

# Electronic Business Interoperability: Concepts, Opportunities and Challenges

Ejub Kajan  
*State University of Novi Pazar, Serbia*

Senior Editorial Director: Kristin Klinger  
Director of Book Publications: Julia Mosemann  
Editorial Director: Lindsay Johnston  
Acquisitions Editor: Erika Carter  
Development Editor: Myla Harty  
Production Coordinator: Jamie Snavelly  
Typesetters: Michael Brehm, Milan Vracarich, Jr. & Deanna Zombro  
Cover Design: Nick Newcomer

Published in the United States of America by  
Business Science Reference (an imprint of IGI Global)  
701 E. Chocolate Avenue  
Hershey PA 17033  
Tel: 717-533-8845  
Fax: 717-533-8661  
E-mail: [cust@igi-global.com](mailto:cust@igi-global.com)  
Web site: <http://www.igi-global.com/reference>

Copyright © 2011 by IGI Global. All rights reserved. No part of this publication may be reproduced, stored or distributed in any form or by any means, electronic or mechanical, including photocopying, without written permission from the publisher. Product or company names used in this set are for identification purposes only. Inclusion of the names of the products or companies does not indicate a claim of ownership by IGI Global of the trademark or registered trademark.

#### Library of Congress Cataloging-in-Publication Data

Electronic Business Interoperability : Concepts, Opportunities and Challenges / Ejub Kajan, editor.  
p. cm.

Includes bibliographical references and index.

Summary: "This book analyzes obstacles, provides critical assessment of existing approaches, and reviews recent research efforts to overcome interoperability problems in electronic business"--Provided by publisher.

ISBN 978-1-60960-485-1 (hardcover) -- ISBN 978-1-60960-486-8 (ebook) 1. Electronic commerce. 2. Internetworking (Telecommunication) 3. Electronic commerce--Computer programs. I. Kajan, Ejub, 1953- II. Title.  
HF5548.32.E335 2011  
658.4'03802854678--dc22

2010054241

#### British Cataloguing in Publication Data

A Cataloguing in Publication record for this book is available from the British Library.

All work contributed to this book is new, previously-unpublished material. The views expressed in this book are those of the authors, but not necessarily of the publisher.

## Chapter 24

# E–Business and Information Security Risk Management: Challenges and Potential Solutions

**Stefan Fenz**

*Vienna University of Technology, Austria*

### **ABSTRACT**

*For almost all private individuals and especially organizations, information technology (IT) including hardware, software, and data is an irreplaceable part of their everyday life/business. Thus, IT has to be protected in an adequate way to ensure that it delivers the expected services. Information security risk management (ISRM) helps to holistically protect the IT and to minimize their failure probability at reasonable costs. This chapter shows why ISRM is important for e-businesses, gives a brief overview about the ISRM history, describes current problems in ISRM, and presents novel ISRM methods as potential solutions to the stated problems. The chapter closes with an outlook on future ISRM research directions.*

### **INTRODUCTION**

Information technology including hardware, software, and data is an integral part of our everyday life and it has brought enormous benefits to almost every economic sector. Nowadays, people and especially organizations are heavily relying and

dependent on information technology (Commission of the European Communities, 2006). To ensure that our world is working as expected we have to protect IT components and the data which is stored on these components. The 2007 cyber attacks on the Estonian IT infrastructure and the July 2009 attacks on governmental websites of South Korea and the US have shown how vulnerable national IT infrastructures are.

DOI: 10.4018/978-1-60960-485-1.ch024

## **E-Business and Information Security Risk Management**

Information security breaches can cause serious harm to commercial organizations and studies have shown that even the stock price of an organization can be affected by information security breaches (cf. Campbell et al., 2003). According to Gefen et al. (2004) trust is especially important in the case of e-Commerce. Mahadevan (2004) proposed a three dimensional framework for defining e-business models. Within the framework, security and trust represent significant values to buyers and sellers. Both concepts are considered major concerns in e-business. Therefore, the author argues that risk management clearly increases the value of e-business operations for buyers and sellers. Besides several other components, trust and security depend on an established and maintained IT-security program which protects hardware, software, and data. Ideally the IT-security program is based on a comprehensive information security risk analysis. In that way sellers can efficiently protect their assets to prevent income loss, and buyers can make sure that their data is processed and stored in a secure way. Forrester Research estimated the IT-security costs of organizations in 2007 to over 100 billion USD worldwide. The Verizon 2009 Data Breach Investigations Report examined 90 confirmed breaches comprising over 285 million sensitive data records (Baker et al., 2009). 87% of these breaches were considered avoidable through simple or intermediate controls. Here Information security risk management (ISRM) comes in. ISRM provides organizations tools and processes to estimate the risk level of their resources<sup>1</sup> and to identify measures to mitigate the risk to an acceptable level. Although, ISRM has been used in the research and industrial field for over 30 years it is still linked to several problems. Therefore, the objectives of this chapter are: (i) to introduce the reader to ISRM, (ii) to give a brief overview about the ISRM history, (iii) to describe current problems in ISRM, (iv) to present novel

ISRM methods as potential solutions to the stated problems, and (v) to provide an outlook to future research directions.

## **BACKGROUND**

Generally risk is defined as the probability per unit time of the occurrence of a unit cost burden (Sage and White, 1980). In the information security context risk is defined as a function of the likelihood of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization (Stoneburner et al., 2002). As the security measures which are necessary to lower the risk are almost always associated with costs, organizations strive for those measures which are capable to reduce the risk to an acceptable level at the lowest possible costs. ISRM addresses exactly these issues and was defined by the National Institute of Standards and Technology (NIST) in Special Publication 800-30 as the process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support their organizations' mission (Stoneburner et al., 2002). Information security risk management represents a crucial element in ensuring a long-term business success and numerous approaches to implementing an adequate information security risk management strategy have been proposed. Although the definition above was published in 2002 we have to keep in mind that information security risk management is not a new domain. The history of information security risk management shows that people are researching in that field for over 30 years. Standards and best-practice guidelines are available and implemented in many organizations. So why be any longer concerned about information security risk management?

