately for further information on physical and infrastructure security as well as some non-IT information security topics. Another periodical publication of Secumedia focusing physical security topics is the biannual **Sicherheits-Jahrbuch** (1987-). Although the publication is indeed a periodical work, it cannot be considered a magazine of the characteristics the present research surveys, nevertheless its importance in the security technology makes necessary to mention it as a first hand resource for professionals and academics in the security field. The periodical appears every two years with 300 hundred pages since 1990 and rather than an analysis publication, it can be regarded as a reference handbook and lexicon for security. The book features three key sections in this sense namely a terminology with thousands of definition entries, security professions, occupations and positions in corporate security structure and a directory of federal offices,

associations and institutions in Germany and Switzerland in the security field as well as a collection of regulation and laws relevant for security officers. The first part of the book is an introduction to the security situation in Germany and Switzerland, which can be considered as the only chapter of the book containing analysis material. The publication is aimed to security officers involved in physical security, loss prevention, surveillance and property protection for instance, lacking totally of interactions with other disciplines such as information security and occupational safety.

A periodical widely aimed to the information technologies and information security is **IT-Grundschutz** (2006-). The publication lies between the category of a monthly newsletter and magazine given its compact size. This publication fills in some way the gap between the other two Secumedia periodical concentrating on IT topics from both technical and organizational points of view in a compact form as well as legal aspects of information technologies in German companies. IT-Grundschutz, a term for baseline protection, contains monthly articles and reports aimed to information and information security officers from a top-level management perspective. The authors and the editorial board of this monthly often publish in peer-reviewed journals and some are recognized in the academic domain. The columns can be roughly classified in informatics, managerial and law related types, where regular topics refer to data protection, ICT infrastructure security, risk analysis of corporate networks and internet, business continuity, awareness and audits. Important highlights of the magazine are also information on international and European IT certifications, reports on software and hardware security tool as well as legislation and regulation news with focus on German-based companies. Compared to other IT security magazines, IT-Grundschutz is clearly shaped by a business informatics approach, which makes it suitable for organization pursuing integral processes based on secure IT infrastructures.

Another periodical referred as journal, but following the same characteristics of Wik in terms of authors' profile, advertisement and other features, is **Kes** (1985-). Kes is also an IT oriented magazine appearing bimonthly with about a hundred pages since fifteen years. In contrast to IT-Grundschutz, Kes contains more detailed analyses on information security, giving to it a more appropriated scope for all kind of IT professionals, from technical positions to decision makers. The authors are also recognized in the security literature or well occupy positions in recognized public and private organizations. The range of topics is quite wide. Typical articles can be classified in trends on network secu-

rity, methodologies and technology on physical and logical access controls, analyses in IT threats such as viruses and protection technology, there also regular studies in risk management and risk analysis for company-wide IT based infrastructures, security planning as well on reactive processes with focus on business recovery and crisis management. Cryptography is also a regularly present topic with articles on PKI, algorithms trends and digital signatures. Similar to the other Secumedia periodicals, Kes provide reports on certifications institutions, compliance and audits. There have been some special editions of the magazine as for example for the topic of mobile security that treat integral analyses on current mobility topics. The Kes contains too the regular BSI-Forum, which is a kind of press organ of the Federal Office for Information Security containing reports and statements of the German government with public character as well as certification and other information emitted by the agency.

4.3.2. Weka

The Munich based Weka Corporate Group concentrates several companies related to media publishing and other communication branches. The subsidiary Weka Media has holdings of over 600 different titles on topics such as safety, fire protection, information privacy, IT security, quality management and environmental safety among many other industrial and economics topics non related to security management such as purchasing and logistics, architecture, business and public administration. The publications are mostly technical literature, reference handbooks, manuals and looseleaf services with few issues in the form of actual hardcover books, but no current periodicals other than looseleaf services are published by this editorial. There used to appear though for over 10 years until past November a **Security Newsletter** (1997-) concentrating on several topics of IT security specializing in computer networks, data backup and confidentiality as well as on informatics attacks. This biweekly has disappeared a couple of times already and been replaced by an online edition of the newsletter. As it have happened before it might be possible that the electronic newsletter gets relaunched as a printed edition eventually. Another subsidiary, the Weka Media Publishing –not to be confounded with the previously mentioned–, edits monthly popular magazines in software, hardware and other technological fields such as photography and audio techniques. Titles such as **PC Magazin** (1998-), **Pc Go!** (1993-), **Connect** (2010-) and **Internet Magazin** (1996-) do not concentrate actually on IT-security or other corporate security topics, but they do repeatedly present several articles with security updates and

news in viruses, known attacks, vulnerabilities and IT security products, which might be of the interest of academics and professionals wanting quick current overviews on these and other general topics on IT and mobile technologies.

CMP-Weka is another company that publishes four magazines related to computer technology. According to research in libraries, it is concluded that all magazines have existed sporadically for many years either as stand-alone issues, digital media and supplements of other publications or else their irregularity is due to market positioning difficulties. As of the time of this research, the only regular printed publication is the **Computer Reseller News** (1998-). This and other two irregular digital and sometimes printed publications –**Informationweek** (1997-2010) and **Network Computing** (1998)– are registered as having a supplement called Security Solutions, IT, Konzepte, Strategien und Lösungen zur Unternehmenssicherheit. The supplement can be obtained currently through the biweekly Computer Reseller News which in turn can be subscribed free of charge by companies in the IT and security branch. The periodicity of Security Solutions as supplement of Computer Reseller News is uncertain. In contrast to the IT editorial line of CMP-Weka, Security Solutions contains other topics related to physical security, although it is indeed not a corporate security publication as it claims. The about 30 pages supplement do treat property protection, IT and business continuity topics. They are though often linked to new technologies such as internet based surveillance and network lock keys with RFID bows (transponder keys) to name a few. On the other hand, at least half of the articles often relate to pure IT security topics such as email security, mobile security, and access control both physical and network.

4.3.3. Boorberg

The editorial Richard Boorberg with the DFS GmbH –Der Fachverlag für Sicherheit– publishes several magazines related with a focus on criminality. Most of the magazines concentrate on public administration, law and order. In this former topic, there is a group of three magazines that, although oriented to states and municipal polices, can interest to physical security and investigation corporate officers. The **Neues Polizeiarchiv** (1952-), **Deutsches Polizeiblatt** (1983-) and **Polizei heute** (1994-) treat in general several topics related with law enforcement, improve civil order and protect public and private property but each keep unique features. Of the three publications, perhaps the less attractive to the security manager might be the Neues Polizeiarchiv. This monthly mainly contains criminal cases and legal procedures related with public law enforcement and therefore not quite relevant for a corporate security environment.

The bimonthly Deutsche Polizeiblatt has also some scope in law and penalties but includes also many articles related to study the nature and control the criminal behavior in public and private sectors, which is relevant for investigations security officers to assess risk and find measure aimed to mitigate possible threats of external and internal offenders. The latter publication, Polizei heute, shares the common characteristic of the three publications of being partially oriented to and having a close relation to police training; nevertheless, this bimonthly pays special attention to the equipment used by police officers and in surveillance tasks, which can give some hints in the private property protection area.

A second group of three magazines, closer to the field of security management, constitutes a set of Boorberg publications for corporate security in the widest sense including logistics and the security industry itself. **Security Point** (1999-) is a compact bimonthly oriented to security officers, plant security directors and IT directors. The regular topics presented in the publication have to do with surveillance and property protection with some insights in IT security. Most of the articles are related to physical security and treat topics such as surveillance, access control, preventive measures, alarm management, theft and vandalism. The magazine aims to keep up-to-date reports on security technology video technology and access control devices. Some other security related topics on the reactive field are treated such as kidnapping and hostage taking. Articles related to information security do not cope with technicalities of networks and software but instead depict general preventive measures and emphasize the importance of reliable information and communication system such as telephone and mobile encoding. Another magazine related to corporate security is **Sicherheitshalber** (2003-), which focus mostly to security in logistics, production and retailers. Some of the topics such as property protection and surveillance are already treated by Security Point. Sicherheitshalber's main focus is the supply chain with a bigger interest in retailer and wholesaler going in to topics such as loss prevention, RFID for consumer and logistics application, cash management and video surveillance. Two other prevalent topics are logistics and production. The former is focused also in physical security topics in e.g. warehousing and shipping environments dealing with topics such as access control, locking mechanisms, some safety topics and haulage security. Save from the classical security topics, the articles almost not cope with infrastructure resilience topics such as service level agreements in the logistics and power or raw material supply to name a few.

The third magazine in this group is the **CD Sicherheits-Management** (1994-), a bimonthly appearing since fifteen years. The magazine is not a peer-reviewed and the public is more likely to be aimed to company managers in the industry market rather than scholarly researchers. Nonetheless, the quality of the articles could be attested by reviewing several exemplaries and, accordingly, a remark of the magazine is that almost all articles published are written by security managers from prestigious companies and not by regular columnist as it happens in other popular publications. The magazine focuses on all aspects of corporate security with some tendency for shielding corporate operations from criminal efforts.

The magazine mostly report experiences in industrial environments on property protection, IT security and compliance, among other teams, which give some hints on how to deal ad hoc security problems. Like many specialized magazines, a great part of the publication serves as a communication link between security professionals where conference calendars, literature highlights and security news have an important weight. Less focused on risk analysis and crisis management the magazine tries to cover solution to classical or new threats in areas such as physical security and IT for instance. The articles discuss which protective measures apply for several scenarios and present related technology to accomplish them as well.

4.3.4. TeMedia

The Von zur Mühlen group is a company dedicated mainly to consulting and some publications on security. The group is composed by two consulting companies on the field of security management and data centre planning. Another company is Simedia, which provides support in congresses and trainings related to security management and also publishes conference proceedings of some congresses it has been involved with. The last Von zur Mühlen company is Temedia, which seems exclusively dedicated to the one magazine reported here. In fact, no other Simedia and Temedia publications were found besides conference proceedings and the biweekly Sicherheit-Berater. Books' authors related to this group, such as the Boorberg's Sicherheits-Management by Rainer von zur Mühlen cited in section 4.1, do not publish in these editorials.

