We are IntechOpen, the world's leading publisher of Open Access books Built by scientists, for scientists

4,800
Open access books available

122,000
International authors and editors

135M
Downloads

Our authors are among the

154
Countries delivered to

TOP 1%
most cited scientists

12.2%
Contributors from top 500 universities

CLARIVATE ANALYTICS BOOK CITATION INDEX INDEXED

WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?
Contact book.department@intechopen.com

Numbers displayed above are based on latest data collected.
For more information visit www.intechopen.com

16

Adopting and Adapting Medical Approach in Risk Management Process for Analysing Information Security Risk

Ganthan Narayana Samy[1], Rabiah Ahmad[2] and Zuraini Ismail[1]
[1]*Universiti Teknologi Malaysia (UTM),*
[2]*Universiti Teknikal Malaysia Melaka (UTeM)*
Malaysia

1. Introduction

Risk management process is defined as a systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying, analysing, evaluating, treating, monitoring and reviewing risk (AS/NZS ISO 31000:2009, 2009). In addition, precise security risk analysis method should provide two key advantages (Kim *et al*., 2007). Firstly, effective monitoring of information security policies by protecting organisations critical assets and secondly, capacity to provide appropriate information for the purpose of future prediction and for the development secured information management. However in the real world, most of the organisations do not have proper data about security breaches because they typically fail to document and systematically record the threats incidents (Bojanc and Jerman-Blazic, 2008). According to (Baker *et al*., 2007) stated that the lack of real data on risk factors is considered as one of the main problem in information security research. Therefore, most of the existing methods intended to estimate probability of an identified vulnerability of security breach is largely relied on guesswork or rough estimation (Baker *et al*., 2007; Ekelhart *et al*., 2009; Spears, 2006).

Moreover, the existing information security risk analysis methods have several shortcomings. First, only capable to identify specific threats such as a malicious attacks rather than various types of information security threats concurrency as stated in (Badr and Stephan, 2007; Kim *et al*., 2007). Second, it is more focus on technology rather than emphasis on the people and process aspects of information systems (Spears, 2006). Third, lack of systematic methods to measure the value of information systems assets from the viewpoint of operational continuity (Suh and Han, 2003). The following limitation of the traditional method is the time-consuming factor and higher cost involved in conducting such analysis especially in medium to large organisations (Spears, 2006). The next limitation is that most of existing methods depends largely on IT professionals or risk analysis experts to conduct the risk analysis. Finally, an IT-centric approach to information security risk analysis indicated it does not involve business users or variety of field managers to understand the risks and threats in promoting security awareness throughout an organisation (Spears, 2006).

Therefore, this research attempt to introduce a new method for performing risk analysis by effectively adopting medical approach namely survival analysis and adapting the risk management process. Under survival analysis approach, a method which is known as Cox Proportional Hazards (PH) Model can be applied to identify significant information security threats. Basically, the risk management process will be based on (AS/NZS ISO 31000:2009, 2009) which provides a sequencing of the core part of the risk management process including establishing the context, risk identification, risk analysis, risk evaluation and risk treatment. Thus, this chapter will describe in greater detail the adoptions and adaptions of medical approach in risk management processes, suitable research method that can be applied and expected benefits from proposed method.

This chapter is organised as follows. The next section describes the previous studies related to this research. Section 3 explains adoptions and adaptions of survival analysis and Cox PH Model in risk management process. Section 4 presents the suggested research method that can be applied in this research. Section 5 presents the discussion, followed by closure and future work in Section 6. Moreover, the following section which is related studies will discuss the existing information security risk analysis methodologies, description about medical research design and approach that related to this research for better understanding of proposed method.

2. Related studies

Basically, there are applications of various risks assessment methods in survivability studies. However, none of the information security risk analysis methodology adopts survival analysis approach or a study has not been previously reported in the research literature as described in (Ma and Krings, 2008b) in order to identify a potential information security threats or factors. Moreover, researchers and information security practitioners or risk analysts can predict better results of events occurring and factors influencing these occurrences more precisely when they adapt medical approaches (Ryan and Ryan, 2008a, 2008b).

2.1 Information security risk analysis methods

Basically, information security risk analysis methods are classified into quantitative, semi-quantitative and qualitative types (AS/NZS ISO 31000:2009, 2009; Badr and Stephan, 2007).

Risk Analysis and Management Method (CRAMM) was developed by Central Computer and Telecommunication Agency (CCTA) by United Kingdom's government (Aime *et al*., 2007). Current version of CRAMM is 5.1 which was released by Insight Consulting in 2005 based on existing best practices. Moreover, this current version complies with part two of the, BS7799 standard. CRAMM is divided into three stages namely; the first stage is asset identification and valuation, second stage is threat and vulnerability assessment and third stage is selection and recommendation. Basically, CRAMM provides well defined stages which cater for both the technical and the non-technical aspects of security. Furthermore, CRAMM will evaluate threats for both tangible and intangible assets. Moreover, this method also applies by combining the same kind of assets together in order to do a fast analysis. Thus, CRAMM contains a very large countermeasure library consisting of over

3000 detailed countermeasures organised into over 70 logical groupings (Siemens Enterprise, 2005). Therefore, this method can be used for reviewing security aspects, continuity and contingency planning, policy development and compliance, system development and compliance audits. CRAMM makes use of both the qualitative and quantitative elements. Fundamentally, CRAMM is a qualitative method, but the range of value can be transformed into quantitative values and subsequently combined to those values to produce values similar to "annual loss expectancy" value. Thus, the range of risks value is from one (low) to seven (high) (Bornman and Labuschagne, 2004; Siemens Enterprise, 2005).

According to (Maglogiannis and Zafiropoulos, 2006) presented a modelling approach for performing a risk analysis study of distributed HIS. This proposed method was based on basic features of the CRAMM risk analysis framework with the Bayesian Network modeling technique in order to identify assets, threats and vulnerabilities of healthcare information systems and present these interrelationships in a concise and flexible model. A case was applied to a healthcare information network operating in the North Aegean Region in Greece and the HIS assets, threats and vulnerabilities had been thoroughly analysed using the basic features of CRAMM. The findings of the analysis had been used to develop a Bayesian Network model to rank the threats with the highest risk, based on their posterior probability of occurrence in the case of the basic services and system failure (Maglogiannis and Zafiropoulos, 2006). Besides that, another study (Maglogiannis *et al*., 2006) also had applied CRAMM methodology as a framework in order to identify healthcare information systems threats and the corresponding risks. The initial findings from CRAMM are used for the construction of a fault tree model for representing the logical interrelationships of failure events. Finally, the relationship was represented using an advanced bayesian network model that provides greater flexibility in modeling failure event scenarios and highlighting system critical areas. The proposed risk analysis framework had been applied to patient monitoring system for homecare telemedicine, namely the VITAL-Home System.

Besides that, Construct a platform for Risk Analysis of Security Critical Systems (CORAS) is another information security risk analysis method which was developed under the European Information Society Technologies (IST) program. Development of CORAS had several purposes namely, semi-formal methods for object oriented modeling, developing a framework for risk analysis method and computerised tools for critical systems. Basically, CORAS relies on The Unified Modeling Language (UML) methodology. Basically, CORAS framework has four main pillars (Aagedal *et al*., 2002). The first pillar is risk documentation framework based on the Reference Model for Open Distributed Processing (RM-ODP). The second pillar is risk management process based on the Australian and New Zealand Standard (AS/NZS 4360:1999). The third pillar is an integrated risk management and development process based on Unified Process (UP). The fourth and last pillar is a platform for tool integration based on Extended Markup Language (XML).The CORAS risk management process is based on AS/NZS 4360:1999 Risk Management. It complements the Code of Practice for Information Security Management (ISO/IEC 17799:2000), Guidelines for the management of IT Security (ISO/IEC 13335:2001) and Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems (IEC 61508) (Aagedal *et al*., 2002).

