Emerald Information Management and Computer Security

An Information Security Risk-driven Investment Model for Analysing Human Factors

Journal:	*Information and Computer Security*
Manuscript ID	Draft
Manuscript Type:	Original Article
Keywords:	Information Security (IS), Information Security Risk-Driven Investment Model (RIDIM), Risk, Social Engineering Attacks (SEAs), S, Security Investment (SI), Return On Investment in Information Security (ROISI).

Abstract

Modern organisational structure and risk management model are characterised by a wide range of forces including the role of human factors which combine to create an unprecedented level of uncertainty and exposure to information security risk, investment and decision making process. Developing a risk-driven investment model for information security systems with consideration of subjective nature of critical human factors, is a challenging task. The overall success of an information security system depends on analysis of the risks and threats so that appropriate protection mechanism can be in place to protect them. However, lack of appropriate analysis of such dependencies and understanding potentially results in information security systems to fail or to fully achieve their that depend on them. Existing literature does not provide adequate guidelines for a systematic process or an appropriate modelling language to support such analysis. This paper fills this gap by introducing a process that allows information security managers to capture possible risk-investment relationships and to reason about them. The process is supported by a modelling language based on a set of concepts relating to trust and control and secure tropos and requirements engineering. In order to demonstrate the applicability and usefulness of the approach a descriptive example from an UK organisation is used.

Keywords: Information Security (IS), Information Security Risk-Driven Investment Model (RIDIM), Risk, Social Engineering Attacks (SEAs), Security Investment (SI), Return On Investment in Information Security (ROISI).

1. Introduction

It is hard to accept that nowadays, organisations get along without having an astute information system. Information systems support organisations to achieve strategic competitive advantage. This is beside cost savings and decision making advantages by assisting for a timely implementation of projects and effective risk management with a great consideration of human factors. Subjective nature of human factors creates risks for achieving information security goals and subsequently organisational objectives. Therefore, human factors perform an important role in IS. The role of people has not only flagged by numerous academic studies but also by IS professionals and various IS regulations and standards. Providing a reliable and coherence information system requires a solid security framework. It ensures confidentiality, integrity, availability, authenticity, and auditability of the critical information assets. Also, it assists to achieve organisational goals and to ensure the continuity of business. Inadequate implementation of security causes serious impacts on organisations' productivity and reputation [1] [2]. According to the "Information Security Breaches: Technical Report" by the UK Department for Business, Information & Skills in 2012, large organisations faced with 93% increase in cyber-threats [3]. Even using the latest security techniques and protocols, most systems still face a lot of security breaches. Technological solutions to deal with issues arise from information security are very similar globally, such as anti-virus, and intrusion detection systems [4]. Numerous technical advancements do not always produce a more secure environment [5].

This paper presents a risk-driven investment model that analyses the human factors which pose potential risks within the organisational context. The novel contribution of this work is to analyse specific critical human factors which have subjective natures in an objective and dynamic domain of risk, security and investment. The study developed a risk-driven security model for understanding of the role of human factors in security incidents, concerning risk, security and return of an investment on security. Social Engineering Attacks (SEA) use as security incidents example because SEAs are greatly influenced by human factors [17]. The proposed model assists the mitigation process from an organisational perspective. It draws on current SEAs curves. The study proposes and validate a holistic model of investment and risk-driven model which supports understanding through identifying key elements and components of Return On Investment in Information Security (ROISI). In addition, provides an understanding of associated risks under the proposed Information Security Risk-Driven Investment Model (RIDIM). These objectives were achieved through the collection of quantitative and qualitative data utilising Requirements Engineering (RE) and secure tropos methods.

The paper is structured in four main section. Following the introduction, section 2 presents business objectives and security relationship, defining risk, ROISI and SEAs concepts. It also reviews the critical human factors. Section 3 presents the risk-driven investment model along with the activities that support the process. Section 4 discusses the applicability of the proposed RIDIM model with a case study. Finally, we will look at the study limitation concluded issues and future work.