Sicherheits-Berater (1974-) is a periodical published two times a month since 1974 by the Bonn based Von zur Mühlen Gruppe, dedicated mainly to IT systems and other topics of corporate security. The magazine itself contains a wider spectrum of security topics such as infrastructure security, data protec-

tion, compliance, data center protection. There is no much further information about the editorial board available but most of the articles contain personal data of the article authors, from which it can be seen that many of them are active in the security industry but many other are rather columnist reporting about several topics in the security area.

The articles can be grouped on most of the disciplines of corporate security such as physical security, safety, IT security, compliance and auditing. In the last five years, an increase of IT related articles is plausible. Indeed the magazine slowly gets shaped to purely IT topics, where all the others topics seem to be present just as side disciplines. This is for instance in the case of access control, fire protection and compliance, where the articles point out the importance of protecting information and IT infrastructure as a focal point. In this regard, it is a little uncertain on whether classifying this periodical in the IT area or the broader corporate security field, at least based on recent volumes, which was not always the case in past years.

4.3.5. Hüthig Jehle Rehm

Hüthig Jehle Rehm is a Heidelberg based editorial group comprising 13 brands with cross-scopes. The company itself belongs to the same group of the Süddeutsche Zeitung. In contrast to other groups the Hüthig Jehle Rehm's magazines are not edited by different subsidiaries but marketed as different brand lines, which in turn each of them publishes several magazines and therefore bibliographic records are misleading, since it is actually Hüthig Jehle Rehm the unique editor. Two out of the twelve imprints belong in certain degree to the scope of security managers in particular for disciplines of safety and IT. Ecomed Sicherheit is one of these imprints that specialize on safety topics; this brand itself is a spinoff of Ecomed Medizin that deals with medicine and safety topics as well. Ecomed Sicherheit regularly mostly books and other types of non-periodical publications. The only two periodical publications of this imprint are Treffpunkt Arbeitssicherheit and Gefahrgut Aktuell. **Treffpunkt Arbeitssicherheit** (n.a. - ongoing) is a bimonthly wall newspaper, that although is not a magazine it represents a useful tool for occupational health and safety officers to create a safety culture within a company, either in office or industrial environments. **Gefahrgut Aktuell** (1992-) is also a safety publication concentrating on certain industrial branches. The biweekly magazine is a newsletter containing articles and reports on hazardous material in several contexts such as haulage, chemical and pharmaceutical industries.

Hüthig Jehle Rehm also publishes since over 10 years under the imprint Datacontext a bimonthly entitled **IT-Sicherheit** (1997-) with several scopes in not only the software and networks fields but in general to all the areas of information security. IT-Sicherheit contains articles and reports on IT security technologies, and their several characteristics such as performance features, system criteria and the application of IT technologies in the security context. The magazine concentrates not only in the technical aspects, but also in organizational features, economical and financial aspects of IT security as well as in legal considerations regarding to corporate governance and IT security. An important feature of the magazine is the continuous interest of the columnist on the implications, and obligations of regulations in the IT infrastructure such as the German Gesetz zur Kontrolle und Transparenz im Unternehmensbereich, Basel II of the banking branch Basel Accords, and the Sarbanes-Oxley Act. The magazine has a clear orientation to German, Austrian and Swiss companies, giving key information for CIOs, CISOs, CSOs and academics coping with the topics of IT security and data protection in general. Given the interactions of IT with other security technologies, the magazine does not only provide computer related topics but has many articles that reach the wider scope of corporate security such as breakdown in IT and power supply systems, business continuity, mobile security, access controls including biometric technologies and video surveillance, security service providers, cloud computing and data protection, security and data protection in the banking industry, industrial espionage, content security focusing on recent attacks reports.

4.3.6. Verlag für die Deutsche Wirtschaft

The editorial Verlag für die Deutsche Wirtschaft is a relative young company with no clear focus on a specific branch but rather publishes several publications, most of them periodicals but also books and electronic media. Regular topics of the editorial are industry trends, office organization, consumer hardware and software, how-to publications and law and finance for physical and legal entities. The company publishes three periodicals related to corporate security topics, namely in the fields of occupational health, data protection and IT security. **Arbeitssicherheit und Gesundheitsschutz im Betrieb aktuell** (2004-) is a concise publication dedicated mainly to occupational health and safety topics. The magazine is mostly dedicated to safety or security officers with certain production context scope. The compact monthly reports on the new trends at German and European level on occupational health and highlights recommendations about recent developments on legislations and regulations for compa-

nies in this field. Many columnists aim continually to illustrate audits and testing schemes to which German companies are subject. In this sense, a feature of the magazine is the preparation, checklisting and methodologies for security and safety officers to comply with current industrial regulations in this topic.

The second periodical of the editorial related to security management is **Datenschutz aktuell**.(2004-) In the same compact format as the first publication, this monthly periodical reports the actual trends of data protection relevant to information and security officers. The magazine concentrates mostly on data protection according to common definitions in the German-speaking countries, which is the obligation of corporations to protect personal information of third persons. The magazine thus does not aim to provide information on know-how and electronic data protection. The articles provide though useful reports and points of view on developments and implications of regulations such as the German Bundesdatenschutzgesetz and give recommendations on how to implement data protection policies and standards.

The last periodical published by the Verlag für die Deutsche Wirtschaft is **MIT Sicherheit** (2004-). This monthly follows the same eight-page format of the other two newsletters described previously providing reports and trends in IT security. The articles are mainly dedicated to IT administrators, information and security officers. The magazine can be considered mainly as a newsletter reporting on recent IT security threats, vulnerabilities in major operating systems and programs and a guideline for increasing the IT infrastructure security in companies. The articles in general do not focus on organizational features of information security but it is very technology oriented. An important characteristic of this and the other magazines of the editorial is that all publications are free of advertisements, which is relevant given that the compact format of the publications could seem to rest relevance on their respective fields. It could though be attested that the amount of articles correspond to regular magazines highly oriented to marketing security products and services.

4.3.7. Springer's Gabler

Springer is a media corporation with thousands of publications in the form of books, electronic media, journals and magazines among others in Europe, America and Asia. Through over thirty editorials and imprints, Springer publishes a wide range of periodicals in most areas of natural and social sciences, engineering, economics, production industry and non scientific consumer magazines to name a few. Gabler Verlag is one of these editorials with long expe-

rience in German-speaking countries that has being acquired recently by Springer. Among the Springer's editorials, Gabler is one of the few that incorporates several branches in a single editorial board combining economics and technique fields of interest. The editorial publishes over twenty periodicals ranging from the banking and financial branch, controlling, sales and informatics. Gabler has two magazines on business informatics with some insights in security management, more concretely in IT security and data protection. **Wirtschaftsinformatik** (1990-) and **Wirtschaftsinformatik & Management** (2009-) are these two bimonthlies with a similar scope. Wirtschaftsinformatik and Wirtschaftsinformatik & Management focus on typical business and production topics in particular authors tend to focus on industry technologies. One of the important features of the magazines is that many articles give insights in business strategies and management trends focusing on the interfaces with information technologies and several business and production areas such as logistics, controlling, management and in some degree infrastructure resilience. On the field of security management, both magazines contain regularly articles on IT security and data protection. In this sense, the authors give information, analyses and reports on access control methodologies, technologies and data confidentiality and availability. Very often, this kind of articles is accompanied with IT security concepts such as redundancy and backup. On the level of data protection, the articles tend to maintain up-to-date information relating the implications of regulations and legislations on personal privacy, handling third party information and corporate governance in the sense of transparency and other regulatory and compliance topics.

A periodical more focused on the matter of information security is the **Datenschutz und Datensicherheit DuD** (1983-). The magazine has existed for over thirty years; in a time prior to the growth of the IT industry the publication aimed the legal and organizational aspects of information handling. Nowadays the magazine copes with both aspects, the technological and legislative fields of information handling. This Gabler's monthly is widely recognized in German speaking countries as the authority magazine in data protection and information security being often cited by many scholars and specialized literature. The background of authors present also a high profile coming from the academic world, the IT and law areas as well as occupying important positions within the government and key companies in these fields. As it was mentioned, articles can be roughly allocated in the technological and legislative domains, where the actuality and current relevance could be attested in relation to major events related in the media as for instance data leaking in companies, employees sur-

veillance scandals and implications of laws on citizens privacy to name a few in German-speaking countries. In this sense typical articles for IT topics are data protection, secure software, penetration tests, person identification, eGovernment, cryptography applications, IT security standards, business continuity, awareness, traffic protocoling, security application in telematic environments, identification cards and secure modules, identity management, network architectures e.g. software oriented, RFID technology. Whereas in the regulatory field typical topics of interest are data privacy, liabilities in government application such as eVoting and health card, service level agreements, obligations for companies handling third person data, bills on data retention and storage, data protection legislation, reports on information legislation offenses, reports on whistleblower and data leakage scandals as well as digital certificates and signatures related to legal matters. Before closing, it is worth two mention a supplement related with the DuD magazine appearing irregularly in Gabler's Versicherungsmagazin (2000-) and Bankmagazin (1993-). In general, the **Special IT-Sicherheit** is a regular IT-Security newsletter, although its feature lies on being very closely applied to the financial industry. The supplement appears at least two times a year covering topics such as IT failures, critical system under internet attacks, awareness and data protection as well as customer service quality.