Furthermore, according to (Bones *et al*., 2007) performed a risk analysis study to analyse the security challenges of an instant messaging (IM) service for healthcare industry based on CORAS risk management process framework. The methodology was based on the Australian and New Zealand standard for risk management (AS/NZS 4360/1999), which clearly sets out the risk analysis process in five main steps. The five main steps are namely, context identification, threat identification, impact and probability analysis, risk evaluation and risk treatment. The findings revealed a number of high risk or threats to instant messaging services used in the healthcare industry, namely, malicious software attacks due to unsecured network, intruder's attacks, hackers, power loss and failures on the device or programming errors.

The following information security risk analysis method is Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE). This method was introduced by the Carnegie Mellon Software Engineering Institute (SEI). This approach focuses on assets, threats and vulnerabilities. One of the main concepts of OCTAVE is self-direction. Primarily, OCTAVE relies on structured interviews as a tool in order to identify the critical for assets and it measures the level of risk. This means that, organisation's employees must lead the information security risk evaluation. Hence, an analysis team, consisting of staff from the organisation's business units as well as its IT department is responsible for leading the evaluation and recording of the results. The OCTAVE approach has three phases' namely organisational view, technological view and strategy and plan development phase (Bornman and Labuschagne, 2004). The three phases are build for asset-based threat profiles, identify infrastructure vulnerabilities and develop security strategy and plans. Each process has certain activities that must be completed, and within each of these activities, different steps must be taken in order to achieve the desired outputs. Finally, the result is based on threat profile of different assets. Each threat profile contains information on which mitigation decisions can it be based on. Basically OCTAVE method can be applied to large firms as well as for smaller firms which is known as OCTAVE-S (Caralli *et al*., 2007).

On top of that, (Coleman, 2004) applied OCTAVE method at three healthcare organisations of different scale, complexity and geographic location in order to access a risk associated with biomedical systems. The evaluation of risks in terms of organisational impact was found to be critically important and was the most influential factor considered when prioritizing risks for mitigation. The differences and similarities observed during the three risk assessments periods, strongly support the concept of a decentralised decision making approach to information security in the healthcare industry. The similarities found between these organisations were in terms of threats that were found in biomedical systems namely related to network infrastructure failures that should have been taken into consideration. In summary, this method allows each organisation the freedom to consider their own unique circumstances, tailor the methodology to their needs and document their decisions accordingly.

The next information security risk analysis method is Information Security Risk Analysis Method (ISRAM). ISRAM is a quantitative based approach using quantitative measures. ISRAM was developed at the National Research Institute of Electronics and Cryptology and the Gebze Institute of Technology in Turkey (Karabacak & Sogukpinar, 2005). This approach allows the interaction between the managers and staffs of the organisation in order to do risk analysis. Basically, ISRAM is a survey-based model which has two main elements of

risk namely, probability and consequence. ISRAM utilises numerical value between 1 and 25 as risk measure. This numerical value will act as qualitative measure for instance high, medium or low value. Finally, qualitative value will be used as a result for risk management decisions. The ISRAM methodology consists of seven steps (Karabacak and Sogukpinar, 2005).

Information Systems (IS) Risk Analysis Based on a Business Model is another risk analysis method which was developed by Korea Advanced Institute of Science and Technology (KAIST) in 2002 (Suh and Han, 2003). This model considers the replacement of assets and the disruption of operations together. Disruption of operations is a category of generic risks for example, consumer or buyer confidence, trust and goodwill of the company. This methodology has four stages namely starts with organisational investigation, asset identification and evaluation, threat and vulnerability assessment and finally annual loss expectancy calculation (Suh and Han, 2003).

2.2 Medical research design and approach

This section will presents the medical research and approach that going to applied in this research.

2.2.1 Retrospective cohort study

There are several different types of cohort studies (Euser *et al.,* 2009; Dunn and Clark, 2001). Type of cohort study that will be applied in this research is retrospective cohort study. Retrospective cohort study uses historical data to identify exposure level at some baseline in the past and respectively, follow-up for subsequent occurrences of disease between baseline and the present time (Friis and Sellers, 2010; Euser *et al.,* 2009).

2.2.2 Survival analysis approach

Survival analysis or failure time analysis is a specialised field of mathematical statistics as stated in (Ma and Krings, 2008c). Basically, survival analysis studies positive random variables with censored observations for describing times to events cases (Kleinbaum and Klein, 2005; Lee and Wang, 2003; Ma and Krings, 2008a, 2008b; Ricci, 2006). Events can be for example reaction from treatment or death and response of a disease. Therefore, "the study of survival data is focused on predicting the probability of response, survival, or mean lifetime, by comparing the survival distributions of experimental animals or of human patients and the identification of risk or prognostic factors related to response, survival, and the development of disease" as stated in (Lee and Wang, 2003).Examples of survival time are the lifetimes of organisms or survival times of cancer patients. There are several approaches to assess the associated risks with survival analysis namely, parametric, semi-parametric and non-parametric (Kleinbaum and Klein, 2005; Ma and Krings, 2008a, 2008b).

Generally, in survival analysis, collected data are subject to censoring (Kim *et al*., 2010). Basically, censored observations can be defined as an exact survival time of the observed subjects is unknown (Clark *et al*., 2003). Censoring may occur due to several reasons as stated in (Clark *et al*., 2003; Kleinbaum and Klein, 2005) namely:

i. A person is lost of follow-up during the study period;
ii. A person does not experience the event before the study ends;
iii. A person withdraws from the study due to death (if death is not the event of interest) or some other reason (for instance, adverse drug reaction or other competing risk).

There are three types of censoring namely, right censoring, left censoring and interval censoring. Generally, the three situation stated above are known as right-censored data. Basically, for these situations the complete survival time intervals, which we do not really know, has been cut off (censored) at the right side of the observed survival time interval.

According to (Lee and Wang, 2003),"left censoring occurs when it is known that the event of interest occurred prior to certain time, but the exact time of occurrence is unknown". For instance, if we wish to know the age of diagnosis in a follow-up study of diabetic retinopathy. Thus, at the time of the examination, a 50 year old participant was found to have already developed retinopathy. However, there is no record of the exact time at which initial evidence was found. Therefore, age at examination that is 50 is a left-censored observation. Hence, it means that the age of diagnosis for this patient is at most 50 years. Interval censoring occurs when the event of interest is known to have occurred between times a and b. For example, according to medical records, it indicates that at the age of 45 years, the respondent did not have retinopathy, his age at diagnosis is between 45 and 50 years.

However, the survival analysis approach has unique mathematical models and methodologies that have been developed in order to extract the partial information from the censored observations without creating any unwanted biasness as mentioned in (Ma and Krings, 2008a) and considered as one of benefit which can be adopt by organisation to conduct risk analysis. Further description of survival analysis with censored data will be discussed in sub section 5.2.2. The following section will describe the Cox Proportional Hazards model which is one of the methods used in survival analysis for analysis data.

2.2.3 Cox proportional hazards (PH) model

Cox Proportional Hazards (PH) model, a popular mathematical model and is widely used for analysing survival time data in medical research. Basically, Cox PH model is a semi-parametric approach. In this research, Cox PH model will be used. Initially, Cox PH model proposed by Cox (1972, 1975) is treated as largely an empirical regression model, but later it was found that the framework of the model possesses exceeding flexibility to capture major hazards effects and failure mechanisms (Bradburn *et al*., 2003; Kleinbaum and Klein, 2005; Lee and Wang, 2003; Ma and Krings, 2008a, 2008b, 2008c).