2. Business objectives and Security Relationship

2.1 Business Objectives

Effective ISMS depends greatly on knowledge of business as much as security architecture is required to understand business problem. Security professionals required translating business requirements and goals into an ISMS solution capable of meetings those goals and requirements. Business domains and process are varied even in a same industry sector with same nature of business. For example, retail banking, investment banking and insurance in finance industry. Despite being in a same industry, the business concepts are divergent. Without understanding business requirements and objectives as well as specific industry trend, it is difficult to design and architecture any security systems. This leads to lack of insight into risks and investment related concepts and ultimately insufficient and inaccurate understanding and estimation of ROISI. Business domain and the IT strategy in use of resources, are two factors that most influenced organisations to adopt security countermeasures [6]. Therefore, the impact of security breaches and consequently the cost of breach and countermeasures are varied. Business domain, risks and critical human factors all provide sources for ISMS requirements (Figure 1).

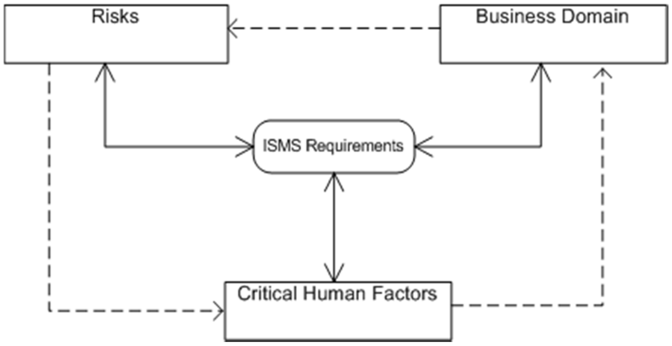

Figure 1. ISMS Requirements Dependency

Organisations are controlled and run by set of policies which shaped by corporate governance.

Information security as part of corporate governance assists organisations to achieve greater productivity with better cost efficiencies, as well as, legal and regulatory compliance. However, information security often seen as a remote activity by many organisations with a technical nature. Therefore, they fail to link business objectives to security goals. Some authors suggested a link between the business domain to the IT domain [7]. The business domain entails, processes, functions, and objects. Therefore, there is a clear link between business domain and information security. In addition, the business domain maps to the ISMS process and is decomposed into procedures, activities and tasks which is historically not be defined with business process [8]. In addition, risks and human factors from the business domain are mapped to the functions and objects of ISMS. The business processes and functions are understood through IT, which aggregates one or more functions from the ISMS. However, IT and consequently security have been seen as an agile project, therefore, they have not been grown into business domain. Based on ISMS requirements and the relation with business domain and risks, the identification of business domain and its concepts are:

- Defining of business processes and their actors
- Categorisation and valuation of assets
- Determining security requirements: vulnerabilities and threats
- Assessing risks
- Identification of countermeasures and control mechanism

Considering this introduction to business objectives and security relationships, we will define the concepts of risk, ROISI and SEA (security incidents). However, before that discussion, we present a review of critical human factors which we identified in our previous studies [9] [10].

2.2 Critical Human Factors

It has been reported that human errors and other factors related to people and system problems caused two-thirds of data breaches and security incidents in 2012 [11]. According to this report, this was included lack of system controls as well as human mishandling of confidential data. The incidents cost financial and healthcare organisations, which are excessively, regulated 70 percent more than other sectors. Same report also estimated that 64 percent of security incidents have directly related to human errors. Despite widely accepted human factors impacts on the security incidents, the average cost of each incident is varied globally. In our previous studies we have identified a number of human factors, including direct and indirect factors that are: Errors, Awareness, Skills, Experience, Apathy, Ignorance and Negligence, Stress, Budget, Culture, Communication, Security Policy Enforcement, Incentive and Disincentive Policy and Management Support. We then prioritised critical human factors, Security Awareness, Communication and Support of Management. These factors considered for developing RIDIM model.

2.3 Risk concepts

Risk management principally emphasis on completing projects successfully through the management and control of known risks. The information security risk management as part of enterprise risk management initiatives focuses on achieving security of assets and information systems by managing and controlling security risks. Speedy evolvement of risks in information security is overtaking this approach. Information security resilience requires acknowledgment that organisations must prepare now to deal with severe impacts from security incidents that are impossible to predict, detect and prevent. Organisations must extend risk management to include risk resilience, in order to manage, respond and mitigate any adverse impacts of information security incidents.