4.3.8. Cornelia Haupt

Cornelia Haupt's **Der Detektiv** (2002-) is the sole periodical of this editor, who publishing as physical person in Vienna runs other tasks such as a private investigations consulting firm and activities with several European associations. In the sprachraum, there are a handful of magazines on the field of private investigations, being Der Detektiv the only one specializing in corporate investigations, i.e. as a company function and not focusing in the private clients branch, and other topics close to security management. The magazine is a quarterly published since 2002 counting with the editorial cooperation of the Österreichischer Detektiv-Verband, where some magazine's columnists are also linked to.

The articles can be classified in a couple of categories such as property protection, corporate investigations, security technology, data protection, secret service and industrial espionage. Typical topics cover embezzlement, sabotage, economic crimes, espionage technology, undercover employees, surveillance, access control, data protection, investigations industry, information security, reports on investigations and security news, data leakage, employee internet use, legislations and regulation regarding information and corporate criminali-

ty, cooperation with government agencies, gadgets and espionage tools as well as VIP security protections among other topics. Besides the articles, the magazine contains interesting sections such as events, consumer devices and specialized and fiction literature reviews.

4.3.9. Schulthess

Schulthess is a Zürich based editorial publishing several types of media in English, French and German. The company is focused to cover all legal concerns of organizations in the sprachraum and francophone European countries. The editorial publishes about twenty different periodicals mostly bimonthlies and quarterlies on commercial law, financial legislation, labor law. Another set of periodicals deal with public law regulations such as laws of succession, traffic legislation and private property to name a few. The structure of the company is composed by a common editorial board, to which partially belong professors of main Swiss institutions such as the universities in Bern, Zürich and Neuchâtel. Every periodical in turn has an own editorial responsible composed of two or more persons from the academia as well. This structure seems to improve the quality of the publications although the periodicals in general are not edited by a peer-review process such as in academic journals.

In relation to security management, Schulthess publishes a quarterly called **Digma** (2001-) since about ten years roughly. The authors and the editorial board are linked to the Swiss government and universities, many of them hold positions as privacy officers, data protection officers in both private and public Swiss institutions as well having key positions in Swiss and French universities and fachhochschules. The scope of interest of the magazine is the legal and technical developments regarding the current deployment of information and communication technologies in the public and private domains, in particular related to the matters of privacy and security. At a first glance, it might seem that the magazine has a strong legislative interest. This is indeed true in some issues of the magazines, in particular after some bill or law has entered into force such as Europe-wide data protection regulations, or German, Swiss and Austrian laws regarding information privacy. In general, technical as much as legislative topics occupy the main interest of the magazine. Nonetheless, articles related with IT are not studied from a technical point of view, but from a perspective of risk analysis and general implication in the organizational and legislative subjects. Typical topics are privacy, reports on information related legislation, records management, data protection, digital signatures and certif-

icates, private and public law on information handling, surveillance, and data storage as well as legal aspects of the Internet.

4.3.10. SEC!

SEC! The Publishing House is an independent editor based in Munich, whose sole publication is a security management magazine with two spinoffs for the Middle East and an international public. **Euro Security** (1996-), the founding magazine, has been published since 1997 concentrating on safety, security and related technology. The other two English speaking publications, **Euro Security International** (1992-) and **MES Security Middle East Security** (2007-) actually follow a very similar approach in content and format but reports and analyses follow certainly the respective markets with some bias to protection technology and organized criminality topics.

The German edition of Euro Security appears nine times a year. The publication has a considerable share of advertisement and in general, the magazine is quite oriented to the security market and products. Writers rarely come from the academia or hold key positions in the industry, and most of the content is written by columnists working for the editorial and is not signed by default. This kind of content make about a third of the publication's content, whereas the resting portion is shared by case studies and advertising. Regular fields in the magazine topics are access control and identification technologies, property protection with special focus in gate locking and video surveillance, building technologies for instance alarm systems and fire protection. IT security occupies only a partial amount of the content and often it copes with IP based security technology such as integrated RFID and surveillance concepts. From time to time, there are articles on information security, backup and business continuity. General articles, case studies and companies' reports tend to depict a topic marketing some security product or services, which might be an important feature for security professionals.

4.3.11. IT Verlag

The IT Verlag für Informationstechnik publishes since fifteen years a couple of magazines with the scope of information technology and some managerial publication for business administration. Nowadays the Sauerlach based editorial publishes a magazine on general networks, software and IT topics with focus to CIO, and a second periodical dedicated to IT security.

IT Security (1999-) appears every two months and concentrates on all aspects of information security including hardware and software technologies as well as access control mechanism for instance in relation to data centers. The editorial board has a classic in-house structure, where the people responsible for the periodicals are not mentioned in other circles out of the editorial publications. The authors, on the other hand, are often linked to the German IT industry, holding CSO or CIO positions or having collaborated in IT conferences and fairs in Europe. The columns and the editorial report often trends in IT security and vulnerabilities having common topics such as backup concepts, IT risk management, access control, cryptography application in software and hardware, business continuity, network security, virus and antivirus and other defense technologies reports and security infrastructure. An important feature is the report of other media such as books and periodicals on IT security as well as updated calendars of Europe wide events in the IT industry. Although the magazine aims to reach IT top managers, the publication contains a high number of advertisements and a considerable number of articles remain unsigned like in other publication of this type.

4.3.12. One-off physical security periodicals

The titles grouping by editorial made in the last sections was due to those editorials publishing mostly two or more relevant titles under a single brand. Since the being presented in the following sections mostly have no similar pairs in the same editorial, and therefore can be considered as isolated publications within the editorial for the purpose of this work, the grouping made from here on is based on the discipline they belong to, in the order: physical, infrastructure, information, and persons topics.

In addition to the physical security publications presented in previous sections, the German Federal Ministries of the Interior and Justice in Berlin have a quinquennial publication called **Periodischer Sicherheitsbericht** (2001-) reporting the criminality situation in the public and private domains and other topics in Germany. Even though the periodical is not a magazine, it is important to mention it since it is one of the key sources to have detailed and more concrete information about this field through its about eight hundred pages. Besides information on criminality in society environments such as juvenile delinquency, road traffic offenses and drugs consumption, the yearbook contains reports relevant to security managers of public and private corporations such as crime against private property, corporate and other economic frauds, environment offences, internet crimes, politics motivated criminality and terrorism.

There is a regular magazine published by the Bundesverband Deutscher Wach- und Sicherheitsunternehmen in Bad Homburg appearing since almost 15 years. The **DSD** (1987-) appears every three months and much of its seventy pages are dedicated to communiqués of the association making it partially an organ magazine. Most of its content though has dedicated columns, news and analyses in security management, common topics are the private security industry, security in logistics, reports in several security branches with focus on valuables transport and other protections services, airport security and event security. Another magazine more concentrated on classic security topics such as property protection is the **Protector** (1977-) published by the editorial Informationsgesellschaft Technik in Munich. The monthly has been published for over thirty years with a regular size of about seventy pages as well. The periodical almost focuses exclusively in physical security topics with no interaction to other branches such as data protection or occupational health. Besides the security, articles there are other columns dedicated to infrastructure resilience topics. A feature of the magazine is its three special supplements on video surveillance, fire protection and access control. These supplements might change from time to time, in the past there were supplements on loss prevention topics such as security in retail stores. Recently there are irregular independent editions of Protector for Austria and Switzerland.

Other magazine aimed to the Swiss public and edited in Forch near Zurich by MediaSec since over fifteen years is **Sicherheits-Forum** (1994-). The one hundred pages bimonthly is one of the few known foreign security magazines in Germany, since its articles do not concentrate in the situation in Switzerland but aims a European public. The magazine has regular columns and special articles in access control and access technologies with focus in biometric and RF-ID devices, it regularly deals with topics on fire protection as well, and property protection subjects in particular for break-in and theft protection. There as well some highlights in information technologies in particular in connection with data centers and know-how protection. The magazine follows in general a risk management focus where columnists introduce the articles starting from a risk analysis perspective.

The Cologne based editorial VdS publishes another security periodical since 1994. The **S+S Report** (1994-) is a magazine appearing every two month with about ninety pages. The company is not an editorial alone but is a whole consulting company with a strong focus to training and certification in the field of damage and loss prevention as well as security technology. The S+S Report is a

little biased to the former topic given that the articles concentrate on burglary protection technologies, fire protection mechanisms and reports and news on the security technology market. Another periodical that cannot be considered a magazine is the **Jahrbuch Unternehmenssicherheit** (2010-) published by Heymanns in Cologne. The publication appears since this year alone, but it had been planned to edit it in a yearly basis with almost three hundred pages. Given it has been published beginning this year, the information given here relates only to a single issue. The publication is designed as collaborative textbook, leaving whole chapters of about twenty pages to a single author specialized in the subject. The yearbook is aimed mostly to CSOs and if it was not for the lack of safety and IT security –there are though sections dedicated to know-how protection– the publication could be analyzed as a book in previous chapters of this research. The topics covered in the current issue are guard and security tasks in corporate environments with focus to airport security, operative security management, security technology and some topics on compliance and regulations.

Another publication focused to security and protection officers in the public and private sectors is the **Info Sicherheit** (n.a. - ongoing) published in Hamburg every three months by the Verband für Sicherheit in der Wirtschaft Norddeutschland. The association is engaged in many activities such as studies and analyses in the security branch for northern Germany as well in certification, seminars and continuing education. In this sense, the Info Sicherheit dedicates considerable space to communiqués of the association. Most part of the ninety pages magazine is focused to security in the economy with regular columns on espionage, product counterfeit, product piracy as well as some regular topics on private investigations and few information security related articles. To conclude, the Darmstadt based GIT editorial, part of Wiley-VCH, publishes **Sicherheit + Management** (1995-) since over fifteen years. The one hundred pages periodical has also a wider topics spectrum in the field of corporate security like other magazines presented so far. This monthly has also a spinoff bimonthly for the international public appearing since about one year called **Security + management** (2007). Both magazines deal physical security, infrastructure resilience and information security topics focusing on loss prevention, property protection, fire and flood protection, IT security and business continuity as well as some regular topics in occupational health and safety.