Basically, Cox PH model is a method for modeling time-to-event data in the presence of censored cases (uncompleted observation). However, Cox PH model allows inclusion of explanatory/predictor variables in the models. Cox PH model will handle the censored cases correctly, and it will provide estimated coefficients for each of the explanatory variables. Besides that, Cox PH model allows us to assess the impact of multiple explanatory variables in the same model. Thus, we can find out which explanatory variables or factors have significant impact on the event and forecast the survival probability according to the influence of factors. Cox (PH) model also can be used to examine the effect of continuous explanatory variables as mentioned in (Lee and Wang, 2003). Therefore, in survival analysis,

event of the incidences will be presented in terms of hazard function and of covariates (Bradburn *et al*., 2003).

The formula for the Cox PH model as expressed in (1), where the hazard function h(t) is dependent on (or determined by) a set of p covariates (x1, x2 …...xp), whose impact is measured by the size of the respective regression coefficients (b1, b2..…,bp). The term h_0 is called the baseline hazard, and is the value of the hazard if all the xi are equal to zero (the quantity exp(0) equals 1).

$$h(t) = h_0(t) \times \exp\{b_1x_1 + b_2x_2 + \ldots.. + b_px_p\} . \quad (1)$$

The Cox model is basically a multiple linear regression of the logarithm of the hazard on the variables x_i with baseline hazard being an 'intercept' term that varies with time. The covariates then acts multiplicatively on the hazard at any point in time and this provides the key assumption of the PH model that the hazard of the event in any group is a constant multiple of the hazard in any other group. Thus, this assumption shows that the hazard curves for the groups should be proportional and will not cross.

This proportionality implies that the quantities $\exp(b_i)$ are called hazard ratios. A value of b_i greater than zero, or equivalently a hazard ratio greater than one, shows that as the value of the ith covariates increases, the event hazard increases and, thus the length of survival decreases. Eventually, a hazard ratio above 1 indicates a covariate that is positively associated with the event probability and negatively associated with the length of survival. In this research, Cox PH model is defined h_0 (t) as the baseline hazard function. The covariates or explanatory variables in this research will be the potential threats that might affect the information systems which cause failure to system.

2.2.4 The application of survival analysis

Survival analysis has a track record for last two decades and has become the de facto standard in biomedical research (Ma and Krings, 2008a). However, today survival analysis has become a major tool for other fields of study for instance, in engineering reliability, networking and software reliability and survivability, machine learning, and prognostics and health management as stated in (Ma and Krings, 2008a, 2008b; Samrout *et al*., 2009)

There are many examples of application of survival analysis approach in the medical field for example, which was done by (Ghazali *et al*., 2010). The purpose of this study is to identify the five years of survival rate and prognostics factors for survival in patients with colorectal cancer. Therefore, in this research, Cox PH model was applied to model the prognostic factors for survival. In summary, factors such as Dukes staging, status of liver metastases and type of treatment are identified as an important independent predictors for survival in patients with colorectal cancer. Moreover, the results also further indicates that the patients with Dukes C staging together with the presence of liver metastases and who are treated with both chemotherapy and radiotherapy are at the greatest risk of death from colorectal cancer.

Another example of survival analysis application in medical domain is presented by (Maida *et al*., 2009) and that study shows that certain selected wound may affect the survivability of cancer patients. Therefore, this study conducted a prospective observational study of 418

advanced cancer patients and derived hazard ratios (HRs) from Cox PH models. The result shows that the presence of pressure ulcers particularly in female cancer patients and 'other' type of wounds in all cancer patients contributes to reduce survival rate. Furthermore, this useful data can be used as an important measure in existing prognostic model in order to enhance prognostic accuracy.

Rabiah, (2006) combines Cox Proportional Hazard Regression and Genetic Algorithms (CoRGA) in order to select variables. In addition, CoRGA was applied to select best combination of risk factors for four-years, eight-years and fifteen-years, all-cause mortality in older people. In addition, CoRGA was used to identify risk factors for mortality in older men and women separately. The results show that CoRGA was able to select a variety of risk factors for short, medium and long-term, and all-cause mortality and also was able to identify new risk factors for mortality. In summary, CoRGA has the potential to complement traditional statistical methods for analysing survival data, particularly in the identification of putative risk factors for all-cause mortality in communities with older people.

The survival analysis approaches is also suitable to be applied in other fields such as in reliability engineering, social sciences and business. Examples of survival analysis in these fields are the life time of electronic devices, components or systems and workers compensation claims (insurance) and their various influencing risk or factors (Lee and Wang, 2003). Besides that, according to (Ma and Krings, 2008b, 2011) stated that other field of computer science and engineering also has great potential benefits by adopting survival analysis approach for example in network reliability and survivability as well as in prognostics and health management which merits further research. Recent evidence has reported that the application of Cox PH model in the reliability engineering field has increased (Samrout *et al*., 2009). Moreover, according to (Samrout *et al*., 2009) studies show that the Cox PH model is used as a modeling tool to integrate the effect of the corrective maintenance on the component's reliability through its relation on the component's age. Finally, the findings show that the corrective maintenance affects on the failure rate and has an effect on the adopted preventive maintenance policy.

Based on (Guo and Brooks, 2009) stated that adoptions of Cox PH model in order to analysis the duration from offering to listing using the data of Chinese A-share IPOs gives several benefits. For example, capability to incorporate information whether censored and uncensored observations to provide consistent parameter estimates and finally the results can be more precise to forecast and assess the listing hazard for a new offering. Therefore, Cox PH model is used in order to identify factors significantly related to the issuer's final listing. In summary, the findings are found to be significant for most of the endogenous factors that affect the issuing system, but factors for example offering price and floatation size reduce in favour of the effect of issuing year.

Besides that, survival analysis approach also has ability to demonstrate the characteristics of unemployment duration in Slovenia as stated by (Borsic and Kavkler, 2009). That study investigated the influence of several variables such as age, gender, level of education, and region using Cox PH model. Primarily, this study stated that Cox PH model has a potential to estimate the ratio of chances of employment for two selected groups of unemployment. Moreover, the results show that it takes a longer time for female and older unemployed persons to find a job and on the average the duration of unemployment decreases with increasing level

of education. Also, the outcome of analysis stated that the results can help to identify potential unemployed target groups in order to improve the effectiveness of the employment policy.

According to (Ma and Krings, 2008c) presents a new dynamic hybrid fault models by extending the traditional hybrid fault models with survival analysis and evolutionary game theory. The application domain is Wireless Sensor Network (WSN). Basically, this research introduces survival analysis, which offers time and covariate dependent hazard or survivor functions. This research used Weibull survival distribution models to simulate the time-dependent survivor function of WSN nodes. The findings show that the new dynamic hybrid fault model which transforms hybrid fault model into time and covariate dependent models and make real-time prediction of reliability more realistic and also allows for real-time prediction of fault-tolerance. Furthermore, this research sets the foundations for integrating the hybrid fault models with reliability and survivability analysis by introducing the evolutionary game modelling and extends the evolutionary game theory in its modelling for the survivals of game players.

Section 2 and sub-sections discussed the related studies in this research in depth. Therefore, the next section will emphasise on how the proposed method been adopt and adapt into risk management process.

3. Adopting and adapting survival analysis and cox PH model into risk management process

This section is divided into two main sections. Section 3.1 and sub-sections presents the description of the proposed method according to risk management process in greater detail. Section 3.2 explains differences between general risk management processes with adoptions and adaptions of medical research design and approach in risk management processes.

