Potential Rating Indicators for Cyberinsurance: An Exploratory Qualitative Study

Frank Innerhofer–Oberperfler, Ruth Breu

Research Group Quality Engineering
Institute of Computer Science, University of Innsbruck
A–6020 Innsbruck, Austria
{frank.innerhofer-oberperfler, ruth.breu}@uibk.ac.at

Abstract. In this paper we present the results of an exploratory qualitative study with experts. The aim of the study was the identification of potential rating variables which could be used to calculate a premium for Cyberinsurance coverages. For this purpose we have conducted semi-structured qualitative interviews with a sample of 36 experts from the DACH[1] region. The gathered statements have been consolidated and further reduced to a subset of indicators which are available and difficult to manipulate. The reduced set of indicators has been presented again to the 36 experts in order to rank them according to their relative importance. In this paper we describe the results of this exploratory qualitative study and conclude by discussing implications of our findings for both research and practice.

1 Introduction

The increased dependency on information technologies poses a variety of risks to organisations. The Congressional Research Service Report for Congress summarises some surveys estimating the losses due to cyber attacks ranging *"[...] from $13 billion (worms and viruses only) to $226 billion (for all forms of overt attacks)"* [1]. Particularly since the Internet and the continuing cross-linking of information systems have become a backbone of modern business the headlines are constantly filled with news about devastating information security incidents. The resulting potential loss of reputation or brand image is a major driver for information security [2].

But not only the potential economic impact of information security moved the topic on the agenda of executives, where it continues to rise [3]. Especially the need to be compliant with the emerging regulatory landscape of the recent years (eg. Sarbanes-Oxley Act in the US, the Basel II accord for financial services companies and others) requires executives to implement a proper risk management in their organisations. Adding to this, rating agencies recently announced that as part of their evaluation of the quality of management they will start to incorporate a review of enterprise risk management [4].

[1] DACH is the combination of the abbreviations of the countries of Germany (D), Austria (A) and Switzerland (CH).

ISO/IEC 73:2002 defines risk management as *co-ordinated activities to direct and control an organisation with regard to risk.* [5]. Risks can be managed through a combination of the following four strategic options [6]:

- reduce the risk,
- avoid the risk,
- transfer the risk,
- knowingly and objectively accept the risk.

One option to transfer the risk related to information technologies and information security which has emerged in the last years is Cyberinsurance [7, 8]. Cyberinsurance has been proposed as a market based solution for information security by different authors in the field [9–11]. Cyberinsurance coverage compensates the insured parties for a wide range of losses including but not limited to data loss, third party liabilities and others[2]. Estimates of the market for Cyberinsurance in the United States range from $450 to 500 million dollar annual gross written premium [13].

However, the insurance carriers still struggle to determine appropriate premium rates for covering cyber risks [2]. The reasons for these difficulties are missing actuarial loss data [14, 2] and the general lack of statistical data about information security incidents [15]. Therefore insurers put a range of exclusions in these policies, which again is a hindrance for wider market adoption Cyberinsurance as an instrument for risk transfer [2].

In this paper the results of an exploratory qualitative study with 36 experts from the DACH region will be presented. The objective of this study was the identification of potential rating indicators which could be used as a basis for the development of a risk classification system for Cyberinsurance.

The paper is structured as follows: In Section 2 the relevant notions and the context of this research are described. In Section 3 the research problem and our contribution will be outlined. In Section 4 the whole research is outlined using a step-by-step description. In Section 5 we present and discuss the results of our exploratory qualitative study. In Section 6 we discuss the limitations of this study. Section 7 positions this study with regard to related work from different fields. The paper is concluded with a conclusion and an outlook of the possible implications of our findings.

2 Background

The business of insurance presumes an exposure – the possibility of a loss. If there is no chance of loss, there is no need for insurance [16]. Even more, if there would be no economic uncertainty regarding the occurrence, timing and magnitude of an event, there would be no reason for insurance neither [17]. An insurer has to determine the price – the insurance premium or rate – for assuming potential losses of a certain type. Therefore, risk rating is a very important aspect – if not the most important – of insurance.

[2] For an overview of different insurance offerings the reader is referred to Baer [12].

The business impact of cyber risks can materialise in different ways [18]. First of all businesses may be exposed to a loss of property if hardware breaks down, is damaged or stolen (*physical resources exposures*). The range extends to a wide spectrum of financial losses (*financial resources exposures*) due to business interruptions or recovery expenses that are related to information technology failures or successful cyber attacks. Even damage to persons (*human resources exposures*) can be a result of information technology incidents (e.g. traffic management or clinical systems). This distinction according to *Loss Type* is made from a legal perspective with regard to the problem of economic loss which can be the result of a pure financial loss, a physical damage to property or personal injury [19, p 169].

Another dimension which is used to classify the losses due to cyber risks is the notion of *Loss Centre*. The dimension of *Loss Centre* describes to whom the loss happens [8]: *First-party losses* are those losses occurring directly to the insured organisation, while *third-party losses* are losses which occurred to other parties (eg. a customer, vendor or another third party). The dimension of *Loss Centre* is useful to distinguish coverages in the context of Cyberinsurance [13]. Third-party coverages are often also labelled as *liability* coverages.

There are different methods for identifying loss exposures which can be categorised along the following groups [20]:

- Document analysis,
- Compliance review,
- Personal inspections,
- Expertise within and beyond the organisation.

In the domain of Cyberinsurance the methods of choice for identifying loss exposures are document analysis and personal inspections. Depending on the size and coverage of the insurance contract either more economic questionnaires or very costly evaluations conducted by a third party which is specialised in information security and performs personal and physical inspections on the clients site are used [21].

No matter what method is used for pricing and rating risks, they all have in common the need to determine factors that have an influence on the expected losses. These factors can be divided in two groups [16]: the *exposure base* (consisting of only one factor) and *rating variables*.

The exposure base is the basis on which the premium is calculated and it should therefore accurately reflect the expected losses. It is important to note, that the exposure base is not the real exposure, but rather a proxy for the real exposure [16]. Examples for exposure bases are car-month or car-mile in automobile insurance, the sum of coverage provided, or total payroll for workers compensation. The insurance premium is normally calculated as a rate per exposure base. Consider as an example the premium property insurance, that is calculated as a fraction of the value of the insured property. If the value of property is used as an exposure base and one homeowner insures his 100.000 Euro home and pays 1.000 Euro premium (i.e. a rate of 1%), then a homeowner insuring his 1.000.000 Euro should pay 10.000 Euro premium (i.e. a rate of 1%). Exposure bases should be correlated proportionally to the expected losses [22].

However, in practice there are many other factors influencing the exposure to loss and therefore insurers use additional rating variables that allow to classify risks and adjust the premium accordingly [16]. Examples for premium-rating variables used e.g. in car insurance include among others age, gender[3], marital status, use of the automobile (pleasure or work), geography (location and area) and other criteria like the type, make and age of the automobile, multiple-car discounts and others [25, 22].

3 Research problem and contribution

Since the market for Cyberinsurance is a relatively new one, there seems to be a lack of sophisticated models. While some authors propose approaches and frameworks for pricing cyber-insurance [7, 26, 27], there is – to the best knowledge of the authors – no research available about rating variables and indicators which could play a role in the premium-rating process.

In this regard the situation of Cyberinsurance is similar to the field of operational risk rating. Power denotes some of the controversies and discussions with regard to operational risk, that in the authors opinion are reflecting also the main problems related to the insurance of cyber risks: *"[. . .] three key domains of policy controversy have been, and remain, particularly visible: definitional issues, data collection and the limits of quantification."* [28]

In an emerging market like Cyberinsurance the insurance companies compete also with the quality of their premium-rating models. According to economic theory in the long run these premium-rating models should converge with the actual security risks, because competition sets an upper and profitability a lower bound to the premiums [29].

The authors gathered several questionnaires which are actually used by insurance companies to assess the exposure to cyber risks. While a comparison of these questionnaires gave an idea about what factors are to be considered in the premium-rating process, the risk model and actuarial tables behind these questionnaires remain a business secret of the insurance carriers.