4.3.13. One-off infrastructure resilience periodicals

In the German speaking countries there is a great assortment of magazines dealing with infrastructure resilience topics such as periodicals published by technical association such as for fire protection, power supply, logistics resilience, disasters and technical safety to name a few. Nevertheless, they fail to take a holistic approach to the whole of critical infrastructures in the public and private sectors as a single topic. There is instead literature offered through books and manuals for further research, from which the German Ministry of the Interior's National Strategy for Critical Infrastructure Protection (Bundesministerium des Innern, 2009) can be an initial source for non-periodical literature. There are though at least three periodic magazines that can somewhat fit in this scope.

The Institut für Krisenforschung in Kiel publishes through its editorial Krisennavigator two journal-type periodicals that focus on the range of topics the institute deals with. The Restrukturierungsmagazin copes with risk management topics in the finance industry and the Krisenmagazin deals with operational risks in several contexts. The about thirty pages **Krisenmagazin** (2010-) appears every three months, but given that it has been published for the first time in 2010 there are only two issues available so far. The periodical is focused to crisis teams in the industry with certain focus to contingencies in their infrastructure, production and other operational aspects. The articles focus on the prevention, early detection, management and follow-up of crises and incidents. The articles in these issues have focused on crises organization and communication with some other case studies on infrastructure crisis intervention, compliance and regulation matters on crises management. The magazine feature also side information on continuing education in the area of crisis management, literature recommendations and general news about recent crisis situations and its handling in the German-speaking industry.

The Munich based Publish-industry editorial is another organization mainly dedicated to the publication of a single media, namely the **S&I Kompendium** (2006-). This publication is not a regular magazine but a looseleaf yearbook appearing with over three hundred pages with topics related to the security of economy and industry. The publication is mostly a compendium on products, companies and services offered in the security branch, and therefore it is strongly based on a marketing scheme, where much of the content promotes certain product or company. The editorial content and articles refer partially to infrastructure resilience topics with articles on plant safety and availability of

industrial processes on the grounds of power supply, logistics and physical security. In this sense, another group of articles is composed by occupational safety and machine safety aimed both to occupational health and production continuity topics, where fire and flooding protection and other related topics occupy valuable content of the publication. The rest of the articles cope with classical topics of corporate security such as property protection, access control and surveillance on one hand as well as IT security, know how and data protection.

Another magazine that lies between the physical protection and infrastructure resilience domains is the **W&S** (2002-) published by the Munich based Informationsgesellschaft Technik editorial mentioned in the last section. The magazine has been published for almost ten years on a two-month basis with over sixty pages. The magazine scope can be divided in two groups. On one hand, the columns focus on economics crimes such as product piracy and corruption, and on the other hand, the periodical copes with classical topics of security such as surveillance and security technology with a strong focus on infrastructure resilience topics such as fire protection and operational availability in production environments. The connection between physical and infrastructure topics is made through recurrent analyses on risk management pursuing the assessment of operational risk in which physical and operational security can minimize breakdowns, failures and other scenarios in the industry.

4.3.14. One-off information security periodicals

The most relevant titles on information and data security magazines were already surveyed in the corresponding section. The assortment of German-speaking periodicals in this area is in certain degree substantial and there are only three relevant magazines that can still be mentioned in this section. The Switzerland based MediaSec editorial already mentioned has an additional publication concentrating on the topic of IT security alone. The **IT-Security** (2004-) has been published since 2004 with a mean size of thirty pages roughly and appears every three months. Besides the IT regular topics, the magazine features some special editions through the years concentrating on areas such as mobile security and data centers. The magazine has a considerable amount of advertising material and regular articles are not signed which points out the magazine is written by dedicated columnists rather than specialized people from the academia and industry. Regular topics of the magazine is everything related with computer technology security such as hardware devices like physical firewalls and routers for secure networks, software quality and security as

well as other topics in programming such as reported attacks and vulnerabilities, the magazine has a special focus on data loss prevention, business continuity and mobile security for road warriors and data backup. There are also several articles for physical security in relation to physical access control of data centers as well as compliance and regulation articles but often biased to the Swiss industry.

Another Swiss magazine is the **Netzwoche** (2000-) published by Netzmedien in Basel on a weekly basis with about fifty pages since ten years. The magazine aims the whole spectrum of information and communication technologies and it is not per se an IT security periodical. What is indeed relevant for this research is that the weekly is published along with six yearly supplements with about twenty pages that partially deal in deep with certain aspects of information and IT security. Supplements such ICT-Riskmanagement, eSecurity and Netzguide in Finance give regular overviews on threat, devices and software aimed to the IT security branch in public and private sectors. In particular, Netzguide in Finance is relevant for compliance officers looking for news and analyses on governance, transparency and other regulations relevant to the IT infrastructures. The Netzwoche covers the German-speaking Switzerland whereas the sister magazine ICT Journal edited in French is aimed to the western territories. Both magazines have also some bias to the Swiss industry in particular on matters pertaining to regulatory subjects. A third Swiss long-running magazine published in Berneck since 1919 is the monthly **Organisator** (2006-). The fifty pages periodical is not a publication focusing on security but it is aimed to managers of small and medium-sized enterprises. The magazine has become only partially relevant to security managers in the last years after few articles and dossiers have been slowly introduced in the publication coping with IT security, occupational health and building security. Nevertheless, the periodical keep a low profile in this topics concentrating on other managerial aspects for this industrial sector.

4.3.15. One-off persons safety and security periodicals

Compared to Austria and Switzerland, Germany has tens if not hundreds of publications for safety, persons security and occupational health. Given this topic is only a partial subject of the research is not necessary to survey all the publication in this matter. Nevertheless, during the collecting process of publication material in this research there was an obvious presence of literature in this matter, which can be at least mentioned in this document for researchers that particularly interested in this topic. Some of the most interesting articles

collected belong to the following magazines: Springer's VDI's Technische Überwachung (1955-), Konradin's Sicherheitsbeauftragter (1966-) and Sicherheitsingenieur (1970-), Austrian Muttenthaler's yearbook Brandschutz – Arbeitssicherheit (2003-), the Austria focused Leykam Dr's Österreichisches Sicherheitsmagazin (2006-) and the SiBe Report of the Unfallkasse Berlin (2005-).For these publication follows complete entries in the bibliography chapter.

Besides these publications and those mentioned in previous sections there is a pair worth to detail. The German Bundesamt für Bevölkerungsschutz und Katastrophenhilfe belonging to the Ministry of the Interior has several publications focusing on civil protection under local and nationwide contingencies. The periodical **Bevölkerungsschutz** (1989-) appears every three months and is not restricted to civil protection topics alone. The magazine has been published since 1989 in an about sixty pages format. The publication lies between the safety and infrastructure resilience fields since every year there is at least one issue dedicated to national critical infrastructures that are the interest of both public and private security officer. More regular articles of the magazine are disaster and emergency medicine, crisis communication and interactions, responsibilities and cooperation between public and private entities in emergency situations.

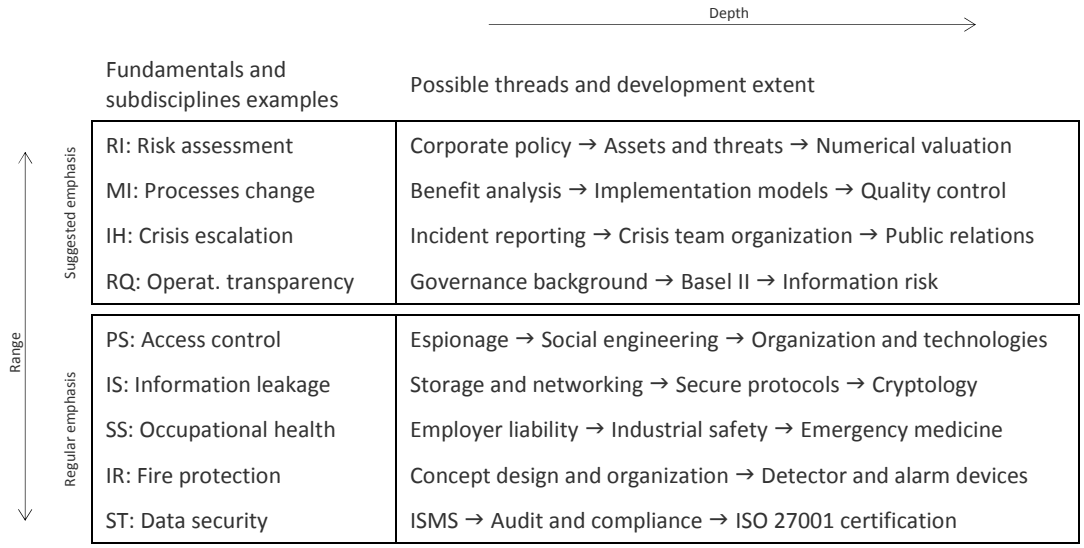
A third magazine published by the Swiss MediaSec is **Safety-Plus** (2001-), which is seventy pages periodical appearing every three months since about ten years. In contrast to other safety and occupational health periodicals, the articles appearing in Safety-Plus seem to have a more holistic approach to the topic of occupational health, since regular columns commonly follow a risk analysis procedure by integrating other security management disciplines such as infrastructure resilience, machine security and cross-topics such as fire protection, security and crisis simulation. As usual in the health and safety fields, publications on this area are always accompanied by regulatory and compliance topics given the importance for national industrial safety regulations, and therefore Safety-Plus focuses to the situation in Switzerland.