3.1 Risk management processes in detail

Risk management process methodology is based on (AS/NZS ISO 31000:2009, 2009). This standard clearly sets out the risk management process into five main processes including, establishing the context, risk identification, risk analysis, risk evaluation and risk treatment. The Fig. 1 shows the main elements of risk management process and will be described in greater detail in the following sub-sections.

3.1.1 Communication and consultation

(AS/NZS ISO 31000:2009, 2009) define communication and consultation as "continual and iterative processes that an organisation conducts to provide, share or obtain information and to engage in dialogue with stakeholders regarding the management of risk". In addition, this component serves as a communication platform for stakeholders at all stages of risk management process (AS/NZS ISO 31000:2009, 2009).

3.1.2 Establishing the context

Establishing the context defines various types of context namely external, internal, risk management process context and sets the scope and risk criteria for following process

with its organisational environment in order to evaluate risk (AS/NZS ISO 31000:2009, 2009). Furthermore, the measurement variables for risk criteria are regression coefficient (bi), hazard ratio [exp (bi)] and p-Value will be used as risk criteria in order to measure the level of risk and to determine which variables are significant information security threats.

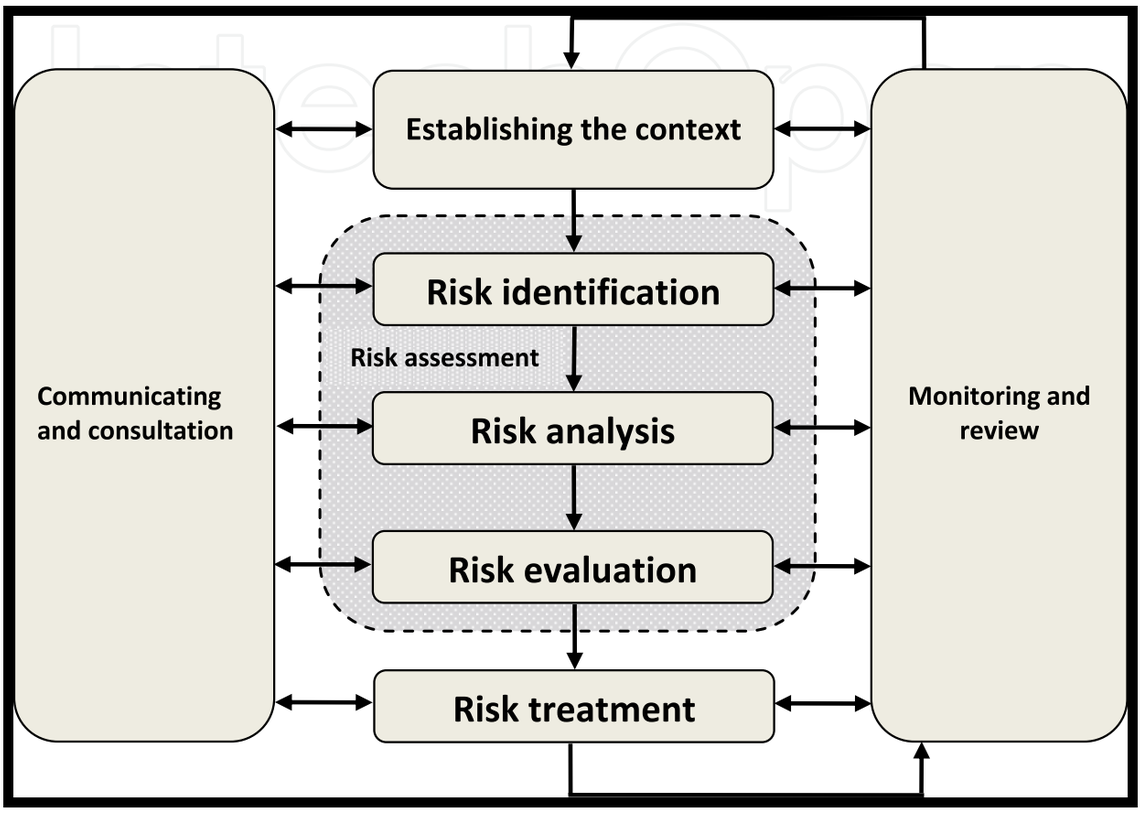


Fig. 1. General Overview of Risk Management Process according to (AS/NZS ISO 31000:2009, 2009)

3.1.3 Risk identification

The following component of risk management process is risk identification process. This process seeks to identify what, why and how the risks can arise and also as an input for further analysis (AS/NZS ISO 31000:2009, 2009). Further identification of appropriate tools and techniques used to identify risks will be carried out at this juncture. There are various methods used to identify risks for instance, brainstorming, scenario analysis, judgments based on experience and records and systems engineering techniques (AS/NZS ISO 31000:2009, 2009). However, the method that is going to be applied should represent or must be capable to identify types of risks correctly.

3.1.4 Risk analysis

Risk analysis process determines the level of the risk. By having identified the various kinds of potential threats from previous processes it will be used as a list of factors in order to

analysis the risks. In addition, method of analysis will be dependent on the purpose of the analysis and also the availability of related information. Methods of analysis can be qualitative, semi-quantitative or quantitative or a combination of any two or three of the above depending on the situations. Furthermore, risk analysis process provides an input to risk evaluation process in order to select appropriate risk treatment strategies and methods to manage the risk (AS/NZS ISO 31000:2009, 2009). According to (AS/NZS ISO 31000:2009, 2009), the risk analysis process will focus to an estimate risk level which is derived from combination of likelihood and consequence.

However in this research, the proposed method namely, retrospective cohort study based on survival analysis will be applied to determine the level of risk. Under survival analysis approach, Cox PH model will be applied to identify which information security threats or independent variables such as technological obsolescence, hardware failures, software failures, malware attacks and power failure is most significant.

According to survival analysis perspectives, status variable (dependent variable) is coded in binary value such as 0 or 1. Therefore in this research, 1 is defined for failure if the event occurs during the study period, and 0 if the event does not happen. Finally, a number of systems will be analysed, for example 200 systems, the duration of the study period (for instance in years, months, weeks or days), its status variable together with its independent variables (explanatory variables) that might be a threats to the system failure will be analysed according to survival analysis which is using the Cox PH model as depicted in Fig. 2.

The final output from the Cox PH model will produce an estimate of hazard ratio of several explanatory variables. Basically, explanatory variable with positive regression coefficients are associated with decreased survival times (increased hazard), while variable with negative regression coefficients are associated with increased survival times (decreased hazard). Thus, based on the findings, the explanatory variables which has high hazard ratio will be consider for following process for evaluation purpose.

3.1.5 Risk evaluation

The purpose of this process is to compare the level of risk results found during the risk analysis process with risk acceptance criteria (AS/NZS ISO 31000:2009, 2009). The result of a risk evaluation is a prioritised list of risks for further analysis. A prioritised list of risks for risk treatment process will be diagnosis according to the medical perspectives namely; hazard ratio which is produced by Cox PH model results in order to determine the most predictor or significant variables. Where the most significant variables considered has a greater impact it, will be forwarded to the next process for treatment purposes.

3.1.6 Risk treatment

(AS/NZS ISO 31000:2009, 2009) stated that risk treatment as "involves selecting one or more options for modifying risks, and implementing those options and once implemented, treatments provide or modify the controls". The first step in risk treatment process is selecting the most appropriate risk treatment option by taking care of values and perceptions of organisation or stakeholders. Thus, in this research Cox PH model which

produced hazard ratio will be used as an indicator to measure the level of risk for identified threats. The next step is to prepare and implement the chosen risk treatment plans. Consequently, the treatment options should be incorporated accordingly with the organisations management processes and also discussed with the appropriate stakeholders (AS/NZS ISO 31000:2009, 2009).