It was 1975 when the U.S. National Bureau of Standards proposed the Annual Loss Expectancy (ALE) as a metric for measuring computer-related

risks in (FIPS, 1975). The Annual Loss Expectancy is calculated by summing up the products of impact and frequency of harmful outcomes. One shortcoming of this early approach is the fact that it does not distinguish between highly frequent, low impact events and rare, high impact events. In the 1980s it was again the U.S. National Bureau of Standards, which pushed on the efforts in the risk management domain (Soo Hoo, 2000). In a series of workshops they developed an iterative process for information security risk management which consists of the steps: identification of the requirements (asset values, threats, vulnerabilities, existing safeguards, etc.); analysis of threats, vulnerabilities and the scenario; risk measurement; acceptance test; and safeguard selection and implementation (Soo Hoo, 2000). Although the information security risk management approaches of the following years provided some additional steps or different process structures, they are mainly based on this approach developed in the 1980s. A combination of qualitative and quantitative risk analysis methodologies has been proposed by Rainer et al. (1991) and comprises the identification of organizational value activities; identification of the IT component of each value activity; identification of linkages among value activities and IT component that supports each; determination of IT assets that support interorganizational linkages; determination of the value of IT assets; identification of possible threats; identification of the vulnerability of assets to threats; and determination of the overall IT risk exposure. The security risk planning model by Straub and Welke (1998) includes the recognition of security problems; risk analysis (threat identification and risk prioritization); alternatives generation (generation of solutions which are able to mitigate the risk); decisions (selection and prioritization of security projects); and implementation. Besides general risk management frameworks, several information security investment decision support methods, which are an integral part of several risk management methodologies, have been proposed

(cf. Finne (1998a,b); Gordon and Loeb (2002); Arora et al. (2004); Cavusoglu et al. (2004)). In 2008, the PCR (perceived composite risk) metric was introduced by Bodin et al. (2008). Their approach extends the traditional ALE by combining it with the expected severe loss and the standard deviation of the loss, and provides organizations with an additional decision support tool for information security investments. To make these academic approaches usable to organizations, some of them have been used as a foundation for today's information security risk management methods, standards and best-practice guidelines (e.g. CRAMM (Farquhar, 1991), NIST SP800-30 (Stoneburner et al., 2002), CORAS (Fredriksen et al., 2002), OCTAVE (Alberts et al., 2003), EBIOS (DCSSI, 2004), and recently ISO 27005 (ISO/IEC, 2007)).

### **Current ISRM Problems**

Recent studies (e.g. Straub and Welke (1998)) have shown that the lack of information security knowledge at the management level is one reason for inadequate or non-existing information security risk management strategies and that raising management's information security awareness and knowledge level leads to more effective strategies. Smith and Spafford (2004) and PITAC (2005) identified information security risk management as one of the top ten grand challenges in information technology security and demanded sound theories and techniques to support and enhance existing risk management approaches. In 2006, the European Network and Information Security Agency (ENISA) addressed these issues in (ENISA, 2006) and rated the establishment of unified information bases for information security risk management and the need for risk measurement methods as high priority issues. Aime et al. (2007) shortly afterwards attested the lack of a set of well-defined formal models for supporting the information security risk management process in 2007. According to

the 2008 Information Security Breaches Survey (BERR, 2008), only 48% of 1,007 interviewed UK organizations formally assess information security risks. To date such organizations have mostly relied on off-the-shelf software solutions, best-practice guidelines, information security standards, and/or domain experts to conduct the risk assessment and mitigation phases. However, problems are linked to these approaches:

- Best-practice guidelines provide excellent knowledge about potential threats, vulnerabilities, and controls, but without an information security domain expert the organization is not always able to consider all the complex relationships between all the relevant information security concepts, with the result of an inadequate information security approach which endangers the performance of the organization's mission (Vitale, 1986; Bandyopadhyay and Mykytyn, 1999; Jung et al., 1999; Baker and Wallace, 2007)
- To identify the concrete infrastructure elements which are endangered by certain threats the organization has to manually combine the knowledge from best-practice guidelines with their actual infrastructure (Baskerville, 1993)
- Especially information security standards only state very abstract implementation suggestions for risk mitigation; concrete controls or combinations thereof are mostly missing, leading to inefficient risk mitigation strategies (Siponen 2006; Baker et al., 2007)
- The determination of threat probabilities is predominantly based on subjective perceptions and not an objective evaluation (Frosdick, 1997; Bandyopadhyay and Mykytyn, 1999; Baker et al., 2007)

Regardless of which information security risk management methodology is considered,

it always includes the assessment of business crucial assets and the assessment of potential threats, corresponding vulnerabilities and controls which are able to minimize the risk to an acceptable level (Baskerville, 1993). While intensive knowledge about the organization itself and the entire information security domain is fundamental to the presented approaches (Jung et al., 1999), only little research has been conducted on the formal knowledge representation of the domains which are relevant to information security risk management (cf. Schumacher (2003); Kim et al. (2005); Herzog et al. (2007)). To elaborate on the ISRM-specific requirements we abstract existing ISRM methodologies in a first step.

### **Abstracting Existing ISRM Methodologies**

To abstract existing ISRM methodologies and to identify their similarities we analyzed and compared the risk management methodologies (i) CRAMM, (ii) NIST800-30, (iii) OCTAVE, (iv) EBIOS, and (v) ISO27005. At the analysis we focused on the activities of each phase as described in the corresponding documentation. Every information security risk management methodology requires the inventory and security classification of the relevant infrastructure elements and the identification of the organizations' missions and goals in a first phase. From a high-level perspective, the subsequent phases always require the identification of threats and the corresponding vulnerabilities to determine the threat probability together with already implemented controls, which is required in combination with the results of the impact analysis to determine the actual risk. The circumstance that the considered methodologies share a lot of commonalities and only few differences allowed us to create generic information security risk management phases, which represent the considered methodologies from a high-level perspective:

1. **System Characterization:** Definition of the system boundaries and assets used and/or required by the defined system → requires the systematic inventory of tangible (e.g., persons or physical assets) and intangible (e.g., data or software) assets → determination of the acceptable risk level for each inventoried asset.
2. **Threat and Vulnerability Assessment:** This phase requires the determination of potential threats, corresponding threat origins and vulnerabilities. A security requirements checklist, which can be used for a compliance evaluation regarding current and/or planned controls, is required for the subsequent risk determination.
3. **Risk Determination:** This phase determines amongst others the probability of a threat exploiting a certain vulnerability in the given system. The subsequent impact analysis determines the impact on the organization's ability to perform its mission, if a threat should successfully exploit a certain vulnerability. By combining the threat probability with the magnitude of the impact, the organization is able to determine the risk level and thus to plan the necessary actions.
4. **Control Identification:** Elaborates, by considering already implemented controls, on additional control implementations which could mitigate or reduce the risks to an acceptable level.
5. **Control Evaluation and Implementation:** Evaluates identified control implementations or combinations thereof regarding their cost/benefit ratio. Those control implementations which are suitable to mitigate the risk to an acceptable level at the lowest possible costs are incorporated in the control implementation plan.

Aligning our research activities to these generic phases ensures that the research results can be applied to a broad range of existing information

security risk management methodologies. The following sections elaborate on current approaches to supporting information security risk management and define, based on their identified shortcomings, the requirements to holistically support the entire information security risk management process.