5. Publishing recommendations

The previous chapter analyzed several security publications that were identified through a methodological research aimed to specialist books, academic journals and professional magazines. The characteristics of security management as a relative new discipline, that integrates key elements of business informatics, property protection, incident management and other aspects in a growing globalizing economy, is one of the reasons why the literature offer in this area is still compact. The recommendations in this chapter are mainly aimed to the structure of specialist books, given that no concrete suggestions for academic journals and specialist magazines could be determined, as explained as follows. The scope for magazine research was the assessment of several periodicals focusing on the subdisciplines. The collected and surveyed publications meet the criteria of this work and therefore no further publication is needed in this area. The case of academic journals is a little less simple given that this type of publication exhibits the ongoing research of institutes, research groups and the academia in general. Since the scope of this work was not the survey of academic research in the security management field, it is hard to provide concrete recommendation that may be based on that security research landscape. Nevertheless, the perspective and recommendations given here for the structuring of specialist books may apply to academic journals as well.

Even though there has been a couple of works that pursued to integrate multidisciplinary aspects of corporate security in a single publication, it was not until the solid establishment of information technologies in the organizations of companies (Hughes, 2008, pp. 110-119), the awareness of global security issues across national borders after 9/11 (Dalton, 2003, pp. 87-98) and the necessity of laws and acts for corporate governance and risk transparency before investors,

that security management was shaped with concrete multidisciplinary requirements reflected, e.g. in Germany, in a growing demand of security management university programs. This demand is approaching the academic world not only in the form of qualification of security professionals, but is defining the shape of security literature, where scholars from informatics, classical security, strategic and operational risk management and public relations to name a few are finding a common meeting place, namely corporate security management. Example of this is that authors such as Gundel, Mülli, Von zur Mühlen and Müller either come from the informatics or physical security fields and most of the significant books have been edited in the last three years and some of them have recent second editions published recently or planned to be released next year.



	Fundamentals and subdisciplines examples	Possible threads and development extent
Suggested emphasis	RI: Risk assessment	Corporate policy → Assets and threats → Numerical valuation
	MI: Processes change	Benefit analysis → Implementation models → Quality control
	IH: Crisis escalation	Incident reporting → Crisis team organization → Public relations
	RQ: Operat. transparency	Governance background → Basel II → Information risk
Regular emphasis	PS: Access control	Espionage → Social engineering → Organization and technologies
	IS: Information leakage	Storage and networking → Secure protocols → Cryptology
	SS: Occupational health	Employer liability → Industrial safety → Emergency medicine
	IR: Fire protection	Concept design and organization → Detector and alarm devices
	ST: Data security	ISMS → Audit and compliance → ISO 27001 certification

Figure 9 Regular segmented approach

Suggestion for structuring a specialist book for security management must consider several aspects and therefore, although some universal guidelines can be proposed, particular recommendations would require concrete information about the aim of the book such as readership, size of the publication, depth of the topics and possible pursued biases of interest. Given that security management is a field composed by several disciplines, perhaps the most determining factor in conceiving a security specialist book is its size and ergo the depth of the topics studied. It was shown in previous chapters that security management books concentrate on a typical shape of modern organizations, that put together in certain degree all aspects of corporate security roughly following the structure shown in Figure 9. The table illustrates on the left side the topics on which a security management publication can range. It was seen that whereas few books pay special attention to the fundamentals, the largest part of

them concentrate on the subdisciplines. The focus on the subdisciplines might be an advantage for readers looking for technical and concrete methodological issues, nevertheless it was attested that commonly this type of books turn out to be composed of disassociated chapters merely reviewing the different aspects of security. In chapter 4 it was mentioned that book that books roughly falling in this category with some exceptions and conditioned to particular characteristics are those books reviewed in section 4.1, save the works of Tenckhoff and Siegmann (2009) and von zur Mühlen (2006), plus Adams' (1990) and Edelbacher's (2000). The lower table section of the figure illustrates this observation under the label Regular emphasis. The acronyms PS, IS, SS, IR and ST of the subdisciplines correspond respectively to physical security, information security, persons safety and security, infrastructure resilience and standards and tools. For book structures that prefer to use a clear separation between fundamentals and subdisciplines, the proposed emphasis should lie on the former set of topics represented by RI, MI, IH and RQ for risk identification, measures identification and implementation, incident handling and requirements. It was likewise mentioned in the book analysis that books that accent the importance and develop the fundamental topics are Gundel and Mülli's (2009), Sack's(2007) and Tenckhoff and Siegmann (2009).There are though elementary disadvantages of these works where the following observations may improve the general structure of the contents. Even though these works consider the fundamental topics as the central focus of security management, in the long run they derive in chapters where a mere description of security disciplines, technologies and organizations is given putting behind or overlooking the integrated structure of the preventive and reactive aspects of security management as given by the fundamental structure. In many cases, depending on the background of the authors, a determined area of security is favored over other fields and the depth covered by the corresponding chapters is unbalanced or well the stressing on certain security area is not sufficiently justified. In this sense, the figure above additionally represents some threads on which the literature develops several security topics. Whereas some books stress the importance of IT in corporate security and even go further on explaining cryptographic tools and algorithms, other books treat information security from a non-technical point of view, and in turn concentrate on property protection topics such as access control technologies and video surveillance devices. It is indeed not stated by this work that security management books cannot go deeper into technicalities of selected fields, but it is perhaps the edition size the main restriction why authors should find a balance between all disciplines. In spite of everything, it should be the

fundamentals the core of a security publication where the subdisciplines topics play the role of contextualizing the readership on risk identification, measure identification and incident handling for a particular area of corporate security. Two authors that do clearly engage into the fundamentals are Müller (2005) and the von zur Mühlen's booklet (2006). Nevertheless they concentrate mainly only in the measures implementation, try to find a very general methodology for all security areas and the illustration of the method is almost based purely on information security models with no visible proof of its possible application to other fields.

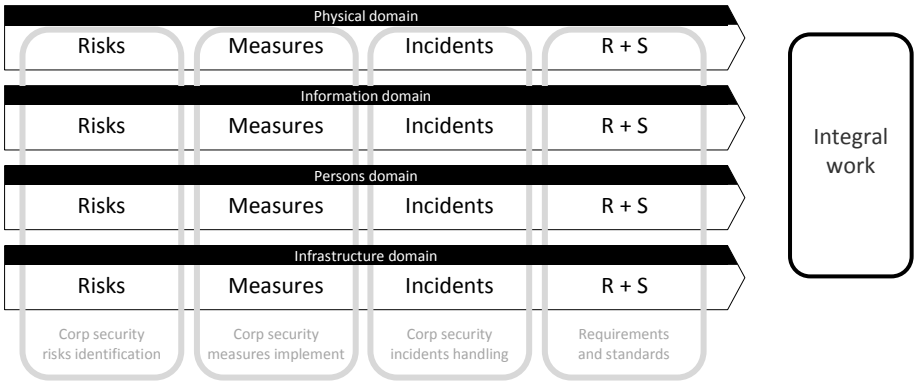


Figure 10 Subdisciplines-based approach with fundamentals as backbone

A second perspective for the design of a security management book is the integration of fundamentals topics not as introductory features but as structural backbone in the development of the subdisciplinary areas. Figure 10 illustrates this outline where either each subdiscipline can be treated horizontally one at a time starting from its preventive to reactive own aspects or else the book can be developed vertically beginning with corporate risk, through corporate measures and corporate incidents to corporate requirements and standards. The second perspective might integrate better all four defined security areas putting together every risk, every measures and every incident scenario that may affect the organization as a single corporate body other than falling again in the disaggregated vision that e.g. assigns information to IT specialists, property protection to security officers and persons and infrastructure to safety and industrial engineers. This structure allows thus to strengthen and the awareness of the upper functional position of a security manager as one central corporate head throughout the textbook. Additionally, the model can help to avoid the prevailing tendency of going deeper into particular technologies and systems for publications with space restrictions. Nevertheless, if a deep development of a particular subdiscipline or fundamental is wished as part of a major work composed for example of two or more bands a vertical or horizontal ap-

proach might be helpful where bands for corporate security risk identification or corporate physical security could be the start point. In any case, either as a single band or multiband work, the model should be regarded as a base in order to keep the focus and balance in corporate security as a single integral discipline.

6. Conclusion

This work presented the development of three principal tasks aimed to the survey, analysis and recommendations in the publication of security management literature. A key initial step in the investigation was to define security management as a discipline in terms of the topics and areas of research treated by it. Without this step, the approach to survey and analysis of security literature may have taken to very different results not based on a standardized schema. By this reason, it seemed suitable and favorable to create a common frame of reference for security management, even though the authors may consider and treat the discipline from different and sometimes differing points of view. This is why, after putting into context the range of tasks in security management, the topics were classified in two upper categories. It was hence recognized that security management is composed of fundamental topics and applied subdisciplines. As it was later stated, the fundamentals have been considered secondarily by the literature and sometimes are completely dismissed. The division in fundamentals and subdisciplines led to the further differentiation of preventive and reactive aspects for the first in the form of risk identification, measure identification and implementation and incident handling. In turn, the applied subdisciplines were classified based not on any particular order but in consideration of their nature in terms of assets, technologies, function and other features. In this sense, it was found appropriate classifying the subdisciplines according to the nature of object pursued by it: material objects, non-material objects, human resources and infrastructure, which corresponded to the set used through the work namely physical security, information security, persons safety and security as well as infrastructure resilience respectively. A final aspect of security management was considered given the interaction with third parties an organi-

zation has with. This refers to legal requirements, which were allocated to the fundamentals, and industry standards and management tools as part of the subdisciplines.