This paper aims to make a first step in the direction of developing better risk models and rating frameworks in the context of Cyberinsurance by addressing the following research question: **What are potential rating indicators for Cyberinsurance?**

[3] The use of rating variables like age, marital status and gender is part of enduring ongoing debate in the light of discrimination [23]. In the European Union in 2004 a Directive regarding equal treatment between men and women has been released, which states: *"(18) The use of actuarial factors related to sex is widespread in the provision of insurance and other related financial services. In order to ensure equal treatment between men and women, the use of sex as an actuarial factor should not result in differences in individuals' premiums and benefits. [. . .]"* [24]

In this paper the results of an exploratory qualitative study addressing this research question will be presented. The results of this study might be a useful resource for insurers who seek additional rating variables to further refine their premium-rating models. From a theoretical perspective the identified indicators provide a starting point for further research into influential risk factors and the development of risk assessment models.

4 Research method

To answer the research question we have chosen a qualitative research approach. Due to the lack of statistical data about information security incidents [15] we have chosen to collect potential rating indicators from experts. Based on semi-structured expert interviews from the DACH region a list of such potential indicators which could be used for rating Cyberinsurance premiums was identified.

In this section the research method is described using a step-by-step description of the whole process, from the preparation to the final ranking of indicators (cf. Figure 6). In the description of the process we partly follow the guidelines of Myers and Newman for conducting qualitative interviews [30].

4.1 1. Step: Preparation, Constructs

Before conducting the qualitative expert interviews a literature review about the related work in the field of Cyberinsurance was conducted, which is partly subsumed in Section 2 and in Section 7. To achieve the objectives of this research and owing to the exploratory nature of the research problem, the authors decided to conduct semi-structured expert interviews.

We wanted to explore the ideas about rating indicators that the experts might come up with as openly as possible. Therefore we have used a minimal structure for the interview using several sections, which each address a particular aspect of rating indicators. In this Section we will outline the constructs and concepts which have been used to structure the interviews.

Exposure and quality The first concept which has been used for structuring the interviews is the distinction between *exposure* and *quality*. With exposure we characterise the inherent risk level of an organisation. The concept of quality stands for the quality of the IT risk management in an organisation. This distinction was based on practical input from our project partners, who outlined the necessity to not only focus on the inherent risk of an organisation but also the quality of its security and risk program [31, p. 347].

Figure 1 outlines these two concepts. The exposure stands for the inherent risk level and the quality of IT risk management acts as a proxy for the risk reduction capabilities in an organisation. In a premium-rating framework, variables which indicate a high quality of IT risk management would lead to a reduction of the premium.

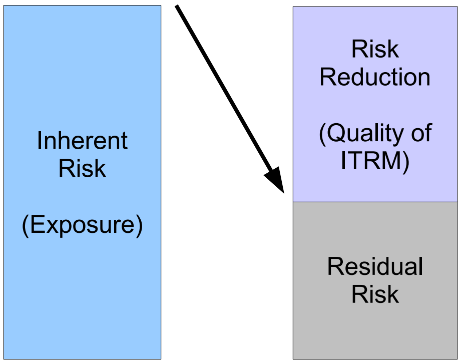


Fig. 1. Concepts of exposure and quality (adapted from ISO/IEC 13335-1:2004 [32])

Loss centre The second concept which we have introduced is the concept of loss centre which was already described in Section 2. The loss centre can be either first-party or third-party. This distinction was also introduced based on comments from practitioners, since these two types of coverages often present different lines of business of an insurer, are treated differently from a legal perspective and impose different requirements [13].

The concept of loss centre was applied to further distinguish the initial concept of exposure. We now have the exposure to first-party losses and the exposure to third-party losses. The concept of quality remained untouched by a further classification using the concept of loss centre. The authors believe that a high quality risk management is evenly capable to reduce both first-party and third-party losses to an acceptable level.

Layer model The last construct we have introduced to structure the interview is a layer model for information management. This concept was introduced to further classify the concept of third-party loss exposure. Why only the concept of third-party loss exposure and not also the one of first-party losses? The rationale behind this further classification of third-party loss exposure is based on the fact, that it is mainly companies from the IT sector (labelled as IT-Providers in the questionnaire) who are requesting this type of insurance coverage.

To account for different types of IT businesses we have explored various constructs for classifying the third-party loss exposure according to the type of offered IT service or product. The solution we came up with is a layer model which is present in many enterprise architecture frameworks. Examples for layered models in the technology domain include e.g. the well known Open Systems Interconnection Basic Reference Model [33] (OSI Model).

From the domain of information management, layered models include Wollnik's Three-Layer-Model of Information Management [34] or Krcmar's Layer-

Model [35]. Both models[4] have in common three different layer of abstraction to distinguish activities of information management in enterprises.

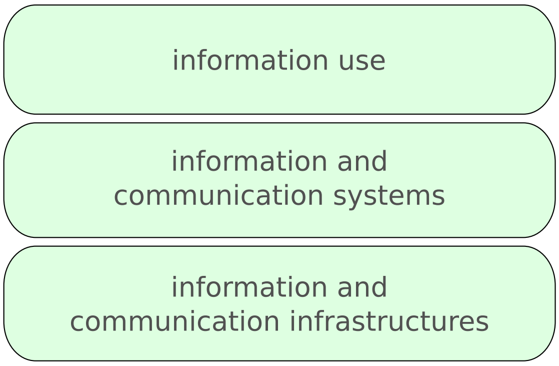

information use
information and communication systems
information and communication infrastructures

Fig. 2. Layer model of information management [34, 35]

The three layers are organised as follows from top to bottom (cf. Figure 2): The top layer represents the abstraction of *information use* in an organisation, the middle layer depicts *information and communication systems* while the bottom layer is used to handle *information and communication infrastructures* [34]. These three layers have been used as an abstraction to further distinguish different types of IT services and products and the related indicators for third-party loss exposures.

The resulting questionnaire The questionnaire we have used to structure the interview is the result of an initial pre-test during which we tested the feasibility of the first versions of our questionnaire. We conducted the pre-test with 5 interviewees. During the pre-test it became clear, that some questions where very difficult to answer and these have therefore either been eliminated or reformulated. Also the ordering of questions has been changed to a more comprehensive logical order.

The resulting questionnaire which we have finally used for the interviews is outlined below (cf. Table 1). In the beginning of the interview we had two additional Sections with a general introduction of the important terms (exposure, quality, loss centre) and additional questions about the interviewees to create a profile of the participants.

The questions of the interview which targeted towards the research question were organised in three Sections. The first Section questioned indicators related

[4] Krcmar's layer model of information management includes a fourth "layer" that encompasses all three abstraction layers and represents the managerial functions related to information management [35].

to the first-party loss exposure. The second Section focused on the quality of the IT risk management. The third Section aimed at indicators related to the third-party loss exposure. The third Section was further subclassified using a general class and the three layers of the layer model (cf. Figure 2).

Table 1. The resulting questionnaire

Section 3: IT Business Risk Exposure Indicators (first-party losses)
1. What are in your opinion relevant drivers and indicators for the IT Business Risk Exposure of an organisation?
Section 4: Indicators for the Quality of the IT Risk Management
1. What are in your opinion indicators for the quality of the IT Risk Management efforts in an organisation?
Section 5: IT Business Risk Exposure Indicators (IT-Providers with regard to third-party losses)
in general 1. Which indicators reflect the potential of IT-Providers in general to cause third party losses due to IT Business Risks?
IT-Infrastructure 2. Which indicators reflect the potential of IT-Infrastructure Providers to cause third party losses due to IT Business Risks?
Information Systems 3. Which indicators reflect the potential of Information Systems and Application Providers to cause third party losses due to IT Business Risks?
Information Use 4. Which indicators reflect the potential of Information Providers and Processors to cause third party losses due to IT Business Risks?