## **CURRENT APPROACHES TO SUPPORTING INFORMATION SECURITY RISK MANAGEMENT**

Since most information security risk management methodologies only slightly differ from a high-level perspective, most of the following approaches are not exclusively designed for supporting a certain methodology. The described approaches are not mutually exclusive or limited to a certain phase of an information security risk management methodology.

**Spreadsheet approaches:** One common approach to support information security risk management efforts is based on simple spreadsheet documents which are used to catalog existing assets, threats, and vulnerabilities including their corresponding attributes, without installing additional programs or databases. Most people are acquainted with spreadsheet technologies, and organizations often prefer these solutions as the further processing of the content is quite easy. In addition, spreadsheet programs offer a broad range of mathematical functions and thus allow for simple quantitative approaches. Analysts can create their own templates and adapt them to the organization's needs, use freely available versions, or purchase one of the many commercial solutions. In most cases the spreadsheets include questionnaires containing questions like "Are regular tests made of the effective capacity to restore data and restart application after an incident?". For each question the user fills in the implementation status (yes or no), weight (numerical value), and potential comments (free text). The organization-wide risk level is finally based on the entire answer

set, i.e. on the implementation status of each security control and its subjective importance (weight). However, growing amounts of data and increasing functionality lead to a significant overhead necessary for maintaining up-to-date and accurate files. Furthermore, the spreadsheet solution lacks an established underlying data model including interrelations. Therefore, it is difficult to efficiently query data and express reusable domain knowledge. Without a formal basis it is not possible to verify the correctness of the modeled data (e.g., detect inappropriate controls, such as the definition of an anti-virus program as a control implementation for the threat of fire) or to automatically enrich or infer new knowledge (e.g., newly added assets should be automatically connected to threats based on their asset classification).

**Questionnaires:** Checklist-based approaches are another possibility to support information security risk management. The assigned employee completes a questionnaire that reveals potential weaknesses and provides corresponding security recommendations. The questions as well as the predefined sets of recommendations are often based on best-practice guidelines. One weakness of checklists is that they usually offer general, high-level recommendations and, thus, cannot support organization specific threat scenarios. Furthermore, there is no underlying data model that makes connections between the involved entities explicit and allow for modification and reuse.

**Hazard and operability studies (HAZOPS):** Some information security risk management methodologies (e.g., CORAS (Fredriksen et al., 2002)) incorporate HAZOP in the phases system characterization, threat and vulnerability assessment, and risk determination. HAZOP is a structured brainstorming exercise in which a multi-disciplinary expert team systematically considers defined assets and their intention. Guide words (e.g., ‘not’, ‘more’, ‘less’) and parameters (e.g., ‘throughput’) are defined to assess possible

operation deviations and potential consequences of any deviations.

**Failure modes, effects and criticality analysis (FMECA):** In contrast to HAZOP, FMECA is conducted by an individual expert who identifies failure modes or design weaknesses of a given system. Each functional component and sub-system of the considered system is considered to identify potential failure modes. The consequences of each identified failure mode are considered at the sub-system and overall system level respectively (Frosdick, 1997). As FMECA commonly uses spreadsheet approaches to manage the gathered expert knowledge, a formal basis of the gathered knowledge is not given, resulting in the typical drawbacks of spreadsheet approaches.

**Fault tree analysis (FTA):** Fault trees show how a system failure might occur. An expert team identifies lower-level events (fault enablers) and their probabilities and combines them by Boolean logic to analyze an undesired top-level event (fault) of a system. After constructing the fault tree the risk manager is able to improve the security status of the given system by lowering the probability of the identified lower-level events.

**Off-the-shelf solutions:** Software solutions incorporating several of the approaches described above and supporting entire information security risk management methodologies (e.g., CRISAM Explorer by Calpana, GSTool by the German Federal Office for Information Security, CRAMM by Insight Consulting or EBIOS by the French DCSSI) are a further possibility to support information security risk management. These solutions support users in preparing, administrating, and updating information security concepts that meet the requirements of the corresponding methodology. After having modeled the organization’s assets relevant to information security, the solutions offer predefined threats and connected controls for the various asset classes. Although these approaches are sophisticated, their underlying data structures are proprietary and thus difficult to apply in different contexts, hindering standard-

ized and collaborative information security risk management.

## **Requirements**

The support approaches described previously, best-practice guidelines, information security standards, and expert knowledge can support organizations in the risk assessment and mitigation phases. Regardless of which of the existing support approaches is used, each organization has to invest a great deal of time and money in manually dealing amongst others with the following questions: (1) What are potential threats for my organization?, (2) How probable are these threats?, (3) Which vulnerabilities could be exploited by such threats?, (4) Which controls are required to most effectively mitigate these vulnerabilities?, and (5) What is the potential impact of a particular threat? According to the generic information security risk management phases we defined the requirements to address the drawbacks of existing support approaches in the phases: (i) system characterization, (ii) threat and vulnerability assessment, and (iii) risk determination. In the risk determination phase we are only addressing the probability determination. The phases control identification and control evaluation are not in the scope of the following requirements assessment.

## **General Requirements**

- Organizations in the same business field and in a similar geographical location often come up with similar answers to most of the questions mentioned above. Therefore, a knowledge base capable to store information security relevant knowledge is required.
- The knowledge base has to allow the incorporation of general information security domain knowledge (e.g. what are potential threats and how can corresponding vulnerabilities be mitigated) and specific knowl-

edge about the considered organization to allow the automatic determination of its current information security status (Jung et al., 1999). As pointed out by Ghillon et al. (2001) the knowledge base has to incorporate not only technical but also organizational and human-centered information security aspects.

- The knowledge has to be represented formally to ensure automatic reasoning (Aime et al., 2007).
- Many organizations carry out certification initiatives especially in sensitive business sectors (e.g., financial or health sector) or to comply with legal regulations (e.g. Basel II, Sarbanes Oxley Act), but complain about high costs, the bureaucratic certification process and the lack of methods for measuring the cost/benefit ratio (BERR, 2008). To ensure automatic compliance checks, controls have to be derived from existing best-practice guidelines and information security standards.
- Controls and their fulfillment requirements have to be expressed formally to ensure automatic compliance checks. As every asset of the organization can be used for fulfilling an information security control, the knowledge model has to express fulfillment requirements formally by incorporating available asset concepts.

## **System Characterization**

- To comprehensively map the assets of the organization to the knowledge model, it has to incorporate concepts for tangible (e.g., persons or physical assets) and intangible (e.g., data or software) assets respectively (cf. Stoneburner et al. (2002)).
- Relations between asset concepts have to ensure that the physical and virtual location of each asset can be described formally in the knowledge model to determine to

which extent existing control implementations are protecting the asset.