3.1.7 Monitoring and review

According to (AS/NZS ISO 31000:2009, 2009) monitoring is defines as "continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected". On the other hand, review is the "activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives" (AS/NZS ISO 31000:2009, 2009). Besides this, any other factor which affects the treatment options also need to be considered in this process. Therefore, it is vital to repeat the risk management cycle on a regular basis in order to identify unwanted risks.

3.2 Medical research design and approach in risk management processes

Fig. 2. illustrates clearly the differences between general risk management processes with adaptions of medical research design and approach in risk management processes. There are three main differences in three different risk management processes. Firstly, under establishing the context process, one of the subsections of this process that is defining the risk criteria will be based on medical approach. According to (AS/NZS ISO 31000:2009, 2009) stated that organisation should define criteria or measure that going to used as an indicator to evaluate the level of risk. Therefore, in this research the establishment of measure will be based on medical approach namely, regression coefficient (b_i), hazard ratio [exp (b_i)] and p-value will be used as risk criteria in order to measure the level of risk and to determine which variable is significant threats based Cox Proportional Hazards (PH) Model output as shown in Fig. 2.

The second most significant dissimilarity can be observed in risk analysis process clearly. Basically, the general components of risk analysis process in order to measure the level of risk according to (AS/NZS ISO 31000:2009, 2009) is combination of livelihood and consequences. However in this research, the level to risk is determine completely based medical research design and approach as depicted in Fig. 2. above. Moreover, the interpretations the level of risk will be based on hazard ratio as an outcome of adopting the cohort study based survival analysis in this process. The following distinction can be noticed in risk evaluation process. In general risk management process, the evaluation of risk is based on outcomes of risk analysis process as mentioned in (AS/NZS ISO 31000:2009, 2009). Therefore in this research, the outcome from the risk analysis process will be evaluated based on medical perspectives as shown in Fig. 2.

4. Method

This section will discuss about suggested research method design that can be applied, justification for chosen research design, assumptions for collecting and analysis data and data analysis software that can used for analysis the collected data.

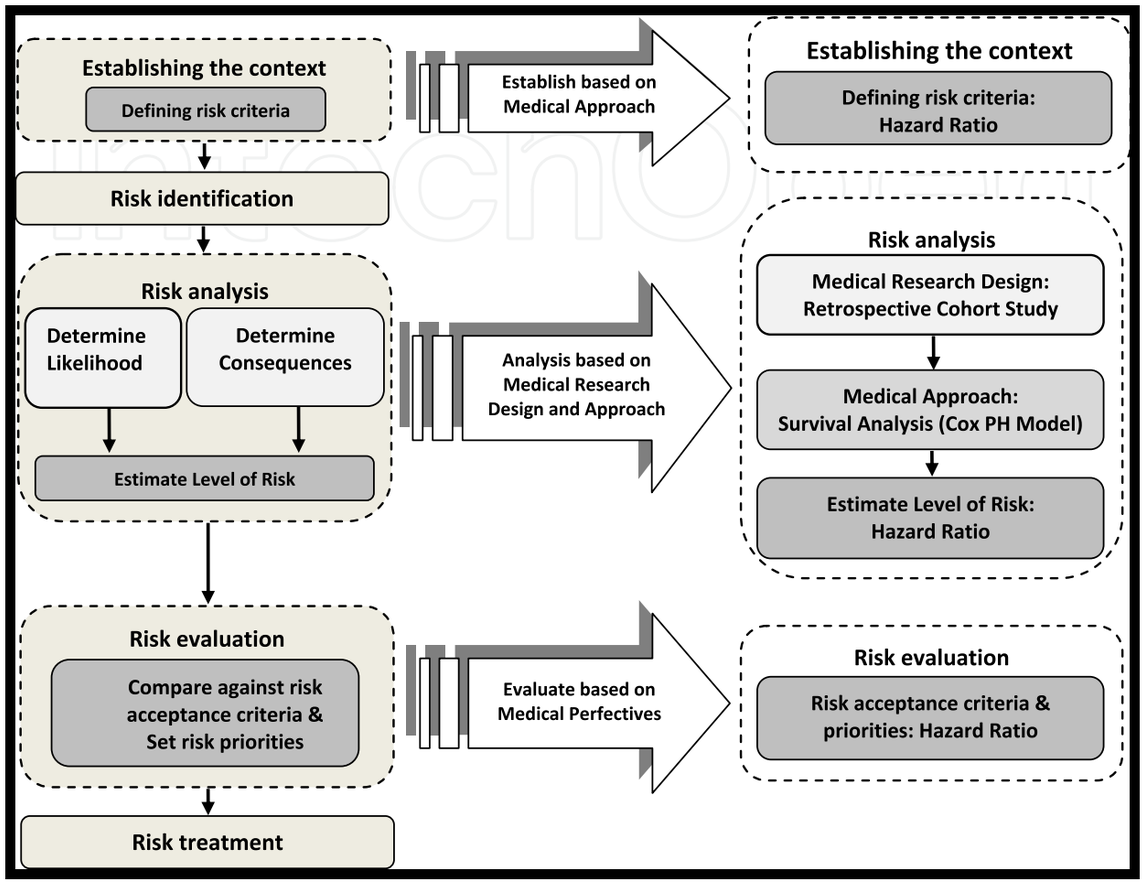


Fig. 2. Differences between General Risk Management Processes with Adoption and Adaption of Medical Research Design and Approach in Risk Management Process

4.1 The suggested research method design

The mixed method design was chosen for this research is termed as exploratory sequential mixed method design. Basically, the first phase of study will be a qualitative exploration (i.e. identification of potential information security threats). From this initial exploration, the qualitative findings (i.e. potential information security threats) will be used as an instrument for following phase. The second phase will be using quantitative approach as a follow up to the qualitative results in order to administer larger sample according to survival analysis approach in order to interpret the entire findings. Thus, in this research, exploratory sequential design is divided into two phases namely qualitative analysis which will take place in the risk identification process and this is followed by the quantitative analysis in the risk analysis process as illustrated in Fig. 3.