Security resilience also requires that organisations have the agility to predict, detect and prevent security incidents by responding rapidly, efficiently and effectively to security incidents, as well as, the consequences of the incidents. This means understanding multidisciplinary units such as risks, investment and business domain, and their functions in organisations, for developing and evaluating control plans and settings for when security incidents occur. This understanding should be able to follow with effective communication channels with all parts of the organisation, employees, contractors who might have been compromised, in addition to, shareholders, regulators and any other stakeholders who might be penetrated. Figure 2 depicts information security risk interdependency concepts in which the following core risk objectives can be defined:

- Identification of critical organisational systems and assets
- Assess and assign value and importance to the identified systems and assets
- Identification of the threats and vulnerabilities to the systems and assets
- Determine the known risks pattern
- Determine the existing control measures or other risk mitigating features
- Identification of the residual risks
- Developing risk profile and aligning it with investment in information security
- Risk mitigation strategy
- Determining inherent risks: value of the unmitigated risk exposure
- Requiring regular reports of evaluation and update of risk profile
- Documentation of risk assessment process, including the risk acceptance criteria and criteria for risk assessment

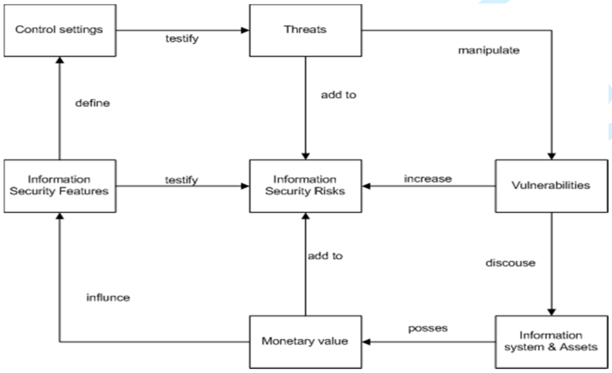

Figure 2: Information Security Risk Concepts

2.4 Return On Information Security Investment (ROISI) Concepts

Tools and strategies are essential to organisations to be cost effective whilst information security professionals endeavour how to demonstrate the value and ROISI. Available tools and methods allow organisations to calculate and analyse the financial impact of a specific security control, which cannot be used to analyse the cost-benefits of other factors, such as critical human factors. Information security management system is now increasingly based on economic principles such as cost-benefit analysis [12]. There are important variables in this measurement that are required to be as precise as possible. Accurate information of likelihood of security incidents and their impacts must be acquired in order to assist the quantification of ROISI. The traditional approach to the return of the investment is used in enterprises as a performance measure to assess the effectiveness of an investment and can be used in ROISI. The two important concepts used in ROISI are: Return On Investment (ROI) and Net Present Value (NPV). The general cost-analysis in organisations draws a picture and understanding of business and technical requirements of return on investment. The classical and general ROI calculation looks like this [12]:

$$ROI = \frac{Gain\ From\ Investment - Cost\ of\ Investment}{Cost\ of\ Investment}$$

The traditional calculation it is quite straightforward when organisations deal with clear amount of tangible investment, where profit is evident and apparent and revenue is acquired that is greater than investment. However, in information security whilst we can calculate the total cost, there is no revenue to be made. Information security typically averts loss rather than generating profit from its investment. Traditional ROI can be extended in ROISI in the following formula:

$$ROISI = \frac{(Risk\ Exposure \times \%Risk\ Mitigate) - Mitigation\ Cost}{Mitigation\ Cost}$$

This calculation based on known risks and their relevant mitigation mechanism. Net Present Value (NPV) would be the method shown below where Io is Initial Investment for security measure; $\Delta\mathrm{E}\ (\mathrm{L}t)$ is Reduction in Expected Loss in a specific period, $\Delta\mathrm{OCC}t$ is Reduction in Opportunity Costs in a Specific Time, Ct is Costs of security measure in a specific Time and $i\ calc$ is the Discount Rate [13].

$$NPV = \ -Io + \sum_{T=1}^{T} \frac{\Delta\mathrm{E}\ (\mathrm{L}t)\ +\ \Delta\mathrm{OCC}t\ -\ Ct}{(1 + i\ calc)^{t}}$$

Organisations receive recommendations for SI based on the outcome of this model depending on positive or negative value. This model and the most proposals in ROISI consider a single security measures rather than ISMS [12]. Also, it has been noted that NPV presents a time value for investment [14]. Therefore, ROISI performs for the time value of investment which technically speaking would be inflation and cost of capital.