### Threat and Vulnerability Assessment

- To holistically model the information security domain, the knowledge model has to incorporate the concepts threat, vulnerability, and control (cf. Stoneburner et al. (2002)).
- Relations have to explicitly express the dependencies between information security concepts (e.g., assets, vulnerabilities, threats, controls) to explicate the effects of concrete control implementations on the security status of the organization.

### Risk Determination

- The knowledge model has to incorporate a priori threat probabilities (e.g. crime statistics of different cities) which are required to determine an organization-specific posterior threat probability (cf. ISO/IEC (2007)).
- Based on existing control implementations posterior threat probabilities have to be calculated automatically.

## **SOLUTIONS AND RECOMMENDATIONS**

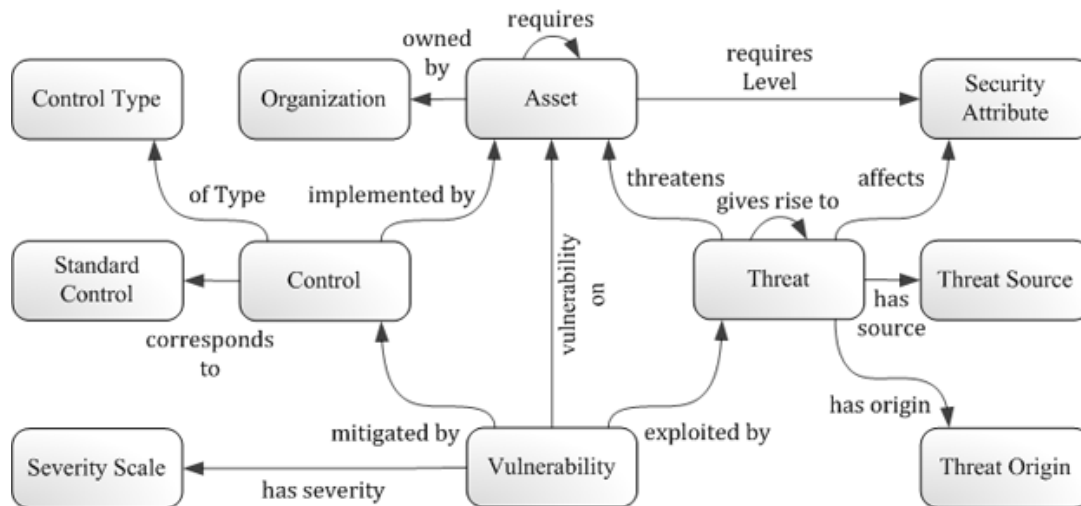
According to these requirements we aimed at developing novel techniques to efficiently gather comprehensive knowledge about the information security domain and the actual organization and provide it in a formal form to support a broad range of information security risk management methodologies. By developing a formal knowledge model, establishing a corresponding knowledge base and developing novel threat probability determination techniques we addressed the stated requirements.

Ontologies are able to elegantly address the stated requirements. They provide concepts to formally describe a domain, which is fundamental for meeting the stated requirements in order to holistically support information security risk management. According to Studer et al. (1998) “an ontology is a formal, explicit specification of a shared conceptualization. A conceptualization refers to an abstract model of some phenomenon in the world by having identified the relevant concepts of that phenomenon. Explicit means that the type of concepts used, and the constraints on their use are explicitly defined. Formal refers to the fact that the ontology should be machine readable, which excludes natural language. Shared reflects the notion that an ontology captures consensual knowledge, that is, it is not private to some individual, but accepted by a group.” (Studer et al., 1998)

### **The Security Ontology: A Formal Information Security Knowledge Base**

As the previous chapters have shown, a conceptual and formal model of information security is required for supporting the information security risk management process in an automated way. Ontologies are one possibility for modeling the information security domain in order to make it accessible to machines. Therefore, we proposed the security ontology based on the security relationship model described in the National Institute of Standards and Technology Special Publication 800-12. Figure 1 shows the high-level concepts and corresponding relations of our ontology (cf. Fenz and Ekelhart (2009) for further details regarding the ontology). A threat gives rise to follow-up threats, represents a potential danger to the organization’s assets and affects specific security attributes (e.g. confidentiality, integrity, and/or availability) as soon as it exploits a vulnerability in the form of a physical, technical, or administrative weakness. Additionally each threat

Figure 1. Security ontology: top-level concepts and relationships



is described by potential threat origins (human or natural origin) and threat sources (accidental or deliberate source). For each vulnerability a severity value and the asset on which the vulnerability could be exploited is assigned. Controls have to be implemented to mitigate an identified vulnerability and to protect the respective assets by preventive, corrective, deterrent, recovery, or detective measures (control type). Each control is implemented as asset concept, or as combinations thereof. Controls are derived from and correspond to best-practice and information security standard controls (e.g. the German IT Grundschutz Manual (BSI, 2004) and ISO/IEC 27001 (ISO/IEC, 2005)) to ensure the incorporation of widely accepted knowledge. The controls are modeled on a highly granular level and are thus reusable for different standards. When implementing the controls, a compliance with various information security standards is implicit. The coded ontology follows the OWL-DL (W3C Web Ontology Language) (W3C, 2004) standard and ensures that the knowledge is represented in a standardized and formal form. The formal representation of the information security knowledge enables its utilization by automated systems, which is described as

one of the most important knowledge management issues according to King et al. (2002).

According to the stated requirements the security ontology allows the incorporation of general information security domain knowledge (threats, vulnerabilities, controls, security attributes, etc.) and specific knowledge about the considered organization. Threats, vulnerabilities, and controls are related to each other. Obvious effects (e.g. threat gives rise to another threat, or threat exploits vulnerability) are explicitly described. The organization is mainly modeled within the organization and asset concepts, their sub-concepts and corresponding relations. To comprehensibly map the assets of the organization to the ontology, concepts for tangible (e.g., persons or physical assets) and intangible (e.g. data or software) assets have been incorporated into the ontology. Physical and virtual asset locations can be described by ontological relations. The entire ontology is coded with OWL enabling automatic reasoning and machine-readability. Formal control descriptions included within the control concepts have been derived from best practice guidelines and information security standards, enabling the usage of the ontology for compliance checks. The security ontology supports existing ISRM meth-

odologies at the abstract phases System Characterization, Threat and Vulnerability Assessment, and Risk Determination.

### **Bayesian Threat Probability Determination**

Based on the security ontology which is used to generate the actual calculation model this section describes a statistical model to determine threat probabilities based on (i) existing control implementations, (ii) the effectiveness of the attacker, (iii) the a priori threat probability, and (iv) relations to corresponding threats. Moreover, this section examines how the security ontology is utilized to build Bayesian networks to support the threat probability determination. The reasons for choosing Bayesian networks for the threat probability determination are: (1) reduction of the calculation complexity, (2) the possibility to incorporate interdependencies into the calculation schema, (3) result consistency, and (4) calculation efficiency.