4.2 2. Step: Selection of experts

Based on the targeted research objective and the aim of the study we started to design candidate profiles for the interviews. The research sample selected for this study was built using a combination of purposive and snowball sampling. Taking into consideration the sensitive nature of the research topic [15] the authors decided to interview candidates which have an internal or external perspective on the topic.

The internal perspective was captured by professionals who are working in an organisation having the role of CISO (Chief Information Security Officer), Risk Manager or General Management and IT Management. The external perspective was captured by professionals who are either working as auditors, consultants in the field of IT risk management or information security experts and have thus a broad experience from many different organisations. Figure 4 outlines the experience profile of the participants. 70% of the sample have professional experience in the field of information security or risk management of more than 10 years. Figure 3 outlines the designation profile of the entire sample.

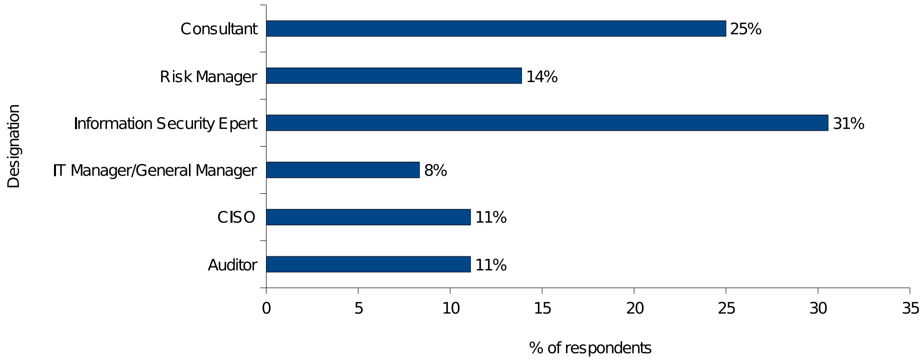


Fig. 3. Designation profile of the respondents

During the process of acquiring experts for the interviews, we put special emphasis on the fact that the interviews are not aiming towards any kind of sensitive information about the risks in the respective organisations. This was a very important issue, which was brought up by most of the candidate experts.

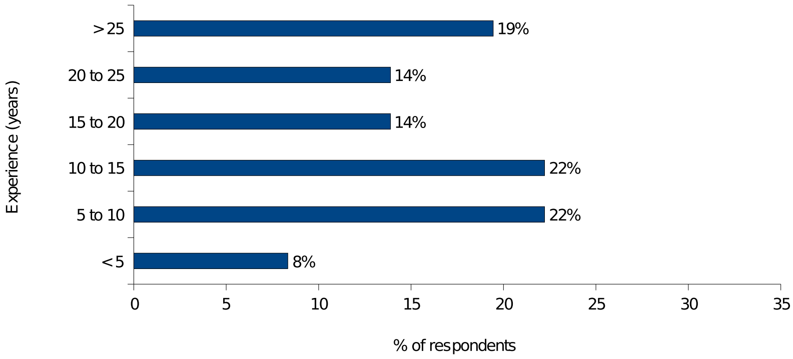


Fig. 4. Experience profile of the respondents

By emphasising that we were interested only in their expert knowledge and what indicators they deem important from a general point of view, we overcame this critical point in all cases. In general the willingness to contribute and support the research project was very high and we had only few refusals to participate in the interviews, and these few were mainly attributable to time constraints on behalf of the candidates.

The first group of experts were purposely identified from a pool of contacts which our research group has built up as part of its ongoing activities to create a regional forum of information exchange about information security involving practitioners and academics. The second group of experts was also selected purposely from a pool of participants who attended the expert forum about IT and Internet Risks in 2005 organised by Swiss Re in Munich.

Beginning with these two initial groups of participants from Austria and Germany, we employed snowball sampling to identify further suitable candidates for the interviews based on the recommendation of the experts from the first two groups. At the closing of each interview the experts were asked whether they could name additional professionals who match our requirements. The requirements for being selected in the sample were the following:

- The candidates are involved in IT or information security risk management activities.
- Each of the candidates should have a minimum of three years of relevant experience working with IT risks.

The interviews were conducted in the period between April 2006 and October 2007. We have interviewed a total number of 36 experts.

4.3 3. Step: Generation of statements

The interviews lasted between 50 minutes and 90 hours depending on the time constraints of the interviewees. 26 of the 36 interviews were conducted in a personal face-to-face meeting with the participants, typically in their office and in a few cases at other meeting places like airports. The other 10 interviews were conducted via phone conversations.

Most of the interviews – given explicit allowance – have been tape-recorded to allow for a later analysis and transcription. The interviews that were not recorded were registered by taking notes and creating a mind protocol shortly after the interview. The recorded interviews were transcribed to identify the main statements, their relations and examples.

The interviews started with an opening which involved an introduction. During this introduction the purpose of the interview and the research project context were explained. After gathering information about the interviewee's role and experience (cf. Figure 3 and 4), the interview entered in its main stage with the key questions (cf. Table 1).

The semi-structured interviews contained just the three main sections about indicators which highlight the first-party loss exposure, the quality of the IT risk management and the third-party loss exposure. The question about the third party loss exposure was further subdivided using the different layers of abstraction of the layer model (cf. Figure 2).

The questions enabled the 36 participants to generate a total of 976 statements, which were written down on paper during the interviews. At the end of the interview the interviewees were presented with the list of the statements they generated to check for inconsistencies and completeness. In the case of face-to-face meetings the statements were highlighted on paper and presented to the participants. In the case of phone conversations the complete list of statements was repeated at the end of the interview.

4.4 4. Step: Interpretation and consolidation of statements

Shortly after the interviews took place they were transcribed and the relevant text sequences were highlighted. After the transcription we have used concept mapping for structuring and organising the gathered knowledge. Concept mapping is an approach which supports the graphical representation of statements [36, 37]. Concept mapping offers some additional possibilities compared to a pure text based analysis [38]. Especially the possibility to outline connections between the mapped statements has been useful in the process of consolidating the gathered knowledge.

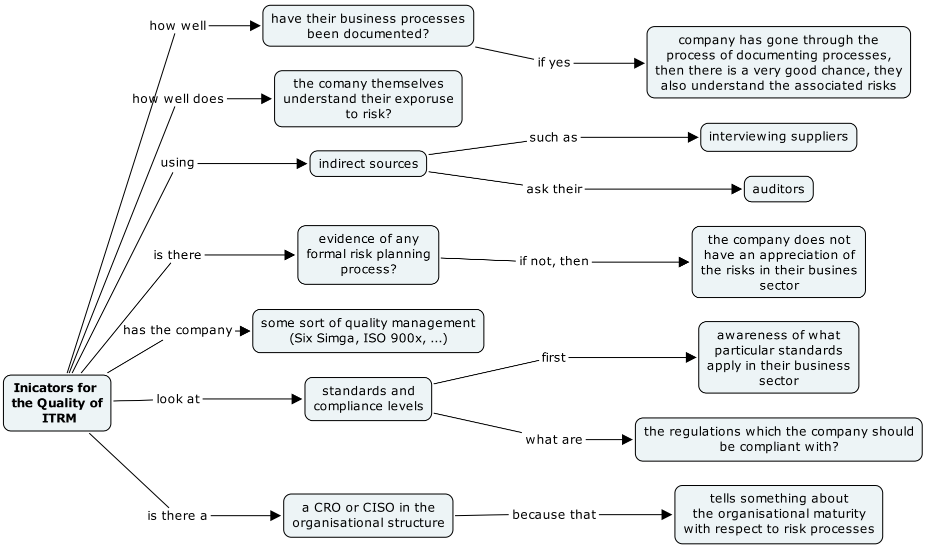

Inicators for the Quality of ITRM
how well
have their business processes been documented?
if yes
company has gone through the process of documenting processes, then there is a very good chance, they also understand the associated risks
how well does
the comany themselves understand their exporuse to risk?
using
indirect sources
such as
interviewing suppliers
ask their
auditors
is there
evidence of any formal risk planning process?
if not, then
the company does not have an appreciation of the risks in their busines sector
has the company
some sort of quality management (Six Simga, ISO 900x, ...)
look at
standards and compliance levels
first
awareness of what particular standards apply in their business sector
what are
the regulations which the company should be compliant with?
is there a
a CRO or CISO in the organisational structure
because that
tells something about the organisational maturity with respect to risk processes

Fig. 5. Example concept map of an interview (excerpt)

For each of the 36 interviews a concept map was created, which included the main statements and included also additional explanations, examples and clarifications. For creating the concept maps we used the software CmapTools from the Institute of Human and Machine Cognition[5]. Figure 5 shows an excerpt from one of the concept maps.