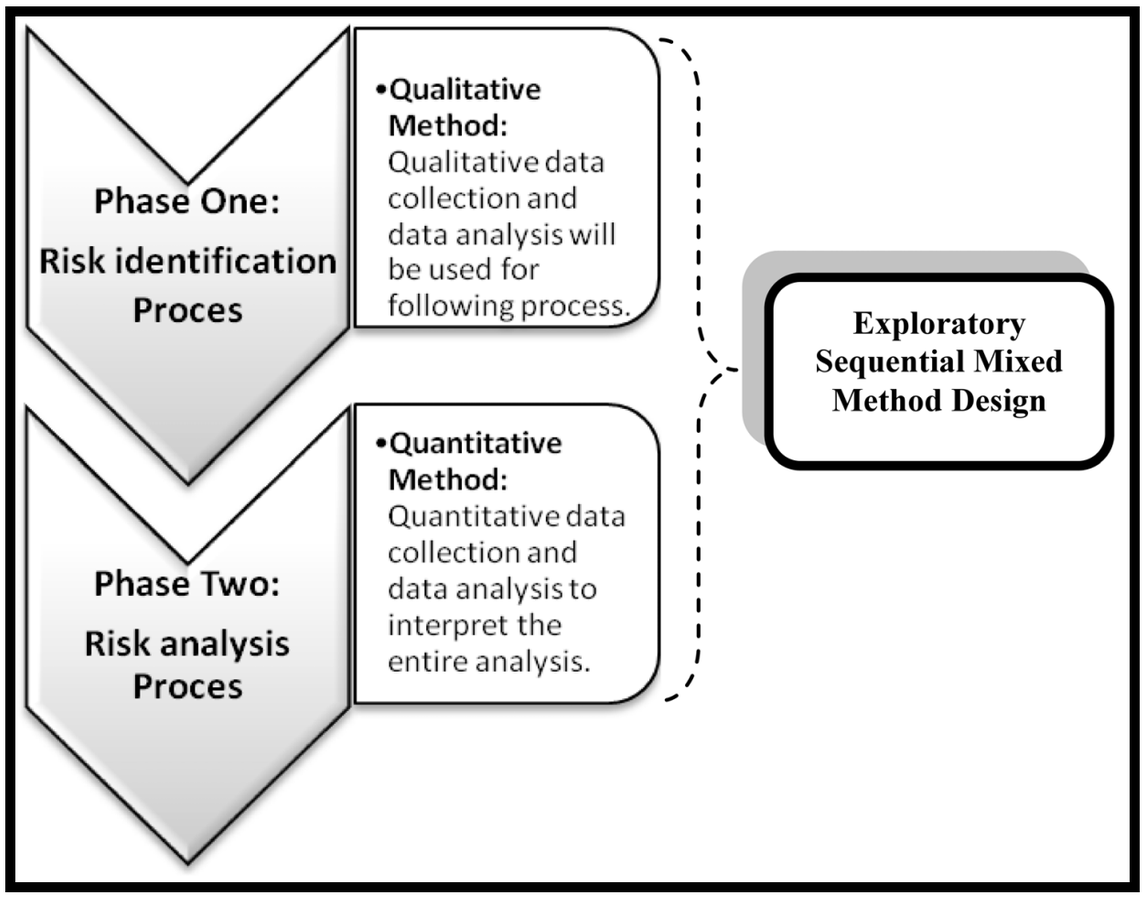


Fig. 3. The Research Design Overview

4.1.1 Justification for chosen research design

There are several key reasons for choosing this method. The reasons are as follows:-

i. The appropriateness to get the intended findings precisely. The exploratory sequential design is most suitable for this research as the results of the first phase, qualitative method basically can assist to develop the second phase, quantitative method (Creswell and Clark, 2011). Moreover, it has the ability to answer the proposed research questions correctly. The researchers cannot answer the proposed research questions using the qualitative method alone. Hence, the combinations of qualitative and quantitative methods are necessarily important in order to answer these research questions.
ii. The usefulness in order to identify important variables to study quantitatively when the variables are unknown (Creswell and Clark, 2007, 2011). There is a importance to conduct qualitative analysis at an early phase that is at the risk identification process in order to identify the potential information security threats and later to use it as a list for the following phase that is at the risk analysis process in order to select the most significant variable using the quantitative analysis.

iii. According to (Creswell and Clark, 2007, 2011) stated this kind of research design is suitable "when a researcher wants to generalise qualitative results to different groups, to test aspects of developing theory or classification, or to explore a phenomenon in depth and then to measure the prevalence of its dimensions". Therefore, this selected research design method is well suited to this research.

4.2 Assumptions for collecting and analysis data

This research has the following assumptions:-

i. In this research all the covariates or variables that is included in the PH Cox model as assumed as time independent variable. According to medical perspective, a time-independent variable is defined to be any variable whose whole value for given individual does not change over time (Kleinbaum and Klein, 2005). For instance, smoking status can change over the period, but for the purpose of research, the smoking covariate is believed as not change once it is measured and only one value per individual is used as stated in (Kleinbaum and Klein, 2005).
ii. Recurrent or repeated events of same variables during the follow-up time for given subject are not included in this research. Thus, the researcher in this research assumes that only first time occurrence of selected variables will be counted for the analysis.
iii. In general, cohort studies are said to be bias due to high rate of lost of follow-up or censored data. In addition, high amount of censored data will affect the significances of result. Thus in this research, the researcher assumes that censored data is low as provided by secondary sources in order to ovoid biasness from expected outcome.
iv. In this study, only the right censored data will be included for analysis.

4.3 Data analysis software

In this research, data analysis will be performed using Predictive Analytics SoftWare (PASW) Statistics, version 18.0. This software has been widely use in analysing statistical data in the medical domain and is well suited for the analysis survival data in this research.

The following section will explain the risk criteria definition and advantages of adopting and adapting medical research design and approach in risk management process.

5. Discussion

The following sub sections will discuss the risk criteria based on the medical interpretation in risk management, advantages adopting and adapting a retrospective cohort study, survival analysis approach and Cox PH model in depth.

5.1 Defining risk criteria

Risk criteria will be based on the medical perspective as described in Table 1. below. Therefore, risk criteria measures namely, regression coefficient (b_i), hazard ratio [exp (b_i)] and p-value will be used as an indicator in order to measure the level of risk in this research. Thus, the following table will describe each variable in more detail in terms of regression cofficient, hazard ratio and p-value with appropriate interpretation.

Measurement Variables	Measurement Value	Medical Perspective Interpretation	Adaption in Risk Management Perspective & Interpretation
Regression Coefficient (b_i)	Positive Coefficient	Associated with decreased survival times (increased hazard) that is risk of death is higher, and the prognosis worse	High level of risk
	Coefficient = 1	No relationship/does not influence survival times	Insignificant
	Negative Coefficient	Associated with increased survival times (decreased hazard) that is risk of death is low, and the better prognosis	Low level of risk
HR-Hazard Ratio [exp (b_i)]	HR > 1	Variable increase the odds of the event occurring (decreases survival times). Example: HR = 5, Exposed group has five times higher the hazard of the unexposed group	Exposed group has higher level of the hazard compare to unexposed group which is depends on HR value and $\boldsymbol{b_i}$ sign (positive/negative coefficient)
	HR = 1	No effect	Insignificant variable
	HR < 1	Variable less the odds of the event occurring (increasing survival times) Example: HR = 0.5, Exposed group has 0.5 times higher the hazard of the unexposed group	Exposed group has lower level of the hazard compare to unexposed group which is depends on HR value and $\boldsymbol{b_i}$ sign (positive/negative coefficient)
***p*-Value**	< 0.05	Variable is significant	Variable have significant impact /influence
	> 0.05	Insignificant variable	Variable does not have significant impact /influence

Table 1. Risk Criteria Measure

5.2 Advantages adopting and adapting medical research design and approach

The following subsections will explain the benefits adopting and adapting medical research and approach in this research.

5.2.1 The advantages adopting and adapting a retrospective cohort study

There are several advantages of using a retrospective cohort study. According to (Euser *et al*., 2009; Friis and Sellers, 2010) stated that the major advantage of this cohort design is does not required long follow up period of observation like prospective cohort study. Therefore this cohort design is time efficient and also suitable to discover new findings based on exiting data as mentioned in (Euser *et al*., 2009). Moreover, this cohort design also does not need a huge amount of expenses in order to conduct the study and at the same time capable to collect sufficient amount of date that required for research as stated in (Friis and Sellers, 2010). Thus based on advantages in term of time and cost factor lead to choose this cohort design in this research. Thus, this advantage can be adapted into risk management process for data collection purpose in order to identify information security threats.

5.2.2 The advantages of adopting and adapting survival analysis approach

Basically, there are many reasons or benefits using survival analysis approach. Firstly, researcher, information security practitioners or risk analyst can predict the study of events occurrence and factors influencing their occurrence more precisely. Further, this approach is more efficient, is a powerful tool and brings more benefits compared to other methods namely, the artificial neuron networks (ANN), evolutionary computing, fuzzy logic, decision tree approach and logistic regression as stated in (Chen *et al*., 2009; Ma and Krings, 2008b; Ma, 2009).