The definition of security management was not only a necessary step in order to analyze and set a common reference scheme for literature. The grouping of security topics set the basis for the literature research giving specific highlights on what was being looked for, since the mere search for security management alone may have returned bigger or insufficient results as expected. The research of literature and the following rest of the work actually correspond to a triple strategy, given that neither the research nor the analyses could be made based on a common approach for all books, journals and magazines. The books research was the first survey made, and also the part that rose key lessons for a better research. At the beginning, it seemed simple to search for titles in the main databases available in Germany including commercial and academic providers. Nonetheless, the question whether no title was left missing always stayed in the background, which made the process repeat a couple of times even with the catalogue unions that link all big libraries in Germany, though not all. The Deutsche Nationalbibliothek provided the sought central resource collecting and monitoring practically all publications in the sprachraum, even if at a first glance it was not considered quite useful given that the physical exemplaries cannot be lent outside its libraries in Leipzig and Frankfurt. Further drawbacks appeared by the database limitations in terms of the accuracy of the bibliographic entries and the research capabilities offered. Even if database fields such as year and discipline reduce significantly the number of matches, it was found out that the only reliable field to be used was the title and subtitle alone. This might be due to a number of reasons such as a faulty data input process and more likely as a consequence of the difficulty of allocating security management literature in economics, computer or engineering sciences for instance. At some point, it was realized that the filtering of data could not be performed by the servers but the main filtering and data management should be done in a local machine. The employed catalogues for books, magazines and journals could not perform some wished functions such as discarding of duplicates and determining frequently useless keywords. This is why a part of the research had put together all the titles and coped with the manual filtering of thousands of titles in order to make as sure as possible that no many titles were being left behind.

Similar processes were followed for the periodicals research. Given that the academic journals research was aimed to both German and mostly English publications, the research had to find two separate resources for both languages or else a single resource containing specifically academic journals regardless the publication language. Even if the research concentrated in German-speaking academic journals alone, the Zeitschriftendatenbank, another service of the Deutsche Nationalbibliothek, would not have offered a discrimination of regular periodicals from the aimed academic ones. For this reasons, both Worldcat and Ulrich's were used to find the relevant security journals since these services could be configured to return only the academic periodicals, saving the effort of borrowing hundreds of publications to find out that most of them were not academic journals indeed. Even though this seems a straightforward step, the present investigation had to deal with tens of bibliography providers and identify the most reliable ones. A similar step was done here for retrieving the result sets and locally managing the data either manually or through scripts. Finally, the most adequate for specialist magazines research was determined to be provided by the Deutsche Nationalbibliothek through the Zeitschriftendatenbank. Given that the scope for magazines was not corporate security as a whole but it aimed the four discipline areas as defined previously, the work in this stage was divided and four independent researches were conducted respectively and similar processes of data retrieving and local machine filtering were done. One significant lesson learned in this process was that, other than in the book survey, the Internet was a key resource for double checking the relevance of the publications, given that almost all editorials, or at least all scoped by this research, have a web site where the general characteristics of the periodicals could be attested prior to borrowing the exemplaries or articles.

The compilation of material was the basis for beginning the analysis of the three types of publications. Since the beginning, prevailed the idea of avoiding an analysis in terms of winners or bad publications, given that it is the end-reader who may find helpful some titles and discard others according to his needs. Nevertheless, at the same time it was somewhat required to evaluate methodically the publication with no intention of setting a hierarchy among them. A first necessary step was to make a systematic reading of all the compiled material in order to devise a non-numerical scale, which may be illustrative enough to give an overview of all the surveyed material and the relevance of their content with each area defined in this work. This resulted in the three charts in the analysis chapter. In a first draft of this investigation stage, it was planned to present those charts with an introductory text as central and single

content of that chapter. Nonetheless, it was later determined that a marginal description without supporting the results with a formal and uniform review of the material would lead to an inconsistent analysis. This consideration resulted thus in the structured review of all publications based on the general structure of fundamental and subdisciplinary topics with the minor disadvantage of increasing in some degree the body of this work.

The concluding recommendations from the last chapter were mainly done for specialist books and partially for academic journals. No recommendations were originally aimed for specialist magazines, since the research scope was to find and analyze the material available in each subdiscipline and adequate periodicals were expected and found for all the subdisciplines. The previous chapter instead concentrated on the general structure of prospective security management books: a conventional segmented approach between fundamentals and subdisciplines as well as a second approach with a generic backbone for the development of the subdisciplines. The research and the recommendations chapter set the basis for two possible lines of investigation for a bachelor thesis. The status of the collected material refers to the present year, nevertheless new material constantly appears in particular for books and specialist magazines, and some other, both journals and magazines, cease to be published or get merged in other publications or other editorials. A possible future work for the collection of material is to design a system or method through which a security management scholar or professional can be aware of this changing behavior in the publishing landscape. Some highlights have been given in this sense. The use of surveyed bibliographic services and the morphological considerations given in the research chapter are a first step for such prospective research. A second future line of investigation is to develop the recommendations for academic journals through a research of investigation institutes and higher education institutions. These bodies can be the base to obtain a picture of the state of the art in security management topics research in German-speaking countries. The mention of this geographic area pursues to delimit the future work in a small domain in order to integrate more research made in a European or worldwide scale. One of the main results of such investigation would be to develop a map of research being made on all aspects of the field and find points of contact with a layout of the discipline in order to evaluate the possible editorial approaches, feasibility and deployment of a security journal.

7. Bibliography

Adams, H. W. (Ed.). (1990). *Sicherheitsmanagement.* Frankfurt: Frankfurter Allgemeine Zeitung.

Adams, H. W. (1992). *Unternehmerisches Risikomanagement: bessere Organisation - mehr Sicherheit.* Cologne: TÜV Rheinland.

Adolphs, U. (2008). *Wahrig Synonymwörterbuch.* Gütersloh: Wissen Media.

Allgemeine Unfallversicherungsanstalt. (2006-). *Österreichisches Sicherheitsmagazin.* Neudörfl: Leykam Dr. GmbH.

Ansorge, K. (2008). *Deutsche Nationalbibliothek: Bewahren für die Zukunft.* Leipzig; Frankfurt: Deutsche Nationalbibliothek.

Arbeitssicherheit und Gesundheitsschutz im Betrieb aktuell : Praxistipps und Informationen für Sicherheitsfachkräfte, Führungskräfte und Sicherheitsbeauftragte. (2004-). Bonn: Verlag für die Deutsche Wirtschaft.

Asfahl, C. R., & Rieske, D. W. (2010). *Industrial Safety and Health Management.* Upper Saddle River, N.J: Prentice Hall.

ASIS International. (2010). Retrieved 9 2, 2010, from CSO Roundtable: http://www.csoroundtable.org/

ASIS International, Inc. (2010). *News*. Retrieved 4-10 2010, from Security Management : Security's Web Connection: http://www.securitymanagement.com/news

Assets protection : an international journal. (1975-1981). Madison, Wisc: Territorial Imperative.

Australian security journal. (1968-1973). Sydney: Institute of Commercial and Industrial Security Executives.

Bankmagazin : für Führungskräfte der Finanzwirtschaft. (1993-). Wiesbaden: Gabler, Springer-Fachmedien Wiesbaden.

Barboza de Souza, A., Pereira da Silva, J., Cavalcante de Oliveira, W. C., Kuma, T. H., & Silveira, I. F. (2008). Recuperação Semântica de Objetos de Aprendizagem. *Anais do Simpósio Brasileiro de Informática na Educação* , 603-612.

Bevölkerungsschutz. (1989-). Bonn: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe.

BNP Media. (2010). Retrieved 3 28, 2010, from Security Magazine: http://www.securitymagazine.com/

Borodzicz, E. P. (2005). *Risk, Crisis and Security Management.* West Sussex, England: Wiley & Sons.

Bundesministerium des Innern. (2009). *Nationale Strategie zum Schutz kritischer Infrastrukturen (KRITIS-Strategie).* Berlin.

Canoo Engineering AG. (2010). *Grammatik der Wortbildung für Deutsch.* Retrieved June 14, 2010, from Canoonet: http://www.canoo.net/services/WordformationRules/ueberblick/

CD Sicherheits-Management. (1994-). Stuttgart: Boorberg.

Computer-Reseller-News : die Zeitschrift für Fachhändler, Integratoren und Systemhäuser. (1998-). Poing: CMP-Weka-Verl.

Connect : Europas grösstes Magazin zur Telekommunikation. (2010-). Stuttgart: WEKA Media Publ.

Corporate security. (1981-2008). New York: Business Research Publications.

CSO. (1999-). Connecticut: IDG Communications.

Dalton, D. R. (2003). *Rethinking Corporate Security in the Post-9/11 Era: Issues and Strategies for Today's Global Business Community.* Amstemdarm: Butterworth-Heinemann.

Damodaran, A. (2008). *Strategic risk taking : a framework for risk management.* Upper Saddle River, N.J.: Pearson Prentice Hall, Wharton School Pub.

Datenschutz aktuell : aktuelle Praxistipps und Informationen für den Datenschutzbeauftragten im Unternehmen. (2004-). Bonn: Verlag für die Deutsche Wirtschaft.

Datenschutz und Datensicherheit : DuD ; Recht und Sicherheit in Informationsverarbeitung und Kommunikation. (1983-). Wiesbaden: Gabler, GWV-Fachverl.

Davies, S. J., & Hertig, C. A. (2007). *Security Supervision and Management.* Oxford: Butterworth-Heinemann.

Der Detektiv : Fachzeitschift für das Sicherheitsgewerbe. (2002-). Wien: Cornelia Haupt.

Der Spiegel. (2010). Retrieved 7 5, 2010, from Amokläufer: http://www.spiegel.de/thema/amoklaeufer/

Deutsches Polizeiblatt : Fachzeitschrift für die Aus- und Fortbildung in Bund und Länder. (1983-). Stuttgart: Boorberg.

Die Zeit. (2010, 2 6). Retrieved 7 3, 2010, from Kindesmissbrauch : Die Kirche kämpft mit ihrer Sexualmoral: http://www.zeit.de/gesellschaft/zeitgeschehen/2010-01/kirche-missbrauch-canisius-kolleg

Digma : Zeitschrift für Datenrecht und Informationssicherheit. (2001-). Zürich: Schulthess Juristische Medien.