According to Heckerman (1996), the initial tasks when creating a Bayesian network include: (1) the identification of the goals of modeling, (2) the identification of existing observations which are potentially relevant to these goals, (3) the determination of the most relevant subset, and (4) the organization of the observations into variables which have mutually exclusive states. While the goal, a more objective threat probability determination, is quite clear, this section more extensively addresses the selection of the necessary variables. Since holistic databases about threat occurrence rates are not available, relevant variables for threat probability determination had to be derived manually from existing best-practice guidelines.

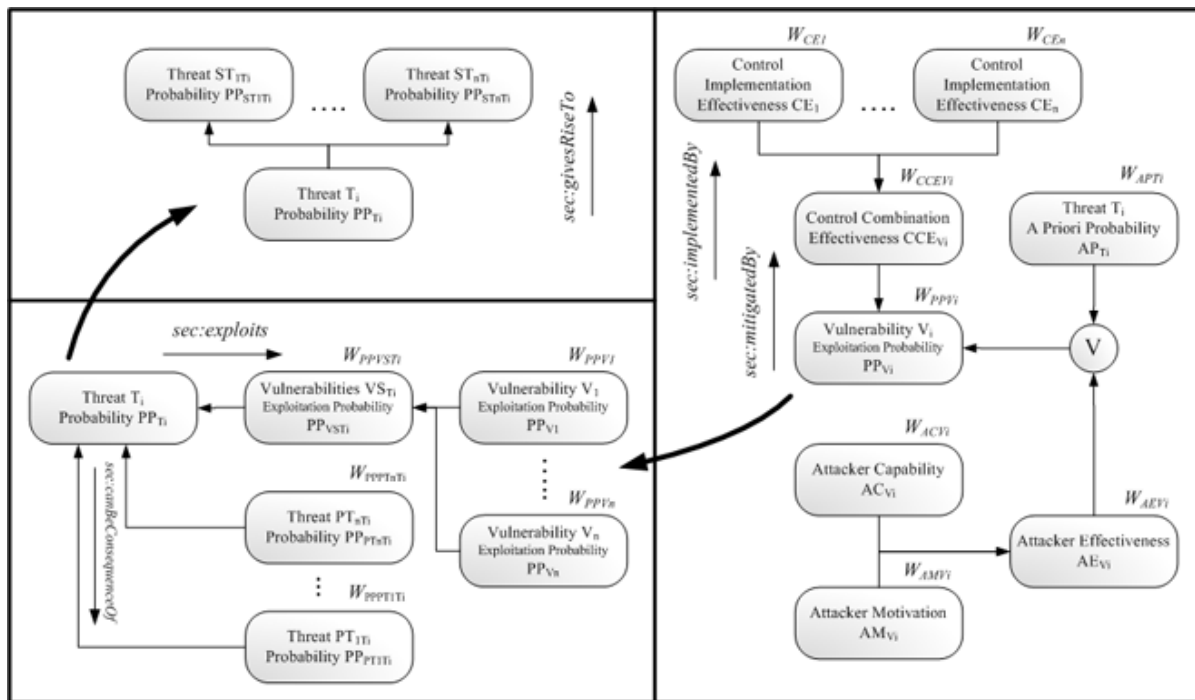
T is assumed to be the set of variables  $\{T_1, T_2, \dots, T_n\}$  representing the threats which probabilities have to be determined. It is assumed that each threat has exactly one of a finite set of probability states (expressed as a vector, representing the probability distribution among distinct states, e.g.

high, medium, and low). Since the threat probability or influencing factors cannot be determined quantitatively, a qualitative rating is used in this approach. The main problem of quantitative methods is that they pretend an accuracy which cannot be achieved by current estimation approaches (OCG, 2007). In contrast to a quantitative rating with which it is hardly possible to determine the occurrence of a certain threat with a 67% and not with a 68% chance, a qualitative rating (e.g. high, medium, and low) is a more human way of estimating or handling a probability. To enable humans to provide the necessary input and to understand the corresponding output respectively, clear definitions for every possible variable state in the Bayesian network were provided according to Druzdzel (1996). For each variable a three-point Likert scale (Likert, 1932) was defined to capture the subjective impressions on the input variables and to represent the results on the intermediate and output variables. The Likert scale was used since it represents an ordinal scale which allows ranking the scale characteristics (Diekmann, 2007).

As already mentioned, the objective of the Bayesian network is to determine the probability of threats taking various influence factors into account. Therefore, the following factors have been identified:

1. predecessor threats ( $PT_{1Ti}, \dots, PT_{nTi}$ ) influence the considered threat ( $T_i$ ) which influences its successor threats ( $ST_{1Ti}, \dots, ST_{nTi}$ ); therefore dependencies amongst a given threat set T had to be considered (see the upper left section in Figure 2),
2. according to Stoneburner et al. (2002), each threat ( $T_i$ ) requires one or more vulnerabilities ( $V_1, \dots, V_n$ ) to become effective; thus the existence of unmitigated vulnerabilities significantly influences the threat probability (see the lower left section in Figure 2),
3. controls can be used to mitigate identified vulnerabilities, while the mitigation depends on the effectiveness of a potential control

Figure 2. Bayesian network for threat probability determination



- combination ( $CCE_{V_i}$ ) which again depends on the actual effectiveness of the controls which are used in this combination ( $CE_1, \dots, CE_n$ ), and
- (a) in the case of deliberate threat sources, the vulnerability exploitation probability ( $PP_{V_i}$ ) is determined by the effectiveness of a potential attacker ( $AE_{V_i}$ ) which is again determined by the motivation ( $AM_{V_i}$ ) and the capabilities ( $AC_{V_i}$ ) of the attacker as stated in (ISO/IEC, 2007), (b) in the case of accidental threat sources and/or natural threat origins, the vulnerability exploitation probability ( $PP_{V_i}$ ) is determined by the a priori probability ( $AP_{T_i}$ ) of the corresponding threat ( $T_i$ ) (see the right section of Figure 2).

Figure 2 shows the proposed model for determining threat probabilities by taking the aforementioned factors into consideration. It should be noted that the risk manager merely has to rate the nodes for the attacker’s motivation  $AM_{V_i}$  and the

attacker’s capabilities  $AC_{V_i}$ . Further input, such as the control implementation effectiveness  $CE_i$  and the calculation schemes for every intermediate node, is derived from the security ontology. The result for each threat probability is represented as a distribution of the chosen rating scale (e.g. high, medium, and low).