2.4.2 Cost of incident

Organisations perceive investment on services and products whilst they are financially viable and justified. Executive boards of management do not consent to any business case prior to cost-benefit analysis [14. The cost-benefit analysis can be done through conventional process of accounting methods such as Net Present Value (NPV) or Internal Rate of Return (IRR). The following sub-factors are characterised the issue of cost:

- Employee costs for resolving security incidents
- Training/Awareness Programs
- Cost of security controls

- Cost of possible maintenance/developing of new software/hardware
- Legal cost and possible fines
- Cost of possible use of external contractors
- Possible cost of insurance
- Reputational cost, including the loss of customers/orders/services

Organisations tend to minimise risks, which threatening information assets. Therefore, the classical financial approach to ROISI is not specifically relevant to measure information security planning. This becomes hard to determine when it comes to non-technical aspects of information security systems, including critical human factors and their cost implications such as training. Therefore, it is extremely difficult to calculate and quantify all the costs that are related to the potential risks and the damages resulted from security investment. In addition, it is really difficult to estimate the precise likelihood of the occurrences of those incidents due to the volatile, erratic, dynamic nature of the critical human factors and the way they fluctuate and inconsistent behaviour. This even harder because no reliable data available to substantiate such estimations. Information security, cost, return of investment all deal with monetary value whilst human factors are quite difficult to be framed and used with financial metrics. Despite this difficulty and as organisations require an estimation of financial consequences of information security incidents for the purpose of quantification which can be achieved by identifying risk concepts and modelling them by looking at the changes to the control settings based on the variation of risks. Therefore, this enables organisations for cost-benefit analysis by comparison of cost and investment with consideration of variety of risks, more objectively. In later activity the ROISI calculation will be presented. This was a short overview of current ROISI calculation methods in industry with a summary of this study approach to consider all concepts of ROISI.

2.5 Security incident concepts

Security Incidents (SI) are regarded as a sequences of events that undesirably affect the information system and assets of an organisation. Therefore, security incidents often include multiple threat events. Regardless of all the controls and protection mechanism organisations built into their information system and applications, they still experience security incidents. Information security standards such as ISO27001 expect that organisations to be prepared for these incidents [15]. Significant losses can be resulted by various types of damage that inflict from many threats. These threats are originated from the vulnerabilities of information processing systems. The type of breach is also important in studying ROISI because the impact is different. Understanding the dynamics by which threats engage with a company's assets and controls allows security professional to model risks. One of the outputs of that model is the ability to see how the risk varies as the control settings change. If the company can estimate the cost required to turn a control setting up one or two clicks, and the model tells how the risk falls when a control turn up with couple of clicks, then it is straightforward to do a ROISI calculation for each proposed change. The ROIS is the reduction in expected harm for the cost of the change.

Security incidents are greatly dependent on human factors. Although impacts are varied but the quantification of the impacts are not clear [16]. One of the main reasons for this would be the nature of controls as it mentioned earlier. Security incident can be defined in details with the following elements:

- Description of incident

- Description of security controls and countermeasures
- Estimation of Losses

Based on above elements, security incident response entails a number of activities. They can be, detection and analysis of an incident and recovery process from it. Considering the above definition and description, this paper used Social Engineering Attacks (SEA) as an example of security incident. In here we define SEA incidents.

2.6 Social Engineering Attacks (SEA)

Social engineering is the act of manipulating a person to take an action that may or may not be in the target's best interest which include obtaining information, gaining access or getting the target to take a certain action [17]. Organisations may use various tools such as web server security to detect and minimize SEAs but they have difficulty in preventing and responding to human actions and behaviour in socially engineered incidences. SEAs resulted mainly in the exploitation of many related issues of human factors. There are specific factors, which were identified, in the previous study and play important roles in such attacks [10]: Lack of awareness and ample set of skills, inadequate communication skills, Lack of supervision and sufficient involvement of management. Therefore, it can be concluded that human factors and human social interactions can be engineered for exploitation in gaining access to an organisation's assets.

2.6.1 Reasons Behind Social Engineering Attacks

Human factors remain essential to any SEAs because no matter how many training programs or control mechanisms are deployed; people are the weakest link in security [18]. SEAs can cause a great deal of disruption to everyday business activities and create financial, social and technical mayhem in which the impacts may go beyond geographical borders and organizational boundaries. Therefore, dealing with SEAs would be in the best interest of any organisation. According to the (Verizon 2014) report, human factors are the main sources of SEAs [19]. People can be easily socially engineered which leads to compromise of information systems in organisations. Even when attackers use complex and sophisticated technical hacking methods they would consider using people as a main tool in delivering their malicious software. Janczewski and Fu identified five main causes of SEAs, i.e., people, lack of security awareness, psychological weaknesses, technology, and defences and attack methods [17].