Disaster Recovery Journal. (2010, 4 10). *Eyjafjallajokull Erupts: Cost of Damage in Millions*. Retrieved 6 20, 2010, from http://www.drj.com/4552-eyjafjallajokull-erupts-cost-of-damage-in-millions.html

DNB. (2010). *http://www.d-nb.de/wir/ueber_dnb/sammelauftr.htm*. (D. Nationalbibliohtek, Producer) Retrieved 8 3, 2010, from Sammelauftrag der Deutschen Nationalbibliothek: http://www.d-nb.de/wir/ueber_dnb/sammelauftr.htm

Donaker, G. (2006, 6 9). *The Stanford Natural Language Processing Group .* Retrieved 5 3, 2010, from http://nlp.stanford.edu/courses/cs224n/2006/fp/gdonaker-1-ProjectWriteup.doc

DSD : Der Sicherheitsdienst : Offizielles Organ des Bundesverbandes Deutscher Wach- und Sicherheitsunternehmen e.V. (1987-). Bad Homburg: DSA GmbH.

Edelbacher, M., Reither, P., & Preining, W. (2000). *Sicherheitsmanagement.* Vienna: Linde.

Elles, A. (2008). *Risiken vermeiden, Krisen bewältigen.* Hamburg: Behr.

Euro Security : das deutsche Sicherheitsmagazin für Planer, Errichter und Anwender. (1996-). Munich: SEC! The Publishing House.

Euro Security : the european magazine for security technology and applications. (1992-). Munich: SEC Publishing House.

Fink, A. G. (2008). *Conducting Research Literature Reviews.* Thousand Oaks, Calif: Sage Publications.

Flast, R. H., & Dickstein, D. I. (2009). *No Excuses: A Business Process Approach to Managing Operational Risk.* New Jersey: Wiley.

FORSI. (2010). *Deutschen Universität für Weiterbildung Newsletter*. Retrieved 7-8 2010, from Forschungsinstitut für Compliance, Sicherheitswirtschaft und Unternehmenssicherheit: http://forsi.duw-berlin.de/forsi-aktuell/duw-newsletter.html

Gefahrgut aktuell : Sofortinformationen für die Praxis. (1992-). Landsberg: Ecomed-Sicherheit.

Geigle, P. (1999). *Unternehmensrisiken : erkennen, bewerten, bewältigen.* Eschborn: AWV - Arbeitsgemeinschaft für Wirtschaftliche Verwaltung e.V.

Gleißner, W. (2008). *Grundlagen des Risikomanagements im Unternehmen.* Munich: Vahlen.

Gundel, S., & Mülli, L. (2009). *Unternehmenssicherheit.* Munich: Oldenbourg.

Gupta, P., & Sharma, A. (2010). Context based Indexing in Search Engines using Ontology. *International Journal of Computer Applications* , 53-56.

Halibozek, E. P., & Kovacich, G. L. (2003). *The Manager's Handbook for Corporate Security: Establishing and Managing a Successful Assets Protection Program.* Boston: Butterworth-Heinemann.

Hames, I. (2007). *Peer Review and Manuscript Management in Scientific Journals.* Maiden, MA: Wiley-Blackwell.

Herder, P. M., & Thissen, W. A. (2003). *Critical Infrastructures: State of the Art in Research and Application.* Boston: Springer.

Hinterscheid, U. (2008). *Ansätze zur Bewältigung existenzbedrohender Unternehmensrisiken : Sicherung globaler Wertschöpfungsprozesse durch betriebliche Kontinuität.* Berlin: Pro Business.

Hodson, W. K., & Maynard, H. B. (2001). *Maynard's Industrial Engineering Handbook.* New York: McGraw-Hill.

Hughes, B. (2008). *Exploiting IT for Business Benefit.* Swindon: British Computer Society.

Hunter, R., & Westerman, G. (2007). *IT risk : turning business threats into competitive advantage.* Boston: Harvard Business School Press.

Ibing, H.-P. (1996). *Sicherheitsmanagement: ein Instrument der Ergebnissteuerung.* Landsberg/Lech: Verl. Moderne Industrie.

Ick, R., & Matschke, K.-D. (1998). *Security-quality-Management-Handbuch : Grundsätze und Verfahren für umfassende Unternehmenssicherheit.* Ingelheim: SecuMedia-Verl.

Info Sicherheit. (n.a. - ongoing). Hamburg: Verband für Sicherheit in der Wirtschaft Norddeutschland.

Information week : das Praxismagazin für CIOs und IT-Manager. (1997-2010). Poing: CMP-WEKA-Verl.

Institut für Krisenforschung. (2010). *Bücher & Studien*. Retrieved 7 8, 2010, from Krisennavigator: http://www.krisennavigator.de/Krisenshop.krisenshop.0.html

International Association of Counterterrorism & Security Professional. (2005-2006). The journal of counterterrorism & homeland security international. Arlington, Virginia: SecureWorldnet, Ltd.

International Journal of Business Continuity and Risk Management. (2009-). Milton Keynes: Inderscience Enterprises.

International Journal of Risk Assessment and Management. (2000-). Milton Keynes: Inderscience Enterprises Ind.

International Journal of Risk, Security and Crime Prevention. (1996~2005). Leicester: Perpetuity Press.

Internet-Magazin : Knowhow für Web-Profis. (1996-). Poing: WEKA Media Publ.

IOMA's Security Director's Report. (1993-). New York: Institute of Management & Administration.

IT Security. (1999-). Sauerlach: IT-Verl. für Informationstechnik.

IT-Grundschutz: Für CIOs, IT-Manager und IT-Sicherheitsverantwortliche. (2006-). Gau-Algesheim: SecuMedia-Verl.

IT-Security : die Schweizer Fachzeitschrift für Informationssicherheit. (2004-). Forch: MediaSec.

IT-Sicherheit : Fachmagazin für Informationssicherheit und Compliance. (1997-). Frechen: Verl.-Gruppe Hüthig-Jehle-Rehm, Datakontext.

Jahrbuch Unternehmenssicherheit. (2010-). Cologne: Heymanns.

Journal of Applied Security Research. (2007-). Binghamton: Haworth Press.

Journal of Contingencies and Crisis Management. (1993-). Oxford: Blackwell Publishers.

Kamiske, G. F. (2008). *Technisches Risiko- und Krisenmanagement.* Düsseldorf: Symposion.

Kes : die Zeitschrift für Informations-Sicherheit. (1985-). Gau-Algesheim: SecuMedia-Verl.

KIT-Bibliothek Karlsruhe. (2009). *Über den KVK*. Retrieved June 13, 2010, from KVK Karlsruher Virtuelle Katalog: http://www.ubka.uni-karlsruhe.de/hylib/virtueller_katalog.html

Konradin; Haefner. (1966-). *Sicherheitsbeauftragter : die Fachzeitschrift für Sicherheit und Gesundheit bei der Arbeit.* Heidelberg: Konradin; Haefner.

Konradin; Haefner. (1970-). *Sicherheitsingenieur : Die Fachzeitschrift für betriebliches Sicherheitsmanagement und Prävention.* Heidelberg: Konradin; Haefner.

Krisenmagazin : Zeitschrift für Krisenmanagement, Krisenkommunikation und Krisentraining. (2010-). Kiel: Krisennavigator, Inst. für Krisenforschung.

Lexico Publishing Group, LLC. (2010, May 30). *Thesaurus.com*. Retrieved May 30, 2010, from Reference.com: http://www.reference.com

Lindner, J. (2007). *Security als Managementaufgabe.* Stuttgart: Steinbeis-Ed.

Linguee GmbH. (2010). Retrieved June 14, 2010, from Linguee – The web as a dictionary: http://www.linguee.de/

Livres Groupe. (2010). *Base de Données Bibliographiques Sur Internet: Libre Accès, Animalbase, Urbamet, Web of Science, Pubmed, Worldcat, Blackwell Publishing, Pascal.* Marseille: Book LLC.

Löhneysen, G. v. (1982). *Die rechtzeitige Erkennung von Unternehmungskrisen mit Hilfe von Frühwarnsystemen als Voraussetzung für ein wirksames Krisenmanagement.* Göttingen: Göttingen, Univ., Diss., 1983.

Mabe, M. (2003). The growth and number of journals. *Serials: The Journal for the Serials Community , 16* (2), 191-197.

Mann, T. (2005). *The Oxford Guide to Library Research .* New York: Oxford University Press.

Mark, R., Galai, D., & Crouhy, M. (2006). *The Essentials of Risk Management.* New York: McGraw-Hill.

Meier, P. (2007). *Praxisleitfaden des operativen Risikomanagements: Prozessorientiertes Vorgehen für den Mittelstand.* Kissing: Weka Media GmbH.

Mensch, G. (1990). *Risiko und Unternehmensführung : eine systemorientierte Konzeption zum Risikomanagement.* Berlin: Berlin, Techn. Univ., Diss., 1990 .

Merriam Webster. (2007). *Merriam Webster's Collegiate Dictionary & Thesaurus.* Oxford.

MES security : magazine for security technology and applications in the Middle East. (2007-). Mettmann: Euro Security Fachverl.

MIT Sicherheit administrieren und vorbeugen : Fachzeitschrift für Netzwerk-, IT & Internetsicherheit. (2004-). Bonn: Verlag für die Deutsche Wirtschaft.

Monahan, G. (2008). *Enterprise Risk Management: A Methodology for Achieving Strategic Objectives.* Hoboken, N.J.: John Wiley & Sons.

Müller, K.-R. (2005). *Handbuch Unternehmenssicherheit.* Wiesbaden: Vieweg.

Müller, K.-R. (2003). *IT-Sicherheit mit System.* Wiesbaden: Vieweg.

Muttenthaler. (2003-). *Brandschutz - Arbeitssicherheit : Jahrbuch.* Petzenkirchen: Muttenthaler.

Network Computing. (1998). Poing: CMP-WEKA.

Netzwoche : das Schweizer ICT-Magazin für Business-Entscheider. (2000-). Basel: Netzmedien.