After introducing the formalisms of the Bayesian threat probability determination, the connection to the security ontology framework, which provides a foundation to enrich the Bayesian network with concrete knowledge is described. Since the security ontology provides detailed knowledge about threat, vulnerability, and control dependencies, this knowledge could be utilized to build up the Bayesian network for the threat probability determination. Figure 2 gives an overview of the connections between the proposed Bayesian threat probability determination and the security ontology.

First of all, a threat net, including the relations between the threats and their a priori threat prob-

ability will be set up. Since each threat modeled in the security ontology is connected by the security ontology relation `sec:givesRiseTo` to follow-up threats (see Figure 2) the corresponding threat net can easily be created. The a priori threat probability vector for each threat  $T_i$  is also derived from the security ontology, depending on the actual physical location of the organization. The `sec:Probability` concept and the `sec:probabilityDistribution` property of the security ontology connect each threat of a given physical location with its a priori probability. Since weights for all threat probability influencing factors (influencing threats and vulnerabilities) are necessary, they are distributed equally. For example, if one threat was influenced by two threats, the weight for each influencing factor, namely the two influencing threats and the vulnerabilities node, would be 0.3333. Tuning these default weights is of course possible, if necessary.

For each threat the approach has to determine the corresponding vulnerabilities. In the security ontology this relationship is modeled by the `sec:exploits` relation (see Figure 2) which allows revealing the vulnerabilities of a given threat. As the vulnerabilities vector is determined by single vulnerabilities and their weights, the weight of each vulnerability which influences the intermediate vulnerabilities vector was determined. Since the security ontology provides a severity rating  $S_{v_i}$  for each vulnerability (high (3), medium (2), and low (1)), a numerical weight for each vulnerability can be determined by dividing the severity of the considered vulnerability by the severity sum of all vulnerabilities relevant to the threat.

The exploitation probability of each vulnerability variable is determined by (1) the effectiveness of the implemented control combination, (2) the attacker's effectiveness in the case of a deliberate threat source or by the a priori threat probability in the case of an accidental threat source. By default all components are weighted equally. While the attacker's effectiveness and the a priori threat probability are not rated on an asset-specific

level, the control combination effectiveness is determined specifically for the considered asset. Therefore, reasoning algorithms query the security ontology regarding those control implementations effectiveness values which are relevant for the considered asset/vulnerability combination (e.g. the effectiveness of the antivirus solution installed on certain PC to determine together with further input factors the malware affliction threat probability).

With the security ontology relation `sec:mitigatedBy` (see Figure 2) the required control implementation combination which is necessary to mitigate the given vulnerability can be derived. Since each implementation in the recommended control combination has a different effectiveness, its weight differs dependently on the implementation's importance for the current control combination. The security ontology concept `sec:ControlImplementation` represents the effectiveness for each control/implementation combination by a three-point Likert scale (high, medium, low).

## Example

Figure 3 shows a simplified example network for calculating the posterior probability of the "unauthorized physical access" threat. Each node presents the probability by a distribution on a three-point Likert scale (high, medium, and low). The grey nodes represent knowledge facts such as a prior probabilities or control implementation effectiveness values which have been derived from the security ontology. As depicted the "unauthorized physical access" threat probability depends on its a priori probability and the posterior probability of the "break-in" threat. The "break-in" threat probability is determined by its a priori probability and exploitation probabilities of the vulnerabilities "no intrusion alarm system" and "no entrance control". Both vulnerability exploitation probabilities are influenced by the (i) attacker's effectiveness, (ii) the effectiveness



the ISRM process. By using machine-readable knowledge models we enable the centralized collection and decentralized usage of information security knowledge. Based on that knowledge the Bayesian threat probability determination enables security professionals to comprehensively determine threat probabilities.

## **FUTURE RESEARCH DIRECTIONS**

As discussed, the developed security ontology and the corresponding Bayesian threat probability determination method are only the first steps to address current ISRM problems. The following research directions should be addressed by the research community to tackle the remaining issues.

### **Research Direction 1: Systematically Assessing ISRM Needs**

First, it is necessary to assess the specific needs of people working in the ISRM field. What are their main problems at their day-to-day work and which technologies can be used to make their work more efficient and reliable? As organization- and information security-specific knowledge is the fundamental issue in ISRM such an assessment has to focus on the corresponding knowledge management issues. Who requires which type of knowledge from whom? How is willing to share its knowledge under which circumstances? Is there a common knowledge baseline such as information security best-practice guidelines or standards?

Only if we have profound knowledge about these and related ISRM needs we can address them by developing technology which helps people at conducting the necessary ISRM activities.

### **Research Direction 2: Extending ISRM Knowledge Bases**

Based on the results of Research Direction 1, ISRM knowledge bases such as the presented security

ontology have to be extended by additional reliable and accepted sources such as best-practice guidelines and information security standards. Besides this static knowledge component they also have to allow the incorporation and management of dynamic and probably conflicting expert knowledge. The questions in the context of this research direction are: How can existing information security knowledge sources be mapped and concentrated in one formal knowledge base? Which extensions are required to allow the incorporation and management of conflicting expert knowledge?

### **Research Direction 3: Combining the Web 2.0 idea with ISRM Knowledge Management**

Based on a knowledge base containing broad but basic ISRM knowledge, we have to find methods to extend the knowledge in a collaborative way. While it would be feasible for one organization to initialize the knowledge base, it would be hardly possible to extend and maintain the knowledge base to all relevant ISRM knowledge domains. Therefore, we have to introduce the Web 2.0 idea into ISRM knowledge management. Similar to Wikipedia and based on a formal knowledge model such as the presented security ontology, people of different domains should be able to contribute to the knowledge base. In return, everybody would be able to use the available knowledge for his organization. To encourage people to contribute we have to develop incentive or knowledge trading systems. The main problem of such trading systems will be how to determine the quality and the corresponding value of knowledge. Another challenge will be how we deal with sensitive knowledge which can be used by competitors against the contributor (e.g. organization-specific vulnerabilities). Technologies such as anonymization<sup>2</sup> or pseudonymization<sup>3</sup> have to be combined with the knowledge base to protect contributors' interests.

## **Research Direction 4: ISRM Usability**

ISRM is also a communication tool, which transforms purely technical issues (e.g. absence of a virus scanner) to monetary terms compatible with the management mind set (e.g. associated risk measured in a certain currency). Therefore, it is extremely crucial to focus on the usability aspects of ISRM. Especially the ISRM result communication should be target group-specific. Therefore, we have to assess the usability needs of different target groups such as management, information security experts, or IT experts. Each target group requires a different visualization and result detail level to use the results for their decisions. Crucial results such as very high risks have to be visualized in a proper way to prevent that they are misinterpreted or simply overseen.