Once all the interviews transcripts and protocols protocols have been transformed to concept maps, these single concept maps were exported to create a unified concept-map including the concepts and propositions of all interviewed experts. The purpose of this combined concept map was the step-wise consolidation of the 976 statements of all 36 interviewees.

The explanations and examples related to each of the statements facilitated the process of interpreting and consolidating the statements in similar groups. The criteria for grouping the statements were syntactic similarity and semantic similarity. Concept mapping has proved to be a valuable tool for this consolidation process. However, we used concept mapping only as a tool for representation of the gathered knowledge, we did not employ multivariate statistical analyses as described by Daley [36] or Trochim et al. [38, 39].

By linking the statements of the single experts to similar groups it was possible to identify emerging themes and levels of hierarchy [36]. However, the purpose of interpreting and consolidating the statements was not to analyse the hierarchical relations of the statements and their connecting links, but to compile a reduced and consolidated list of statements. After the systematic grouping and categorisation of the statements we have reduced the list of 976 statements to a list of 198 consolidated indicators (cf. Appendix A).

4.5 5. Step: Reducing the resulting list of indicators

This list of 198 consolidated indicators was discussed and presented to actuaries who are experienced in the external risk assessment of organisations in the context of Cyberinsurance. The intention was to reduce the list of 198 indicators to a list of variables, which are considered useful for practical uses in the context of Cyberinsurance. During a workshop held with three actuaries of our project partner the 198 were presented, discussed and a selection based on specific criteria was made.

The American Academy of Actuaries lists the following basic principles that should be present in any sound risk classification system and therefore also in the selection of rating variables[6]. The principles state that a classification system should [17]:

- reflect expected cost differences,
- distinguish among risks on the basis of relevant cost-related factors,
- be applied objectively,
- be practical and cost-effective,
- be acceptable to the public.

[5] Download of IHMC CmapTools: http://cmap.ihmc.us/

[6] For a more detailed treatise see Finger, who provides an overview and a discussion of criteria for selecting rating variables. Finger groups the criteria in four categories, namely: *"actuarial, operational, social, and legal"* [22].

For selecting the indicators in this research project we used only two criteria which were taken from a paper of Bouska. Bouska cites Webb who uses the following three criteria for selecting exposure bases: *"First and foremost, of course, it should be an accurate measure of the exposure to loss. Second, it should be easy for the insurer to determine. Finally, it should be difficult for the insured to manipulate."* [16] The last two criteria were actually used to filter the indicators that were identified in the first round:

- *Are the indicators measurable?*
- *Are the indicators unmistakable and difficult to manipulate?*

The workshop with the three actuaries resulted in the selection of 94 indicators which were deemed useful for premium-rating in the context of Cyberinsurance, since they were considered measurable and objectively answerable.

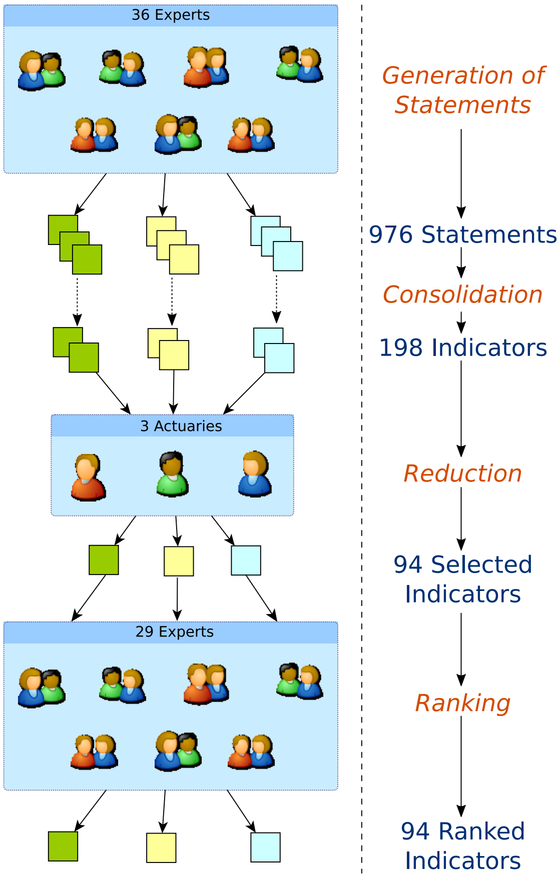


Fig. 6. Schematic overview of the research process

4.6 6. Step: Ranking indicators

The 94 indicators which were selected by the three actuaries were again sent to the initial 36 experts asking them to rank the indicators according to their relative importance. For ranking the indicators we used a 10-point Likert scale as illustrated in Figure 7. The ranking of the 94 indicators was collected using a web-based questionnaire (cf. Figure 8).

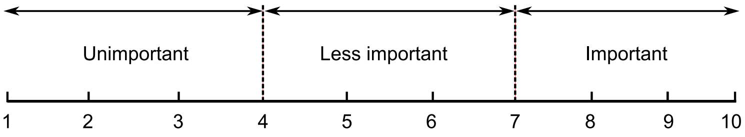
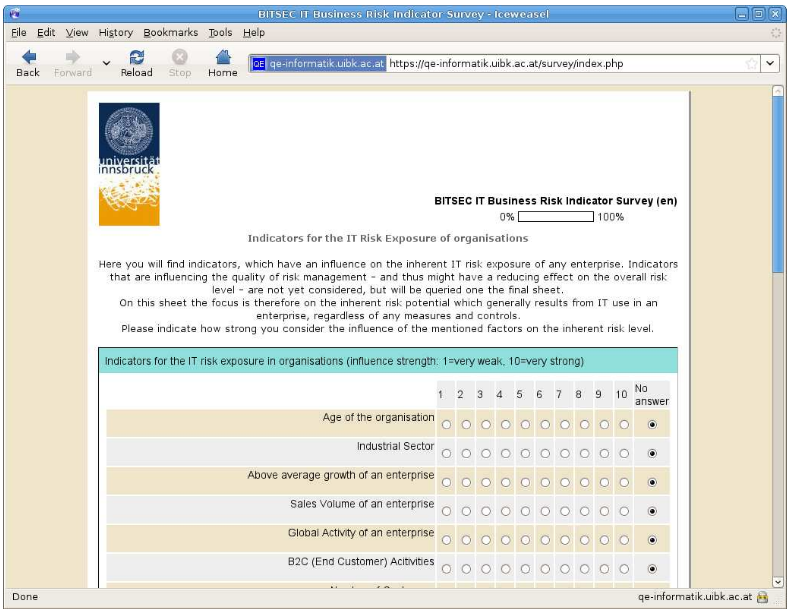


Fig. 7. Intervals of rating [40]

In the final step of ranking the indicators 29 of the initial 36 experts have participated. Seven experts were not able to participate in the final ranking due to time constraints. Finally, descriptive statistics were used to analyse the ranking of the indicators.


BITSEC IT Business Risk Indicator Survey - Iceweasel
File Edit View History Bookmarks Tools Help
Back
Forward
Reload
Stop
Home
qe-informatik.uibk.ac.at
https://qe-informatik.uibk.ac.at/survey/index.php
universität innsbruck
Done
qe-informatik.uibk.ac.at

BITSEC IT Business Risk Indicator Survey (en)

0% 100%

Indicators for the IT Risk Exposure of organisations

Here you will find indicators, which have an influence on the inherent IT risk exposure of any enterprise. Indicators that are influencing the quality of risk management - and thus might have a reducing effect on the overall risk level - are not yet considered, but will be queried one the final sheet.
On this sheet the focus is therefore on the inherent risk potential which generally results from IT use in an enterprise, regardless of any measures and controls.
Please indicate how strong you consider the influence of the mentioned factors on the inherent risk level.