In addition, certain independent variables in reliability engineering field which is related to failure time analysis cannot be analysed using multiple regression techniques. For example, multiple linear regression technique cannot be used for analysis of time-to-event data due to the limitation to handle censored observations or cases for which the event of interest has not yet occurred. Therefore, survival analysis approach such as the Cox PH model is recommended. Thus, survival analysis approach can generate more dynamic characteristics of the event, which were not found in traditional methods (Ma, 2009; Norusis, 2004; Yu and Bi, 2008).

Besides that, the flexibility of the survival analysis approach itself, i.e., information censoring. (Ma and Krings, 2008a) stated that information censoring as "observation of survival times is often incomplete". Basically, the survival analysis approach has unique mathematical models and methodologies that have been developed in order to extract the partial information from the censored observations without creating any unwanted biasness as mentioned in (Ma and Krings, 2008a). Meanwhile, this approach also can be used to identify which factors have significant impact on the event and forecast the survival probability according to the influence of factors (Ma and Krings, 2008a, 2008b; Yu and Bi, 2008). Therefore, it is important to introduce survival analysis in risk management process. Therefore, this advantage can be used as a tool among the organisations that lack appropriate data to do risk analysis practice. Moreover, the organisation no need to worried about the reliability of result due to ability to handle incomplete data in appropriate manner is the most important and unique advantage of survival analysis approach (Ma and Krings, 2008a, 2008b).

5.2.3 The advantages of adopting and adapting cox proportional hazards (PH) model

In this sub section we are going to discuss a key reasons why we are choosing the Cox PH model for our research. Basically, Cox PH model is robust. This is because, even though the baseline hazard is not specified, reasonably good estimates of regression coefficients, hazard rations of interest and adjusted survival curves can be obtained for a wide variety of data situations. Thus, the results from using this Cox PH model will closely approximate the results for the correct parametric model as stated in (Kleinbaum and Klein, 2005).

Secondly, the Cox PH model is very reliable. Hence, when we may not be completely certain that a given parametric model is appropriate then the Cox PH model will give reliable enough results, so that, it is a safe choice of model to be used. Moreover, the researchers do not need to worry if a wrong parametric model is chosen (Kleinbaum and Klein, 2005). Moreover, the Cox PH model also is a powerful technique to examine the simultaneous relationship of the variables to survival as mentioned in (Lee and Wang, 2003). Basically, the identification of each variable can only identify which variable is significant. However, to determine the simultaneous effect of the variables, an appropriate multivariate statistical method is needed to apply (Lee and Wang, 2003). In this sense, the Cox PH model can be applied.

6. Closure and future research

Firstly, an important contribution of this proposed method is adopting a medical research design and approach and adapting them into risk management process in order to identify potential or influential information security threats, which previously were not undertaken. Therefore, this new way of conducting risk analysis studies holds significant impact among information security practitioners and risk analysis experts in order to identify and manage their information security breaches more effectively. Thus, this will be a new breakthrough in the field of risk management and information security in order to gain advantage using other domains approach.

The following contribution is flexibility of proposed method compared to existing information security risk analysis methods. The most important advantage adopting medical approach namely in survival analysis is information censoring. Information censoring referring to the observation of survival times is often incomplete. Basically, survival analysis approach has unique mathematical models and methodologies that have been developed in order to extract the partial information from the censored observations without creating unwanted bias. Therefore, existing organisation particularly small and medium size can conduct risk analysis studies in order to identify potential information security threats even though they does not have incomplete data about security breaches. Moreover, from the analysis the particular organisation can take appropriate security measure in order to prevent unwanted security breaches.

Lastly, this study provides guidelines for information security practitioners, risk analysts and for top level management in terms of making investment by focusing on the most significant threats based on a proposed method in order to manage their threats effectively. As a result, risk analysis outcomes will be used by organisations in order to identify the gaps in the existing security controls, policies and procedures.

Adopting and adapting medical research design and approach in risk management process in order to identify potential information security threats which are not previously been undertaken. Therefore this chapter discusses the proposed method according to medical perspective in risk management processes in detail. Moreover, the proposed method will be applied in selected government supported hospitals in Malaysia in order to identify potential information security threats in healthcare information systems. Thus, the expected results will be demonstrate the applicability of medical approach in risk management process and in information security domain.

7. References

Aagedal, J. O., den Braber, F., Dimitrakos, T., Gran, B. A., Raptis, D., & Stolen, K. (2002). Model-based risk assessment to improve enterprise security, *Proceedings of Sixth International Conference on Enterprise Distributed Object Computing, 2002 (EDOC'02)*, pp. 51–62, 2002

Aime, M. D., Atzeni, A., & Pomi, P. C. (2007). AMBRA: automated model-based risk analysis, *Proceedings of the 2007 ACM workshop on Quality of protection*, pp. 43–48, 2007

Aschengrau, A., & Seage, G. R. (2003). *Essentials of epidemiology in public health*, Jones & Bartlett Learning

Badr, Y. & Stephan, J. (2007).Security and risk management in supply chains. *Journal of Information Assurance and Security*, Vol. 2 (4), pp. pp. 288-296

Baker, W. H., Rees, L. P., & Tippett, P. S. (2007). Necessary measures: metric-driven information security risk assessment and decision making. *Communications of the ACM*, *50*(10), pp. 101–106

Bhopal, R. S. (2002). *Concepts of epidemiology: an integrated introduction to the ideas, theories, principles and methods of epidemiology*, Oxford University Press, New York

Bojanc, R., & Jerman-Blazic, B. (2008). Towards a standard approach for quantifying an ICT security investment. *Computer Standards & Interfaces*, *30*(4), pp. 216–222

Bones, E., Hasvold, P., Henriksen, E., & Strandenaes, T. (2007). Risk analysis of information security in a mobile instant messaging and presence system for healthcare. *International journal of medicl informatics*, *76*(9), pp. 677–687

Bonita, R., Beaglehole, R., & Kjellstrom, T. (2006). *Basic epidemiology*, WHO

Bornman, W. G., & Labuschagne, L. (2004). A comparative framework for evaluating information security risk management methods. *Proceedings of the ISSA 2004 enabling tomorrow Conference*, 2007

Borsic, D., & Kavkler, A. (2009). Modeling Unemployment Duration in Slovenia using Cox Regression Models. *Transition Studies Review*, *16*(1), pp. 145–156

Bradburn, M. J., Clark, T. G., Love, S. B., & Altman, D. G. (2003). Survival analysis part II: Multivariate data analysis–an introduction to concepts and methods. *British journal of cancer*, *89*(3), pp. 431-436

Caralli, R. A., Stevens, J. F., Young, L. R., Wilson, W. R., & INST, C.-M. U. P. P. S. E. (2007). *Introducing octave allegro: Improving the information security risk assessment process*, Citeseer

Chen, Y., Zhang, H., & Zhu, P. (2009). Study of Customer Lifetime Value Model Based on Survival-Analysis Methods, *WRI World Congress on Computer Science and Information Engineering,* pp. 266–270, 2009

Clark, T. G., Bradburn, M. J., Love, S. B., & Altman, D. G. (2003). Survival analysis part I: basic concepts and first analyses. *British journal of cancer*, *89*(2), pp. 232-238

Coleman, J. (2004). Assessing information security risk in healthcare organizations of different scale, *International Congress Series*, pp. 125–130, 2004

Creswell, J. W, & Clark, V. L. P. (2007). *Designing and conducting mixed methods research*, Sage Publications, Inc.