## **CONCLUSION**

Information technology is fundamental for our economical and private life, and developed as well as emerging markets would not be able to survive without IT. Information security risk management provides us a toolset to protect our IT from common threats by implementing appropriate and cost-efficient safeguards. Although, ISRM is now used for over 30 years it is still linked to several problems that have been discussed in this chapter. By abstracting the phases of existing information security risk management methodologies, developing a security ontology, and a Bayesian concept for threat probability determination this chapter addressed some of the identified problems. The security ontology enables the storage of ISRM-specific knowledge in a formal, reusable, and machine-readable knowledge base, helping organizations to reduce their costs for knowledge acquisition. The presented Bayesian threat probability determination method enables organizations to comprehensibly calculate organization-specific threat probabilities based on the knowledge stored

in the security ontology. The following future research directions have been identified: (i) systematically assessing ISRM-needs, (ii) extending ISRM knowledge bases, (iii) combining the Web 2.0 idea with ISRM knowledge management, and (iv) enhancing the usability in ISRM.

## **ACKNOWLEDGMENT**

This work was supported by grants of the Austrian Government's FIT-IT Research Initiative on Trust in IT Systems under the contract 813701 and was performed at the research center Secure Business Austria funded by the Federal Ministry of Economy, Family and Youth of the Republic of Austria and the City of Vienna.

## **REFERENCES**

- Aime, M., Atzeni, A., & Pomi, P. (2007). *AMBRA: Automated Model-Based Risk Analysis*. In *QoP '07: Proceedings of the 2007 ACM workshop on Quality of protection*. (pp. 43-48). New York: ACM.
- Alberts, C., Dorofee, A., Stevens, J., & Woody, C. (2003). *Introduction to the OCTAVE approach. Technical report*. Pittsburgh, PA: Carnegie Mellon - Software Engineering Institute.
- Arora, A., Hall, D., Pinto, C., Ramsey, D., & Telang, R. (2004). Measuring the risk-based value of IT security solutions. *IT Professional*, 6, 35-42. doi:10.1109/MITP.2004.89
- Baker, W., Hutton, A., Hylender, D., Novak, C., Porter, C., & Sartin, B. (2009). *2009 data breach investigations report*. Verizon Business.
- Baker, W., Rees, L., & Tippett, P. (2007). Necessary measures: Metric-driven information security risk assessment and decision making. [New York: ACM.]. *Communications of the ACM*, 50, 101-106. doi:10.1145/1290958.1290969

- Baker, W., & Wallace, L. (2007). Is information security under control?: Investigating quality in information security management. *IEEE Security and Privacy*, 5, 36–44. doi:10.1109/MSP.2007.11
- Bandyopadhyay, K., & Mykytyn, P. (1999). A framework for integrated risk management in Information Technology. *Management Decision*, 37, 437–444. doi:10.1108/00251749910274216
- Baskerville, R. (1993). Information Systems security design methods: Implications for Information Systems development. *ACM Computing Surveys*, 25, 375–414. doi:10.1145/162124.162127
- BERR. (2008). *2008 information security breaches survey. Technical report, Department for Business Enterprise and Regulatory Reform*. BERR.
- Bodin, L., Gordon, L., & Loeb, M. (2008). Information security and risk management. *Communications of the ACM*, 51, 64–68. doi:10.1145/1330311.1330325
- Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic severity of publicly announced information security breaches: Empirical evidence from the stock market. *Journal of Computer Security*, 11(3), 431–448.
- Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). A model for evaluating IT security investments. [New York: ACM.]. *Communications of the ACM*, 47, 87–92. doi:10.1145/1005817.1005828
- Commission of the European Communities. (2006). Communication from the Commission to the Council, The European Parliament, The European Economic and Social Committee and the Committee of the Regions ‘A strategy for a Secure Information Society - Dialogue, partnership and empowerment.
- DCSSI. (2004). *Expression des Besoins et Identification des Objectifs de Securite (EBIOS) - Section 2 – Approach*. General Secretariat of National Defence Central Information Systems Security Division (DCSSI).
- Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: Towards socio-organizational perspectives. *Information Systems Journal*, 11(2), 127–153. doi:10.1046/j.1365-2575.2001.00099.x
- Diekmann, A. (2007). *Empirische Sozialforschung. Grundlagen, Methoden, Anwendungen*. Rowohlt Taschenbuch.
- Druzdzal, M. (1996). Qualitative verbal explanations in Bayesian belief networks. *Artificial Intelligence and Simulation of Behaviour Quarterly*, 94, 43–54.
- ENISA. (2006). *Risk management: Implementation principles and inventories for risk management/risk assessment methods and tools. Technical report*. European Network and Information Security Agency.
- Farquhar, B. (1991). One approach to risk assessment. *Computers & Security*, 10, 21–23. doi:10.1016/0167-4048(91)90051-E
- Fenz, S., & Ekelhart, A. (2009). Formalizing information security knowledge. *Proceedings of the 4th ACM Symposium on Information, Computer, and Communications Security*, ACM, 2009, (pp. 183-194).
- Finne, T. (1998a). A conceptual framework for information security management. *Computers & Security*, 17, 303–307. doi:10.1016/S0167-4048(98)80010-2
- Finne, T. (1998b). The three categories of decision-making and information security. *Computers & Security*, 17, 397–405. doi:10.1016/S0167-4048(98)80045-X
- FIPS. (1975). *Guideline for automatic data processing risk analysis, Federal Information Processing Standards Publications (FIPS PUB) 65*. National Bureau of Standards.