Indicators for the IT risk exposure in organisations (influence strength: 1=very weak, 10=very strong)

	1	2	3	4	5	6	7	8	9	10	No answer
Age of the organisation	○	○	○	○	○	○	○	○	○	○	●
Industrial Sector	○	○	○	○	○	○	○	○	○	○	●
Above average growth of an enterprise	○	○	○	○	○	○	○	○	○	○	●
Sales Volume of an enterprise	○	○	○	○	○	○	○	○	○	○	●
Global Activity of an enterprise	○	○	○	○	○	○	○	○	○	○	●
B2C (End Customer) Acitivities	○	○	○	○	○	○	○	○	○	○	●

Fig. 8. Screenshot of the web based survey

5 Results

Table 2. Ranking of first-party loss exposure indicators

Rank	Indicator	Mean	SD
1	Critical dependency of business processes on IT	8,83	1,13
2	Low failure tolerance with regard to IT	8,78	1,20
3	Processing sensitive data with high confidentiality requirements	8,38	1,31
4	Existence of worth-protecting know how, patents and otherwise valuable information	8,29	1,70
5	High demands on the availability of data and systems in the organisation	8,19	1,63
6	Online execution of Business Processes	7,83	1,62
7	Environmental and physical risks at the location of the data centre	7,79	1,70
8	Link-ups of external partners to the enterprise IT	7,67	1,11
9	High level of automation in the production of goods and services	7,50	1,71
10	Data recoverability in data loss scenarios	7,26	2,54
11	Just-in-time supply/delivery relationships with partners	7,25	1,73
12	Above average growth of an enterprise	7,11	1,74
13	Industrial Sector	7,07	1,92
14	Labour turnover rate (in general)	6,90	2,27
15	Availability of qualified workforce	6,85	1,68
16	Use of mobile devices in the organisation	6,72	2,29
17	Outsourcing of IT processes including coordination and control	6,68	1,94
18	IT-personnel / overall number of employees ratio	6,57	1,95
19	Demand on the professional qualification of employees (in general)	6,42	1,81
20	Number of PC-Workplaces in the enterprise	6,34	1,48
21	Global Activity of an enterprise	6,14	1,75
22	B2C (End Customer) Activities	6,00	1,93
23	Private Internet use of employees in the organisation	5,93	2,21
24	Centralised IT-Infrastructure	5,86	2,08
25	Number of employees (overall)	5,62	1,89
26	Separate IT budget existent	5,62	2,06
27	Operation of standardised IT solutions	5,48	2,02
28	Number of Customers	5,21	1,94
29	Geographical distance between day-to-day business and IT production	4,89	2,18
30	Sales Volume of an enterprise	4,61	2,11
31	Age of the organisation	3,69	2,06

Table 3. Ranking of third-party loss exposure indicators

Rank	Indicator	Mean	SD
1	Control and Coordination of outsourced customer processes by the outsourcing provider	8,21	1,57
2	Access to central systems and information of customers	7,96	1,73
3	Quality of Patch-Management for the offered Information Systems	7,52	1,67
4	High service level requirements	7,48	1,86
5	Traceability of provider actions and interventions at customers sites	7,39	1,75
6	Extensive test procedures during development and deployment	7,16	2,05
7	Adoption of standardised methods and practices in software engineering	7,08	1,81
8	Availability of qualified workforce at the provider	6,92	1,80
9	Clarity and detailing of Service Level Agreements	6,84	2,36
10	Outsourcing of Information Systems Development (Offshoring)	6,81	1,94
11	Remote maintenance of systems installed on customers sites	6,76	1,75
12	Existence of Update- and Version-management of the offered information systems	6,75	1,73
13	Sole Seller for customers	6,73	2,68
14	Offer of Backup Services (Data backup)	6,71	1,86
15	Offered IT solutions could cause bodily injury	6,65	2,58
16	Quality and standardisation of project management	6,54	2,11
17	Definition of liability provisions and contractual sanctions in Service Level Agreements	6,46	2,42
18	High portion of employees occupied with further technical development and innovation	6,25	1,96
19	High portion of internal activity in offered services	6,25	1,88
20	Customers have the possibility to switch to alternative providers	6,08	2,32
21	Industry classification of customers	5,92	2,34
22	Offering of training concepts and courses for customers	5,88	1,71
23	Certification of employees/organisation by manufacturers or for specific products	5,67	2,47
24	Longevity of customer and contractual relationships	5,48	1,78
25	Sales Volume per customer	5,39	2,58
26	Number of employees of the provider	5,04	1,88
27	Sales Volume of provider	5,04	2,30
28	Provider offers a Central Contact Point or Service Desk	4,92	2,00
29	Customer structure (Number and quality of customers)	4,87	2,05

Table 4. Ranking of quality indicators for the IT risk management

Rank	Indicator	Mean	SD
1	Existing Role of a Risk Officer or Security Officer	8,78	1,26
2	Business Continuity concept and contingency and emergency plans available	8,46	1,35
3	Continual improvement process in Risk Management (PDCA Cycle)	8,41	1,37
4	Existence of an institutionalised risk management in the organisation	8,37	1,48
5	Policies concerning handling of confidential information	8,15	1,58
6	Security Policies for employees	8,04	1,35
7	Acceptance Testing required prior to release of new technologies and product versions	8,04	1,37
8	Investments in further education and training of employees to increase security awareness	8,04	1,15
9	Existence of a proper IT Risk Reporting	8,04	1,66
10	Periodical internal and/or external audits	8,00	1,54
11	Documentation of IT-Infrastructure	7,96	1,09
12	Existence of Protection requirements analysis	7,85	1,76
13	Password Policy available	7,85	1,59
14	Accounted budget for IT Security present	7,85	1,36
15	Existence of an IT-Governance function	7,74	1,70
16	Redundancies in the technical infrastructure	7,65	1,61
17	Security Manual available	7,63	1,68
18	Systematic Problem and Solution Management in IT	7,59	1,85
19	Policies and Guidelines for and control of external service providers	7,52	1,57
20	International standards and best practices orientation (in general and with regard to IT)	7,48	1,73
21	Physical protection measures	7,38	1,79
22	Ratio of IT employees dedicated to security	7,33	1,85
23	Physical control and registration of visitors at the entrance area	7,31	1,75
24	Maintenance of a proper Loss database	7,22	1,62
25	Measurement of performance indicators and and operating figures for assessing IT processes	7,00	1,70
26	IT-Management reports directly to the board level or is part of the board of directors	6,96	2,72
27	Information Security Certification(s)	6,96	2,13
28	IT-Service-management approach based on Standards	6,81	1,95
29	Quality Assurance of published content (Legal Review)	6,78	1,88
30	Employee Background Check	6,58	2,06
31	Quality Management System(s) Certification(s)	6,48	1,99
32	Definition of Life cycles for the IT-Infrastructure	6,44	1,87
33	Size of the enterprise	5,59	2,19
34	Age of the organisation	4,96	2,14

The results of the whole research process are outlined in Table 2, 3 and 4 on the previous pages. Since the questions of the interview targeted towards the identification of indicators one might have expected, that in the final ranking all of the selected indicators should have been attributed a high importance rating.

Regarding the first-party loss exposure indicators indicators which focus on the dependency of the business on IT have been ranked highest. The reader might remark that the indicators are rather abstract and already known or obvious. This is especially true for the highest ranked indicators like *Critical dependency of business processes on IT* and *Low failure tolerance with regard to IT*. However, we have willingly included these indicators, as related statements were recurring again and again. The highest ranked indicator (cf. Table 2, Rank #1) has emerged out of the consolidation of 51 statements from the total of 976 statements (cf. Appendix A).