Neues Polizeiarchiv. (1952-). Stuttgart ; München ; Hannover: Boorberg.

OCLC. (2009). *What is WorldCat?* (OCLC Online Computer Library Center, Inc) Retrieved 8 3, 2010, from WorldCat.org: http://www.worldcat.org/whatis/default.jsp

Ohder, C. (1999-). *Unternehmensschutz: Praxishandbuch.* Stuttgart ; München et al.: Boorberg.

Online Computer Library Center. (2006). *Journalseek Database*. Retrieved 07 6, 2010, from OCLC The World's Libraries Connected: http://nj.oclc.org/journalseek/

Organisator : Das Magazin für KMU. (2006-). Berneck: Organisator.

Ortmeier, P. J. (2009). *Introduction to Security.* Upper Saddle River, N.J.: Prentice Hall.

PC go! : das verständliche Computer-Magazin. (1993-). Poing: WEKA Computerzeitschriftenverl.

PC Magazin. (1998-). Poing: Weka-Computerzeitschr.-Verl.

Periodischer Sicherheitsbericht. (2001-). Berlin: Bundesministerium des Innern ; Bundesministerium der Justiz.

Pidcock, W. (2009, October 6). *What are the differences between a vocabulary, a taxonomy, a thesaurus, an ontology, and a meta-model?* Retrieved May 27, 2010, from Infogrid: http://infogrid.org/wiki/Reference/PidcockArticle

Polizei heute: Führung, Technik, Ausbildung. (1994-). Stuttgart ; München: Boorberg ; Inspekteur der Bereitschaftspolizeien der Länder, Bundesinnenministerium.

Proceedings, the Institute of Electrical and Electronics Engineers Annual International Carnahan Conference on Security Technology. (1982-). New York: Institute of Electrical and Electronics Engineers.

ProQuest LLC. (2009). *About the Ulrich's Database*. (ProQuest LLC) Retrieved 10 4, 2010, from The Global Source for Periodicals: http://www.ulrichsweb.com/ulrichsweb/ulrichsweb_news/ulrichsinsideabout.asp

Protector : Die europäische Fachzeitschrift für Sicherheit. (1977-). Munich: I.G.T. Informationsgesellschaft Technik mbH.

Purpura, P. P. (2008). *Security and Loss Prevention.* Oxford: Butterworth-Heinemann.

Richard Boorberg Verlag. (2010). *Fachbeiträge im Sicherheitsmelder*. Retrieved 8 9, 2010, from Sicherheitsmelder: http://www.sicherheitsmelder.de/gate.dll?op=start

Richard Boorberg Verlag. (2008-2010). *Sicherheits-News-Archiv*. Retrieved 5-8 2010, from http://www.boorberg.de/sixcms/detail.php?id=61471

Risk UK : the journal of security and loss prevention. (2003-). Chislehurst: Pro-Activ.

Roselieb, F. (2008). *Krisenmanagement in der Praxis.* Berlin: Erich Schmidt Verlag.

Rost, F. (2010). *Lern- und Arbeitstechniken für das Studium.* Wiesbaden: Vs Verlag.

Rothstein, P. J., Kaye, D., & Graham, J. (2006). *A Risk Management Approach to Business Continuity: Aligning Business Continuity with Corporate Governance.* Brookfield, Conn: Rothstein Associates.

S & I Kompendium : das Referenzbuch für Sicherheit & Industrie. (2006-). Munich: Publish-Industry-Verl.

S+S-Report : VdS-Magazin Schadenverhütung + Sicherheitstechnik. (1994-). Cologne: Vds Schadenverhütung Verl.

Sack, D. K. (2007). *Corporate Security – Standort Security.* Stuttgart/Berlin: Steinbeis-Hochschule Berlin, Steinbeis-Transfer-institut Business Academy.

Safety-Plus : Schweizer Fachzeitschrift für Arbeitssicherheit und Gesundheitsschutz. (2001-). Forch: MediaSec.

Schleswig-Holstein, U. L. (1999-2007). BackUP : Magazin für IT-Sicherheit. Kiel: Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein.

Schmidt, K. (2010). *High Availability and Disaster Recovery.* New York: Springer.

Schneier, B. (2010). Retrieved 3 22, 2010, from Crypto-Gram Newsletter: http://www.schneier.com/

Security + management : magazine for safety and security. (2007). Darmstadt: GIT Verl.

Security and property protection. (1973-1980). Sydney: Institute of Commercial and Industrial Security Executives.

Security insider. (1995-). Crows Nest, New South Wales: Australian Security Industry Association.

Security management. (1972-). Arlington: American Society for Industrial Security.

Security management bulletin : protecting property, people & assets. (1985-2000). Watterford, Conn: National Foremen's Institute.

Security newsletter : Analysen und Lösungen zu aktuellen Gefahren für die Daten- und Netzwerksicherheit. (1997-). Kissing: Weka Media.

Security point : Fachzeitschrift für Sicherheitslösungen in öffentlichen Bereichen. (1999-). Stuttgart: Boorberg.

Security watch : protecting people, property & assets. (1990-2003). Waterford, Conn: Bureau of Business Practice.

Seidlhofer, B. (2005). English as a lingua franca. *ELT Journal* , 339-441.

Sesink, W. (2007). *Einführung in das wissenschaftliche Arbeiten.* Munich: Oldenbourg.

Sheffi, Y. (2007). *The Resilient Enterprise.* Cambridge, Mass.: MIT Press.

Sicherheit + Management : Magazin für Safety und Security. (1995-). Darmstadt: GIT-Verl.

Sicherheits-Berater : Informationsdienst zur Sicherheit in Wirtschaft und Verwaltung. (1974-). Bonn: TeMedia.

Sicherheits-Forum : Schweizer Fachzeitschrift für Sicherheit. (1994-). Forch: MediaSec.

Sicherheitshalber : Zeitschrift für Sicherheit in der Supply Chain. (2003-). Stuttgart: Boorberg.

Sicherheits-Jahrbuch für Deutschland und die Schweiz. (1987-). Zürich; Ingelheim: SecuMedia-Verl.

Sicherheits-Markt. (1993-). Gau-Algesheim: SecuMedia-Verl.

SIG security, audit & control review. (1982-1997). New York: Association for Computing Machinery.

Staatsbibliothek zu Berlin. (2010). *Über die Zeitschriftendatenbank*. Retrieved 9 3, 2010, from http://www.zeitschriftendatenbank.de/ueber-uns.html

Stober, R. (2010). *Recht der Sicherheit · Private, Public & Corporate Security · Sicherheitsgewerbe und Public Relations.* Cologne: Heymann.

Stucki, C., & Marcella, A. J. (2004). *Business Continuity, Disaster Recovery, and Incident Management Planning: A Resource for Ensuring Ongoing Enterprise Operations.* Altamonte Springs, Fla: The Institute of Internal Auditors Research Foundation.

Süddeutsche Zeitung. (2010, 4 21). Retrieved 6 20, 2010, from Die Luft ist rein, das Chaos bleibt am Boden: http://www.sueddeutsche.de/politik/europaeischer-flugverkehr-normalisiert-sich-die-luft-ist-rein-das-chaos-bleibt-am-boden-1.933815

Tenckhoff, B., & Siegmann, S. (2009). *Vernetztes Betriebssicherheitsmanagement [BSM ; Qualitätsmanagement, Risiko- und Krisenmanagement, Brandschutz, Umweltschutz, Betriebssicherheit, Arbeits- und Gesundheitsschutz, Datenschutz].* Heidelberg: Haefner.

The Holmes Report. (2009, 10 13). Retrieved 7 2, 2010, from The France Telecom Suicides: Implications for Crisis PR and Change Management: http://www.holmesreport.com/hblog/post.cfm/the-france-telecom-suicides-implications-for-crisis-pr-and-change-management

Treffpunkt Arbeitssicherheit: Die Wandzeitung für jeden Betrieb. (n.a. - ongoing). Landsberg: Ecomed-Sicherheit.

Unfallkasse Berlin. (2005-). *SiBe-Report : Informationen für Sicherheitsbeauftragte.* Berlin: Unfallkasse Berlin.

Verband der Technischen Überwachungs-Vereine e.V. (1955-). *Technische Überwachung : Anlagensicherheit, Arbeits- und Gesundheitsschutz, Umweltschutz.* Düsseldorf: Springer-VDI-Verl.

Versicherungsmagazin : die Zeitschrift für Finanzdienstleistungen und Vertrieb. (2000-). Wiesbaden: Gabler.

von zur Mühlen, R. A. (2006). *Sicherheits-Management: Grundsätze der Sicherheitsplanung.* Stuttgart ; München et al.: Boorberg.

W & S : das Sicherheitsmagazin. (2002-). Munich: I.T.G., Informationsgesellschaft Technik.

WIK: Zeitschrift für die Sicherheit der Wirtschaft. (1987-). Gau-Algesheim: SecuMedia-Verl. ; Arbeitsgemeinschaft für Sicherheit in der Wirtschaft.

Wirtschaftsinformatik & Management : Ddie Praktikerzeitschrift für Wirtschaftsinformatiker. (2009-). Wiesbaden: Gabler/GWV-Fachverl.

Wirtschaftsinformatik : WI ; Organ der Fachbereichs Wirtschaftsinformatik der Gesellschaft für Informatik e.V. und der Wissenschaftlichen Kommission Wirtschaftsinformatik im Verband der Hochschullehrer für Betriebswirtschaft e.V. (1990-). Wiesbaden: Gabler.

Wissen Media Verlag GmbH. (2006). Wahrig Synonymwörterbuch. Munich.

Eidesstattliche erklärung – Affidavit

Hiermit versichere ich, dass ich die vorliegende Diplomarbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel verwendet habe.

Brandenburg an der Havel, den 29. November 2010

_____

(Unterschrift des Kandidaten)