- Fredriksen, R., Kristiansen, M., Gran, B. A., Stølen, K., Opperud, T. A., & Dimitrakos, T. (2002). *The CORAS framework for a model-based risk management process*. In SAFECOMP '02: *Proceedings of the 21st International Conference on Computer Safety, Reliability and Security*. (pp. 94-105). London: Springer-Verlag.
- Frosdick, S. (1997). The techniques of risk analysis are insufficient in themselves. *Disaster Prevention and Management*, 6, 165–177. doi:10.1108/09653569710172937
- Gefen, D., & Straub, D. W. (2004). Consumer trust in B2C e-commerce and the importance of social presence: Experiments in e-products and e-services. *International Journal of Management Science*, 32, 407–424.
- Gordon, L., & Loeb, M. (2002). The economics of information security investment. *ACM Transactions on Information and System Security*, 5, 438–457. doi:10.1145/581271.581274
- Heckerman, D. (1996). *A tutorial on learning with Bayesian networks*, Technical Report MSR-TR-95-06, Microsoft Research, Advanced Technology Division, Redmond, WA.
- Herzog, A., Shahmehri, N., & Duma, C. (2007). An ontology of information security. *International Journal of Information Security and Privacy*, 1, 1–23.
- ISO/IEC. (2007). ISO/IEC 27005:2007, Information technology - Security techniques – Information security risk management.
- Jung, C., Han, I., & Suh, B. (1999). Risk analysis for electronic commerce using case based reasoning. *International Journal of Intelligent Systems in Accounting Finance & Management*, 8, 61–73. doi:10.1002/(SICI)1099-1174(199903)8:1<61::AID-ISAF156>3.0.CO;2-6
- Kim, A., Luo, J., & Kang, M. (2005). *Security ontology for annotating resources* (pp. 1483–1499). OTM Conferences.
- King, W. R., Peter, V., Marks, J., & McCoy, S. (2002). The most important issues in knowledge management. [New York: ACM.]. *Communications of the ACM*, 45, 93–97. doi:10.1145/567498.567505
- Likert, R. (1932). A technique for the measurement of attitudes. *Archives de Psychologie*, 140, 1–55.
- Mahadevan, B. (2000). Business models for Internet-based e-commerce: An anatomy. *California Management Review*, 42(4), 55–69.
- OCG. (2007). *Österreichisches Informationssicherheitshandbuch (Austrian information security handbook)*, Bundeskanzleramt Österreich. Vienna, Austria: Federal Chancellery Austria.
- PITAC. (2005). *Cyber security: A crisis of prioritization-report to the president. Technical report*. President's Information Technology Advisory Committee.
- Rainer, R., Snyder, C., & Carr, H. (1991). Risk analysis for Information Technology. *Journal of Management Information Systems*, 8, 129–147.
- Sage, A., & White, E. (1980). Methodologies for risk and hazard assessment: A survey and status report. *IEEE Transactions on Systems, Man, and Cybernetics*, 10, 425–446. doi:10.1109/TSMC.1980.4308532
- Schumacher, M. (2003). *Security engineering with patterns-origins, theoretical model, and new applications*. Springer.
- Siponen, M. (2006). Information security standards focus on the existence of process, not its content. *Communications of the ACM*, 49(8), 97–100. doi:10.1145/1145287.1145316

Smith, S., & Spafford, E. (2004). Grand challenges in information security: Process and output. *IEEE Security & Privacy*, 2, 69–71. doi:10.1109/MSECP.2004.1264859

Soo Hoo, K. (2000). *How much is enough? A risk management approach to computer security*. Unpublished doctoral thesis, Stanford University.

Stoneburner, G., Goguen, A., & Feringa, A. (2002). *Risk management guide for Information Technology systems*. NIST Special Publication 800-30, National Institute of Standards and Technology. Gaithersburg, MD: NIST.

Straub, D., & Welke, R. (1998). Coping with systems risk: Security planning models for management decision making. *Management Information Systems Quarterly*, 22, 441–469. doi:10.2307/249551

Vitale, M. (1986). The growing risks of information systems success. *Management Information Systems Quarterly*, 10, 327–334. doi:10.2307/249185

## **ADDITIONAL READING**

Baker, W., Rees, L., & Tippet, P. (2007). 'Necessary measures: metric-driven information security risk assessment and decision making', *Communications of the ACM (Vol. 50, pp. 101–106)*. New York, NY, USA: ACM.

Baker, W., & Wallace, L. (2007). 'Is information security under control?: Investigating quality in information security management', *IEEE Security and Privacy (Vol. 5, pp. 36–44)*. Piscataway, NJ, USA: IEEE Educational Activities Department.

Baskerville, R. (1993). Information systems security design methods: Implications for information systems development. *ACM Computing Surveys*, 25, 375–414. doi:10.1145/162124.162127

Bodin, L., Gordon, L., & Loeb, M. (2008). Information security and risk management. *Communications of the ACM*, 51, 64–68. doi:10.1145/1330311.1330325

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). 'A model for evaluating IT security investments', *Communications of the ACM (Vol. 47, pp. 87–92)*. New York, NY, USA: ACM.

Farquhar, B. (1991). One approach to risk assessment. *Computers & Security*, 10, 21–23. doi:10.1016/0167-4048(91)90051-E

Finne, T. (1998a). A conceptual framework for information security management. *Computers & Security*, 17, 303–307. doi:10.1016/S0167-4048(98)80010-2

Finne, T. (1998b). The three categories of decision-making and information security. *Computers & Security*, 17, 397–405. doi:10.1016/S0167-4048(98)80045-X

Gordon, L., & Loeb, M. (2002). The economics of information security investment. *ACM Transactions on Information and System Security*, 5, 438–457. doi:10.1145/581271.581274

Sage, A., & White, E. (1980). *Methodologies for risk and hazard assessment: A survey and status report*. *IEEE Transactions on Systems, Man, and Cybernetics, SMC-10*, 425–446. doi:10.1109/TSMC.1980.4308532

Straub, D., & Welke, R. (1998). *Coping with systems risk: Security planning models for management decision making*. *Management Information Systems Quarterly*, 22, 441–469. doi:10.2307/249551

Studer, R., Benjamins, V. R., & Fensel, D. (1998). Knowledge engineering: Principles and methods. *Data & Knowledge Engineering*, 25, 161–197. doi:10.1016/S0169-023X(97)00056-6

Vitale, M. (1986). The growing risks of information systems success. *Management Information Systems Quarterly*, 10, 327–334. doi:10.2307/249185

## KEY TERMS AND DEFINITIONS

**Bayesian Network:** A directed acyclic graph. The nodes of the graph represent relevant variables of the problem domain and links between the nodes connect dependent variables. Conditional probability tables in each node enable the calculation of conditional probabilities for each node by taking the state of its parent node(s) into account.

**Information Security Risk Management:** A methodology which enables organizations to select cost-efficient safeguards to reduce the risk for their resources to an acceptable level.

**Ontology:** Machine-readable specification of a knowledge domain consisting of formal concepts, relations, and individuals.

**Security Ontology:** A formal knowledge model describing the information security domain and a formal knowledge base providing knowledge

about threats, vulnerabilities, controls, and control implementation effectiveness values.

**Threat Probability:** Probability that a threat realizes. The probability is influenced by its a priori probability, the probability of its predecessor threats, and the exploitation probability of the vulnerabilities which can be exploited by the threat.

## ENDNOTES

- <sup>1</sup> In the context of this chapter the term resources includes the hardware, software, and information of an organization.
- <sup>2</sup> Anonymized data does not contain any data which can be used to associate a certain person with the considered data (e.g. removing personal-related data from electronic health records).
- <sup>3</sup> Pseudonymization removes identifying data (e.g. names or social insurance numbers) and replaces it with a pseudonym. Only under specified and controlled circumstances it is possible to associate the pseudonyms with the original personal data.