What was puzzling the authors was that an indicator like *Sales Volume of an enterprise*, which is often used as an exposure base in Cyberinsurance contracts has been ranked as a less important indicator with a mean ranking of only $4,61$.

The third-party loss exposure indicators have been collected using the classification of the layer model as outlined in Section 4.1. As can be seen in Section A.2 in the Appendix A, the classification we have employed to further classify the third-party exposure indicators according to the layers of information management did never yield more than 10 indicators per class. Therefore in the result the indicators for third-party loss exposure have been compiled in a unique list (cf. Table 3).

The highest ranked indicator for the third-party loss exposure was the degree of *Control and Coordination of outsourced customer processes by the outsourcing provider* with a mean of $8,21$, followed by *Access to central systems and information of customers* with a mean of $7,96$. Interesting to note, that also in the case of the third-party loss exposure indicators the *Sales Volume of provider* ranked third-lowest on the relative importance scale with a mean of only $5,04$.

The indicators for the quality of the IT risk management have generally a higher mean ranking than the first-party and third-party loss exposure indicators. The top 13 first-party exposure indicators have a mean ranking higher than 7. In the case of the third-party loss exposure indicators only 7 indicators have a mean ranking higher than 7. The ranking of the indicators for the quality of the IT risk management has yielded 25 indicators with a mean ranking higher than 7.

6 Limitations

In this Section we discuss some limitations of this research. First of all, as with any Delphi-type study, the results are based on a sample with a limited number of subjects. While we tried to compose the sample with professionals who have a broad and long experience managing security or risks inside organisations or as external consultants and experts, we cannot claim any kind of representativeness of our sample. We used a convenience sample based on our direct relations with industry. Also the selection of additional participants was not random since we employed a snowball strategy to identify additional candidates.

Another potential weakness is the cultural background of the experts. Since the sample of interviewees is taken solely from the DACH region, there is potential bias in the findings, due to the lack of cultural diversity. Schmidt et al. conducted an international Delhi study to identify software project risk with panelist from Hong Kong, Finland and the United States [41]. They identified differences in the relative importance of risk factor across the various cultures. Thus in this paper, the results might be biased since the whole sample has a common cultural background.

Another significant limitation of this research is the fact that a great part of the study was conducted in German, necessitating the translation of the indicators in English for this paper.

A limitation of the research process as outlined in Section 4 is the fact that we have not conducted any type no validation of the consolidated list of factors as it would be in a Delphi type of study. Due to the restricted time budgets of the participating experts, it would not have been realisable to introduce one more step to check the results of the consolidation process. This might introduce a potential bias since the authors of this study have interpreted the statements and consolidated them.

Another potential point of criticism is the decision not to reduce the resulting list of indicators with the experts who participated in the interviews. Instead the reduction was done in a workshop with three actuaries who are experienced in risk assessments in the context of Cyberinsurance. These three actuaries were not interviewed and taking part in the initial interviews. This raises the possibility of varying interpretations of the indicators. In addition it introduces a potential bias since the initially interviewed experts had no influence on the selection of indicators. To reduce the risk of misinterpretations we have used the concept maps including the statements and examples as an additional aid during the selection workshop with the three actuaries.

The premium-rating models and indicators contained in the actuarial tables of the underwriters are a business secret of the insurance companies. How they do calculate rates can not be transparently said. Therefore the indicators that were identified in this chapter might already be in use and not contribute to an improvement of the state of the art in practice. Despite this limitation we believe that the results of this research represent an interesting resource for practitioners and there may be some additional factors, that might be worth incorporating into the existing models. Classification systems evolve over time [22, 25] and hence the rating variables used for classification will also continue to improve.

Regarding the theoretical value of these lists of indicators, we have just marked a first step in the direction of developing a rating model for cyber risks. We have not conducted any type of evaluation regarding the validity of the identified indicators. In addition, there might be interesting relations and an interplay between the various indicators and their influence on the actual risk exposure. These are interesting questions that might stimulate further research.

7 Related work

To the best knowledge of the authors there are no related works focusing on indicators for premium-rating in the context of Cyberinsurance. There are however different works from other fields which are providing risk factors.

This related work on risk factors in information systems and information technology provides additional valuable input for developing premium-rating models. Some of these works are focusing on software development risk such as Jiang et al. [42] of software project risk such as Schmidt et al. [41]. Sherer and Alter have conducted a review of different risk models used in the information systems literature [43].

The only exposure model that the authors came across was the *Risk Exposure Model for Digital Assets* published in Turban et al. Their exposure model for digital assets contains five general factors [44]:

- Asset's value to the company
- Attractiveness of the asset to a criminal
- Legal liability attached to the asset's loss or theft
- Operational, marketing, and financial consequences
- Likelihood of a successful attack against the asset

This risk exposure model is focusing on digital assets and therefore provides also valuable input for rating cyber risks. In contrast we are focusing on a risk exposure model for organisations and therefore focus on a different level of abstraction.

8 Conclusions and Outlook

The results presented in this paper provide lists of indicators which could serve as potential candidates for rating variables for Cyberinsurance. The indicators have been consolidated from semi-structured expert interviews with 36 participants from the DACH region. After a reduction of the indicators to a set of 94 indicators which are measurable and objectively answerable, the indicators were again presented to the initial 36 experts. In the ranking step 29 experts have ranked the indicators according to their relative importance.

These indicators could be used to build new or refine existing risk classification systems and premium-rating models. Due to the lack of concrete scenarios with quantified losses, it was out of scope of this research to validate which of these potential rating variables actually reflect the risk exposure.

Further research would also investigate the relations and the interplay between the listed indicators. For some indicators, which are rather abstract and difficult to objectively assess, it would be interesting to research better indicators which could act as proxies for them.

Another important question is regarding the relation and the interplay between these indicators. We have already identified some relations during the course of the interviews and in the combined concept map of all statements.

However, we have not systematically analysed the hierarchical structure of the statements.

The list of 94 ranked indicators and the initial list of 198 indicators in the Appendix provide a starting point for developing a model and a framework for risk rating in the context of Cyberinsurance. A task that is surely left to do is to organise the presented indicators in meaningful categories. The authors believe that some of the identified indicators might only be relevant for certain types of coverages. Such a categorisation of exposure indicators would also provide an excellent baseline for developing a theoretical exposure model for organisations.

Another task that is left to future work is the important issue of operationalization of these indicators. While some of the indicators are binary and can be easily answered using yes or no, most of the indicators are not binary. Some indicators might be measured using a qualitative range of values to reflect the degree to which they apply in a certain organisation. We are currently investigating the operationalization of these indicators.

In a previous publication we have analysed publicly announced security incidents to identify different types of losses related to security incidents [45]. Matching the identified indicators presented in this paper with damages and losses resulting from security incidents will provide further valuable insights.

Acknowledgements

This research is part of the results of the research project BITSEC between the Research Group Quality Engineering, Swiss Re Germany and Arctis Softwaretechnology which focused on the external assessment of IT related risks in the context of cyber-insurance. The research cooperation was funded by the Austrian Research Agency FFG.