2.6.2 Social Engineering Attacks Taxonomy

SEAs undermine organisations' efforts to deal with security in an effective way. There are several malicious practices such as Advanced Persistent Attack that create security breaches in organisations [20]. Janczewski and Fu (2010) defined the SEAs with two distinct methods; the "Human-Based and Technology-Based" attacks [17]. However, the role of people and certain human factors are contributing greatly to SEAs. The attackers crack the security of an information system by exploitation of human weaknesses. It is a challenging task for organisations to deal with SEAs because they are human-oriented activities and human factors are difficult to deal with. Figure 3 depicts the link between human factors, SEAs, their objectives and consequences.

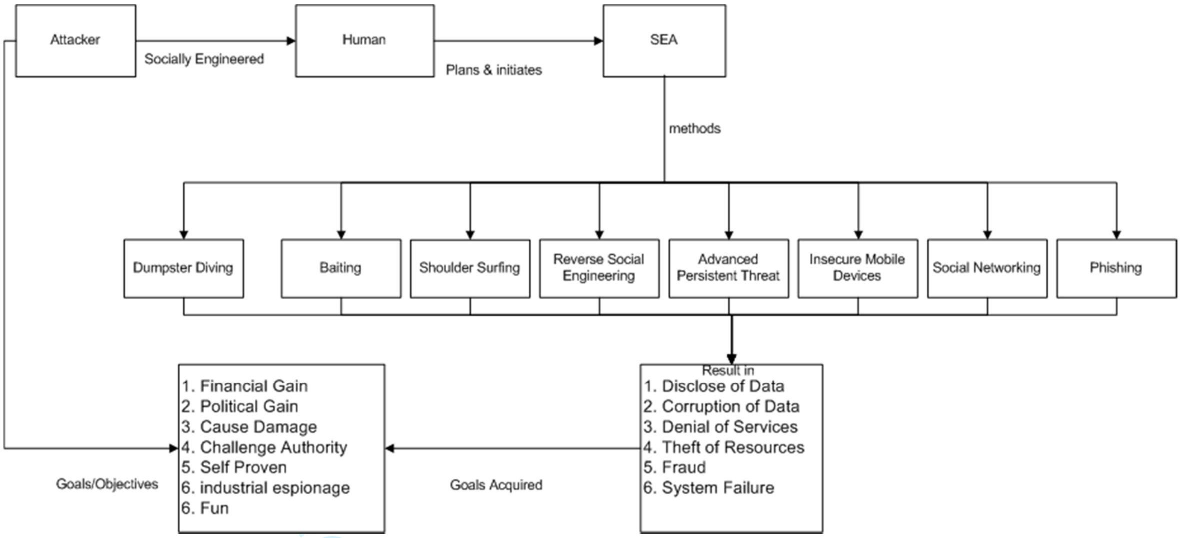

Figure 3: Social Engineering Attack Taxonomy

There have been a number of works that focus on analysing SEA attacks. Janczewski & Fu (2010) provided a conceptual model in order to understand SEAs impacts on individuals and businesses and present a defensive approach to mitigate these risks [17]. The study focused on IT departments and a more abstract view of SEAs without considering SEAs concepts related to critical human factors and their relationships to the concept of SI. Greitzer et al (2014) looked at the insider threat that derives from SEAs [21]. The study considered some related human factors but concentrated mainly on unintentional insider threats whilst observing psychological and social characteristic of people. Karpati et al (2012) used a comparison study between mal-activity diagram and misuse cases and presented two modelling techniques [22]. There are advantages and efficiencies of each approach. Some other studies concentrated on specific attacks such as phishing attacks [23] or advanced persistent attacks [24].

All the above-mentioned works contribute towards investigating SEAs security incidents. However, none of these works explicitly focus on critical human factors, which are one of the main reasons for SEAs. Therefore, it is important, analysing human factors whilst considering SI in so that an organisation can make the right decision relating to information security.