Creswell, John W., & Clark, D. V. L. P. (2011). *Designing and Conducting Mixed Methods Research* (Second Edition.), Sage Publications, Inc., California

Dunn, OL., VA. Clark, VA. (2001). *Basic Statistics: A Primer for the Biomedical Sciences*, John Wiley & Sons, New York

Ekelhart, A., Fenz, S., & Neubauer, T. (2009). AURUM: A framework for information security risk management. *42nd Hawaii International Conference on System Sciences, 2009 (HICSS'09)*, pp. 1–10, 2009

Euser, A. M., Zoccali, C., Jager, K. J., & Dekker, F. W. (2009). Cohort studies: prospective versus retrospective. *Nephron Clinical Practice*, *113*(3), pp. 214–217

Friis, R. H., & Sellers, T. (2010). *Epidemiology For Public Health Practice* (4th ed.), Jones & Bartlett Learning

Ghazali, A. K., Musa, K. I., Naing, N. N., & Mahmood, Z. (2010). Prognostic Factors in Patients With Colorectal Cancer at Hospital Universiti Sains Malaysia. *Asian Journal of Surgery*, *33*(3), pp. 127–133

Guo, H., & Brooks, R. (2009). Duration of IPOs between offering and listing: Cox proportional hazard models–Evidence for Chinese A-share IPOs. *International Review of Financial Analysis*, *18*(5), pp. 239–249

Karabacak, B., & Sogukpinar, I. (2005). ISRAM: information security risk analysis method. *Computers & Security*, *24*(2), pp. 147–159

Kim, Y. G., Jeong, D., Park, S. H., Lim, J., & Baik, D. K. (2007). Modeling and Simulation for Security Risk Propagation in Critical Information Systems. *Computational Intelligence and Security*, pp. 858–868

Kim, Y., Kim, B., & Jang, W. (2010). Asymptotic properties of the maximum likelihood estimator for the proportional hazards model with doubly censored data. *Journal of Multivariate Analysis*, *101*(6), pp. 1339–1351

Kleinbaum, D. G., & Klein, M. (2005). *Survival analysis: a self-learning text* (2nd. edition), Springer, New York

Lee, E. T., & Wang, J. W. (2003). *Statistical methods for survival data analysis* (3rd. edition). Wiley-Interscience, New Jersey

Ma, Z., & Krings, A. W. (2011). Dynamic Hybrid Fault Modeling and Extended Evolutionary Game Theory for Reliability, Survivability and Fault Tolerance Analyses. *IEEE Transactions on Reliability*, *60*(1), pp. 180–196

Ma, Z. (2009). A new life system approach to the prognostic and health management (PHM) with survival analysis, dynamic hybrid fault models, evolutionary game theory, and three-layer survivability analysis, *Aerospace conference, p*p. 1–20, 2009

Ma, Z., & Krings, A. W. (2008a). Survival Analysis Approach to Reliability, Survivability and Prognostics and Health Management (PHM), *Aerospace Conference,* pp. 1–20, 2008

Ma, Z., & Krings, A. W. (2008b). Competing Risks Analysis of Reliability, Survivability, and Prognostics and Health Management (PHM), *Aerospace Conference,* pp. 1–21, 2008

Ma, Z. S., & Krings, A. W. (2008c). Dynamic hybrid fault models and the applications to wireless sensor networks (WSNs), *Proceedings of the 11th international symposium on Modeling, analysis and simulation of wireless and mobile systems*, pp. 100–108, 2008

Maglogiannis, I., & Zafiropoulos, E. (2006). Modeling risk in distributed healthcare information systems. *28th Annual International Conference on Engineering in Medicine and Biology Society* (*EMBS'06)* pp. 5447–5450, 2006

Maglogiannis, I., Zafiropoulos, E., Platis, A., & Lambrinoudakis, C. (2006). Risk analysis of a patient monitoring system using Bayesian network modeling. *Journal of Biomedical Informatics*, *39*(6), pp. 637–647

Mikolajczyk, R. (2010). Methods and Concepts of Epidemiology. *Modern Infectious Disease Epidemiology*, pp. 193–208

Norusis, M. J. (2004). *SPSS 13.0: advanced statistical procedures companion*. Prentice-Hall, New Jersey

Rabiah Ahmad (2006). *Cox Proportional Hazard Regression and Genetic Algorithms (CoRGA) for Analysing Risk Factors for All-Cause Mortality in Community-Dwelling Older People*, Ph.D. Thesis, University of Sheffield, United Kingdom.

Ricci, P. F. (2006). *Environmental and health risk assessment and management: principles and practices* (Vol. 9), Kluwer Academic Publication

Rohrig, B., Du Prel, J. B., Wachtlin, D., & Blettner, M. (2009). Types of study in medical research: part 3 of a series on evaluation of scientific publications. *Deutsches Arzteblatt International*, *106*(15), pp. 262-268

Ryan, J. J. C. H., & Ryan, D. J. (2008a). Biological systems and models in information security. *Proceedings of the 12 Colloquium for Information Systems Security Education,* pp. 127-130, 2008

Ryan, J. J. C. H., & Ryan, D. J. (2008b). Performance metrics for information security risk management. *Security & Privacy, IEEE*, *6*(5), pp. 38–44

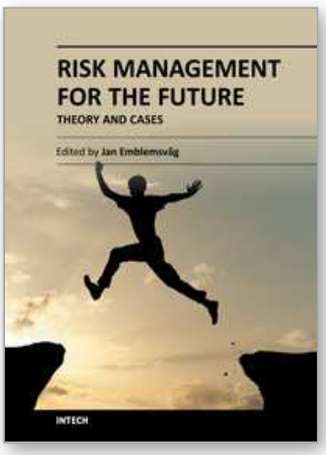
Samrout, M., Chatelet, E., Kouta, R., & Chebbo, N. (2009). Optimization of maintenance policy using the proportional hazard model. *Reliability Engineering & System Safety*, *94*(1), pp. 44–52

Spears, J. (2006). A Holistic Risk Analysis Method for Identifying Information Security Risks. *Security Management, Integrity, and Internal Control in Information Systems*, pp. 185–202

Standards Australia/Standards New Zealand. (2009). *Australian/New Zealand Standard for Risk management – Principles and guidelines (AS/NZS ISO 31000:2009)*, NSW and Wellington

Suh, B., & Han, I. (2003). The IS risk analysis based on a business model. *Information & Management*, *41*(2), pp. 149–158

Yu, C., & Bi, X. (2008). Survival Analysis on Information Technology Adoption of Chinese Enterprises, *4th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM'08),* pp. 1–5, 2008



Risk Management for the Future - Theory and Cases
Edited by Dr Jan Emblemsvåg

ISBN 978-953-51-0571-8
Hard cover, 496 pages
Publisher InTech
Published online 25, April, 2012
Published in print edition April, 2012

A large part of academic literature, business literature as well as practices in real life are resting on the assumption that uncertainty and risk does not exist. We all know that this is not true, yet, a whole variety of methods, tools and practices are not attuned to the fact that the future is uncertain and that risks are all around us. However, despite risk management entering the agenda some decades ago, it has introduced risks on its own as illustrated by the financial crisis. Here is a book that goes beyond risk management as it is today and tries to discuss what needs to be improved further. The book also offers some cases.

How to reference
In order to correctly reference this scholarly work, feel free to copy and paste the following:

Ganthan Narayana Samy, Rabiah Ahmad and Zuraini Ismail (2012). Adopting and Adapting Medical Approach in Risk Management Process for Analysing Information Security Risk, Risk Management for the Future - Theory and Cases, Dr Jan Emblemsvåg (Ed.), ISBN: 978-953-51-0571-8, InTech, Available from: http://www.intechopen.com/books/risk-management-for-the-future-theory-and-cases/adopting-and-adapting-medical-approach-in-risk-management-process-for-analysing-information-security

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821

IntechOpen