References

1. Cashell, B., Jackson, W., Jickling, M., Webel, B.: The Economic Impact of Cyber-Attacks. Congressional Research Service Documents, CRS RL32331 (Washington DC) (2004)
2. Ernst & Young: Moving beyond compliance: Ernst & Young's 2008 Global Information Security Survey (2008) Accessed: 2009-02-24.
3. Deloitte Touche Tohmatsu: Protecting what matters. The 6th Annual Global Security Survey (2009) Accessed: 2009-02-24.
4. Cummings, J.: S&P Rolls Out ERM Review. http://businessfinancemag.com/article/sp-rolls-out-erm-review-0513 (March 2008) Accessed: 2009-01-31.
5. ISO (International Organization for Standardization): ISO/IEC 73:2002 Risk management – Vocabulary – Guidelines for use in standards (2002)
6. BSI (British Standards Institution): BS 7799-3:2006 Information security management systems – Part 3: Guidelines for information security risk management (2006)

7. Gordon, L.A., Loeb, M.P., Sohail, T.: A framework for using insurance for cyber-risk management. Commun. ACM **46**(3) (2003) 81–85
8. Böhme, R.: Cyber-Insurance Revisited. In: Workshop on the Economics of Information Security (WEIS), Harvard University, Cambridge, MA (2005)
9. Kesan, J.P., Majuca, R.P., Yurcik, W.J.: Cyberinsurance as a Market-Based Solution to the Problem of Cybersecurity. In: Workshop on the Economics of Information Security (WEIS), Harvard University, Cambridge, MA (2005)
10. Schneier, B.: The Insurance Takeover. Information Security (Feb 2001)
11. Yurcik, W., Doss, D.: CyberInsurance: A Market Solution to the Internet Security Market Failure. 1st Workshop Econom. Inform. Security (2002)
12. Baer, W.S.: Rewarding IT Security in the Marketplace. In: TPRC 2003. (2003)
13. Betterley, R.S.: Cyberrisk Market Survey 2008 (June 2008) The Betterley Report.
14. Kovacs, P., Markham, M., Sweeting, R.: Cyber-Incident Risk in Canada and the Role of Insurance. ICLR Research Paper Series 38, ICLR (Institute for Catastrophic Loss Reduction) (Aril 2004)
15. Kotulic, A.G., Clark, J.G.: Why there aren't more information security research studies. Information & Management **41**(5) (2004) 597–607
16. Bouska, A.S.: Exposure Bases Revisited. Proceedings of the Casualty Actuarial Society Casualty Actuarial Society - Arlington, Virginia **LXXVI, Part 1**(145) (1989) 1–23
17. AAA (American Academy of Actuaries Committee – Committee on Risk Classification): Risk Classification Statement of Principles Retrieved: 2008-07-21.
18. Büchel, M., Favre, R., Wiest, R.: Law, insurance and the Internet: The new perils of cyberspace. Technical report, Swiss Re Publishing (2000)
19. Mattiacci, G.D.: The Economics of Pure Economic Loss and the Internalisation of Multiple Externalities. In: Pure Economic Loss. Volume 9 of Tort and Insurance Law. Springer (2004) 167–190
20. AICPCU (American Institute for CPCU/Insurance Institute of America): Foundations of Risk Management, Insurance, and Professionalism (Course Leader Handbook 2006) CPCU 510 Appendix A.
21. Ogut, H., Raghunathan, S., Menon, N.: Information security risk management through self-protection and insurance. (2005)
22. Finger, R.: Risk Classification, Chapter 6. In: Foundations of Casualty Actuarial Science. Fourth edition edn. Casualty Actuarial Society, Arlington, VA (2001) 287–342
23. Wiegers, W.A.: The Use of Age, Sex, and Marital Status as Rating Variables in Automobile Insurance. The University of Toronto Law Journal **39**(2) (1989) 149–210
24. Official Journal of the European Communities: Council Directive 2004/113/EC of 13 December 2004 implementing the principle of equal treatment between men and women in the access to and supply of goods and services (December 2004) Retrieved: 2008-09-11.
25. Trowbridge, C.: Fundamental concepts of actuarial science. Actuarial Education and Research Fund (1989)
26. Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., Sadhukhan, S.K.: e-Risk Management with Insurance: A Framework Using Copula Aided Bayesian Belief Networks. In: HICSS, IEEE Computer Society (2006)
27. Herath, H., Herath, T.: Cyber-Insurance: Copula Pricing Framework and Implications for Risk Management. Proc. of Workshop on the Economics of Information Security (WEIS) (2007)

28. Power, M.: The invention of operational risk. Review of International Political Economy **12**(4) (2005) 577–599
29. Bohme, R., Nowey, T.: 15 Economic Security Metrics. In: Dependability Metrics. Springer (2008) GI-Dagstuhl Research Seminar, Dagstuhl Castle, Germany, October 5-November 1, 2005, Advanced Lectures.
30. Myers, M., Newman, M.: The qualitative interview in IS research: Examining the craft. Information and Organization **17**(1) (2007) 2–26
31. Tipton, H., Krause, M.: Information Security Management Handbook. 6, illustrated, revised edn. Auerbach Pub (2007)
32. ISO (International Organization for Standardization): ISO/IEC 13335-1:2004 Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management (2004)
33. Zimmermann, H.: OSI Reference Model–The ISO Model of Architecture for Open Systems Interconnection. Communications, IEEE Transactions on [legacy, pre-1988] **28**(4) (1980) 425–432
34. Wollnik, M.: Ein Referenzmodell des Informationsmanagements. Information Management **3**(3) (1988) 34–43
35. Krcmar, H.: Informationsmanagement. Springer (2005) 4., überarb. und erw. Aufl.
36. Daley, B.: Using concept maps in qualitative research. Concept Maps: theory, Methodology, Technology: Proceedings of the First International Conference on Concept mapping, Pamplona, Spain **1** (2004) 191–197
37. Novak, J.D., Cañas, A.J.: The Theory Underlying Concept Maps and How to Construct Them. Technical Report Technical Report IHMC CmapTools 2006-01, Florida Institute for Human and Machine Cognition (2006)
38. Jackson, K., Trochim, W.: Concept Mapping as an Alternative Approach for the Analysis of Open-Ended Survey Responses. Organizational Research Methods **5**(4) (2002) 307
39. Trochim, W., Kane, M.: Concept mapping: an introduction to structured conceptualization in health care. International Journal for Quality in Health Care **17**(3) (2005) 187–191
40. Imriyas, K., Pheng, L.S., Teo, E.A.L.: A framework for computing workers' compensation insurance premiums in construction. Construction Management and Economics **25**(6) (2007) 563–584
41. Schmidt, R., Lyytinen, K., Keil, M., Cule, P.: Identifying Software Project Risks: An International Delphi Study. Journal of Management Information Systems **17**(4) (2001) 5–36
42. Jiang, J., Klein, G., Ellis, T.: A measure of software development risk. Project Management Journal **33**(3) (2002) 30–41
43. Sherer, S., Alter, S.: Information System Risks and Risk Factors: Are they mostly about Information Systems? Communications of the Association for Information Systems (Volume 14, 2004) **29**(64) (2004) 29
44. Turban, E., Leidner, D., McLean, E., Wetherbe, J.: Information Technology for Management: Transforming Organizations in the Digital Economy. John Wiley & Sons, Inc. New York, NY, USA (2008)
45. Innerhofer-Oberperfler, F., Breu, R.: An empirically derived loss taxonomy based on publicly known security incidents. In: Proceedings of the Fourth International Conference on Availability, Reliability and Security – ARES/CISIS 2009, Fukuoka, Japan. (2009)

A Appendix

A.1 First-party loss exposure indicators

Table 5: Exposure indicators for first-party losses

Indicator	**Count**	**Selected**
Critical dependency of business processes on IT	51	√
Existence of worth-protecting know how, patents and otherwise valuable information	20	√
Industrial Sector	16	√
Environmental and physical risks at the location of the data centre	12	√
Demand on the professional qualification of employees (in general)	10	√
Number of employees (overall)	8	√
Availability of qualified workforce	7	√
Above average growth of an enterprise	6	√
Link-ups of external partners to the enterprise IT	6	√
High demands on the availability of data and systems in the organisation	5	√
Low failure tolerance with regard to IT	5	√
Processing sensitive data with high confidentiality requirements	5	√
Separate IT budget existent	5	√
Centralised IT-Infrastructure	4	√
High level of automation in the production of goods and services	4	√
Labour turnover rate (in general)	4	√
Number of PC-Workplaces in the enterprise	4	√
Online execution of Business Processes	4	√
Outsourcing of IT processes including coordination and control	4	√
Geographical distance between day-to-day business and IT production	3	√
Just-in-time supply/delivery relationships with partners	3	√
Number of Customers	3	√
Operation of standardised IT solutions	3	√
Private Internet use of employees in the organisation	3	√
Sales Volume of an enterprise	3	√
Data recoverability in data loss scenarios	2	√
Global Activity of an enterprise	2	√
IT-personnel / overall number of employees ratio	2	√

Continued on next page

Table 5 – continued from previous page		
Use of mobile devices in the organisation	2	√
Age of the organisation	1	√
B2C (End Customer) Activities	1	√
Enterprise subject to strict legal regulations	11	
High-profile enterprise	11	
Market leader	4	
Age of the IT infrastructure	3	
Owner Management	3	
Short-term optimisation	3	
High competitive pressure	2	
High number of transactions per day	2	
Highly dynamic business environment	2	
Highly dynamic IT landscape	2	
Homogeneous IT landscape	2	
Obligations to supply and exchange data	2	
Sufficient safety stock	2	
Systems based on open standards	2	
Current high risk IT projects	1	
Early adopter and use of recent technologies	1	
Enterprise operates in a high technology sector	1	
Enterprise operates in a niche market with high market share	1	
High number of heterogeneous applications	1	
Highly complex production processes	1	
Highly interlinkage of processed data	1	
Incidents can strongly affect customers	1	
Operating system in use	1	
Potential to damage the economy	1	
Production of goods and services in front of customer	1	
Products or services subject to strict legal regulations	1	
Reputation in the market	1	
Revenues per employee	1	
Stock turnover ratio	1	
Strict contractual obligations toward customers	1	
Technical state of the art infrastructure	1	
Volume of stored critical data	1	

A.2 Third-party loss exposure indicators

Table 6: Exposure indicators for third-party losses (in general)

Indicator	**Count**	**Selected**
High service level requirements	12	√
Industry classification of customers	12	√
High portion of internal activity in offered services	11	√
Clarity and detailing of Service Level Agreements	10	√
Availability of qualified workforce at the provider	9	√
Sales Volume of provider	8	√
Certification of employees/organisation by manufacturers or for specific products	6	√
Longevity of customer and contractual relationships	6	√
Traceability of provider actions and interventions at customers sites	5	√
Customer structure (Number and quality of customers)	4	√
Offered IT solutions could cause bodily injury	4	√
Provider offers a Central Contact Point or Service Desk	4	√
Sole Seller for customers	3	√
Definition of liability provisions and contractual sanctions in Service Level Agreements	1	√
High portion of employees occupied with further technical development and innovation	1	√
Number of employees of the provider	1	√
Sales Volume per customer	1	√
Assumption of risk management tasks for customers	18	
Standardised solutions	15	
Location of offered services in the OSI model	11	
Sufficient financial stability	11	
Provider references	9	
Offerer of stand-alone or black-box systems	8	
Market adoption of offered products and services	5	
Partnership with manufacturers	5	
Frequency of occurrence on vulnerability lists	4	
System commission and integration competencies	4	
Provider focuses on core competence fields	3	
Regional activity	3	
State of the art tools	3	
Global activity	2	
High-profile provider	2	
In-house IT know-how	2	
Low cost strategy	2	

Continued on next page

Table 6 – continued from previous page

Offerer of brand-new products	2	
Proactive description of error scenarios and risks	2	
Reputation in the market	2	
Service provider business model	2	
Strategy alignment between customer and provider	2	
Established provider	1	
Individual arrangement of rules with customers	1	
Products and services require specialised know-how on the customer side	1	
Provider is market leader	1	
Provider is technological leader	1	
Provider uses cyber-insurance	1	
Regular reporting to the customer	1	
Service controllability	1	

Table 7: Exposure indicators for third party losses (Information Use)

Indicator	**Count**	**Selected**
Control and Coordination of outsourced customer processes by the outsourcing provider	3	✓
Access to central systems and information of customers	1	✓
Stability of outsourced processes	2	
Capacity management	1	
Established case-law in business sector	1	
Local distance to the customer	1	
Provision of dedicated resources for customers	1	

Table 8: Exposure indicators for third party losses (Information Systems)

Indicator	**Count**	**Selected**
Adoption of standardised methods and practices in software engineering	8	✓
Quality and standardisation of project management	5	✓
Offering of training concepts and courses for customers	3	✓

Continued on next page

Table 8 – continued from previous page		
Existence of Update- and Version-management of the offered information systems	2	√
Extensive test procedures during development and deployment	2	√
Outsourcing of Information Systems Development (Offshoring)	1	√
Quality of Patch-Management for the offered Information Systems	1	√
Solutions corresponding to customer requirements	3	
Offered information systems equipped with security features	1	
Professional competencies for offered industry solutions	1	
Software architecture	1	
Supported platforms	1	

Table 9: Exposure indicators for third party losses (IT Infrastructure)

Indicator	**Count**	**Selected**
Customers have the possibility to switch to alternative providers	14	√
Remote maintenance of systems installed on customers sites	4	√
Offer of Backup Services (Data backup)	2	√
Few providers of critical core services on the market	1	
High market maturity	1	
Infrastructure of business location	1	
Products are subject to certification obligation	1	
Products used in adverse physical environments	1	
Provider has a depot of spare parts and components	1	

A.3 Indicators for the quality of IT risk management

Table 10: Indicators for the quality of IT risk management

Indicator	**Count**	**Selected**
Existence of an institutionalised risk management in the organisation	36	√
Business Continuity concept and contingency and emergency plans available	24	√
Existence of a proper IT Risk Reporting	23	√
International standards and best practices orientation (in general and with regard to IT)	19	√
Investments in further education and training of employees to increase security awareness	19	√
Information Security Certification(s)	17	√
Existing Role of a Risk Officer or Security Officer	15	√
IT-Management reports directly to the board level or is part of the board of directors	15	√
Security Policies for employees	14	√
IT-Service-management approach based on Standards (e.g. ITIL)	12	√
Policies concerning the handling of confidential information	12	√
Continual improvement process in Risk Management (PDCA Cycle)	10	√
Maintenance of a proper Loss database (Incident reporting)	10	√
Redundancies in the technical infrastructure	10	√
Documentation of IT-Infrastructure	6	√
Periodical internal and/or external audits	6	√
Accounted budget for IT Security present	4	√
Acceptance Testing required prior to release of new technologies and product versions	3	√
Existence of an IT-Governance function in the organisation	3	√
Existence of Protection requirements analysis	3	√
Physical control and registration of visitors at the entrance area	3	√
Physical protection measures	3	√
Quality Management System(s) Certification(s)	3	√
Size of the enterprise	3	√
Systematic Problem and Solution Management in the IT area	3	√

Continued on next page

Table 10 – continued from previous page

Age of the organisation	2	√
Employee Background Check	2	√
Measurement of performance indicators and and operating figures for assessing IT processes	2	√
Password Policy available	2	√
Policies and Guidelines for and control of external service providers	2	√
Definition of Life cycles for the IT-Infrastructure	1	√
Quality Assurance of published content (Legal Review)	1	√
Ratio of IT employees dedicated to security	1	√
Security Manual available	1	√
High degree of organisation	23	
Contracts contain liability exclusions or limits	15	
Comprehensive decision making for selecting product and service providers	6	
Provider subject to legal form obligations	6	
Business oriented management of IT risks	5	
Tidiness and cleanliness of IT premises	5	
Existing logical and physical security architecture	4	
Presence at risk forums and interest groups	4	
State of the art of technical security controls	4	
High security and quality requirements of customers	3	
Internal control system	3	
Asset-Management	2	
Corporate Governance Guideline	2	
Presence of risk provisions	2	
Pursuance and external communication of innovative IT projects	2	
Safeguards for organisational security	2	
Adequate backup facilities	1	
Availability of controlling instruments	1	
Clear specification of service level agreements with providers	1	
Contractually guaranteed alternatives in case of failure	1	
Crisis public relation	1	
Defined corporate communications interfaces	1	
Employee suggestion system	1	
License-Management	1	
Methodical approach to IT investment appraisal	1	
Portfolio-management of IT projects	1	