3. Information Security Risks-Driven Investment Model

This section presents the proposed model. The model consists of a systematic process to identify the business risks posed against crucial information assets, providing best way to eliminate and mitigate those risks. For this reason and in order to provide specifications of the process of development of SEAs risk-based artefact, there are certain activities required. The information security standards such as ISO27000 family that includes and embraces ISMS with ISO27001, advise for adopting risk and standards-based approach to implement an ISMS. In this study we use some of the guidelines provided by ISO27000 family of information security standards and introduce the Information Security Risk-Driven Investment Model (RIDIM).

RIDIM activities are performed that we show in Figure 4, include tasks and steps involved within the modelling process. Organisational analysis is the commencing activities of initial Secure Tropos requirements process. This will follow by the analysis of incident whilst the consent of all involved parties are obtained. The final phase consists of the calculation of ROISI. The modelling process will map of all the activities including the recommendations of the mitigation process. It also provides a justification for the control mechanism in this process based on the SI concepts. In order to to map and evaluate the concepts of the proposed RIDIM model the following activities are planned.

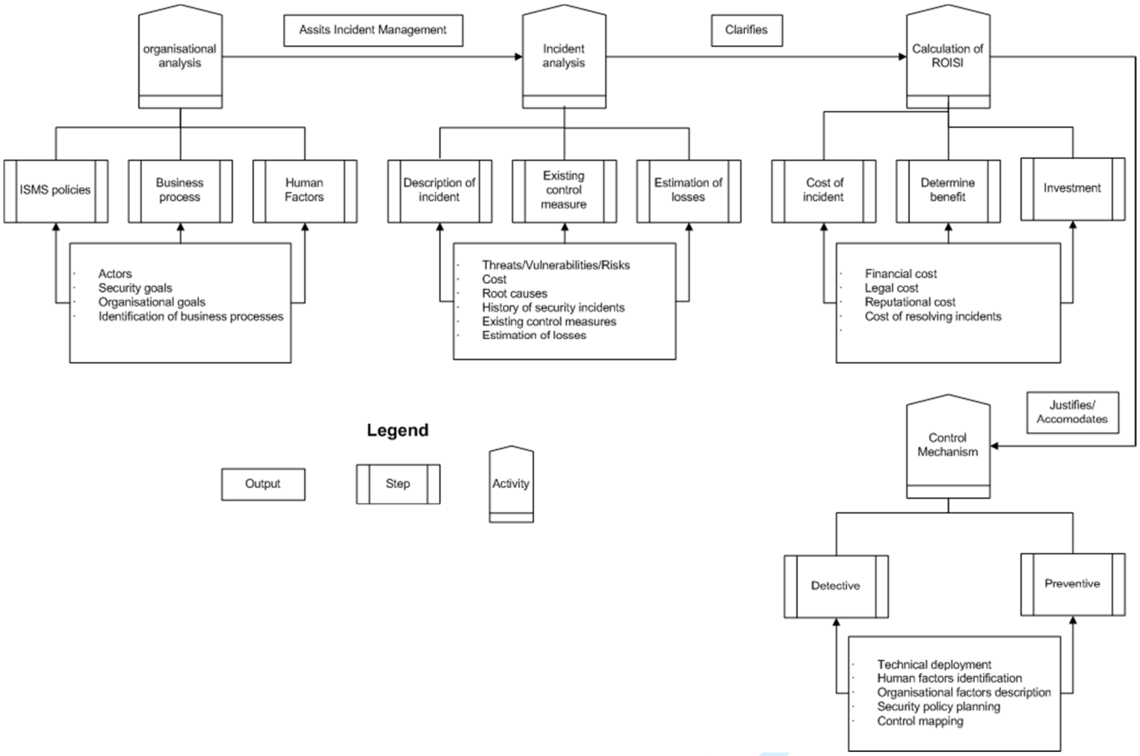

Figure 4: The Activities for Information Security Risk-Driven Investment Model (RIDIM)

Activity 1: Organisational Analysis

This activity consists of the following steps that cover the ISMS policies, business process and human factors:

- **Defining Critical Human Factors**

In order to define critical human factors, we used Delphi Expert Panel Technique. The Delphi method is seen as a popular an established tool in the field of information security [27] [28] [29]. Its purpose was to develop a stable and consistent method that could be used to achieve consensus of a group of experts [27]. Delphi technique was incorporated in three stages:

1. Brainstorming sessions to identify human factors
2. Narrowing down main human factors
3. Prioritising and ranking human factors

Figure 5 shows an overview of tasks, identifying and rankings of human factors.

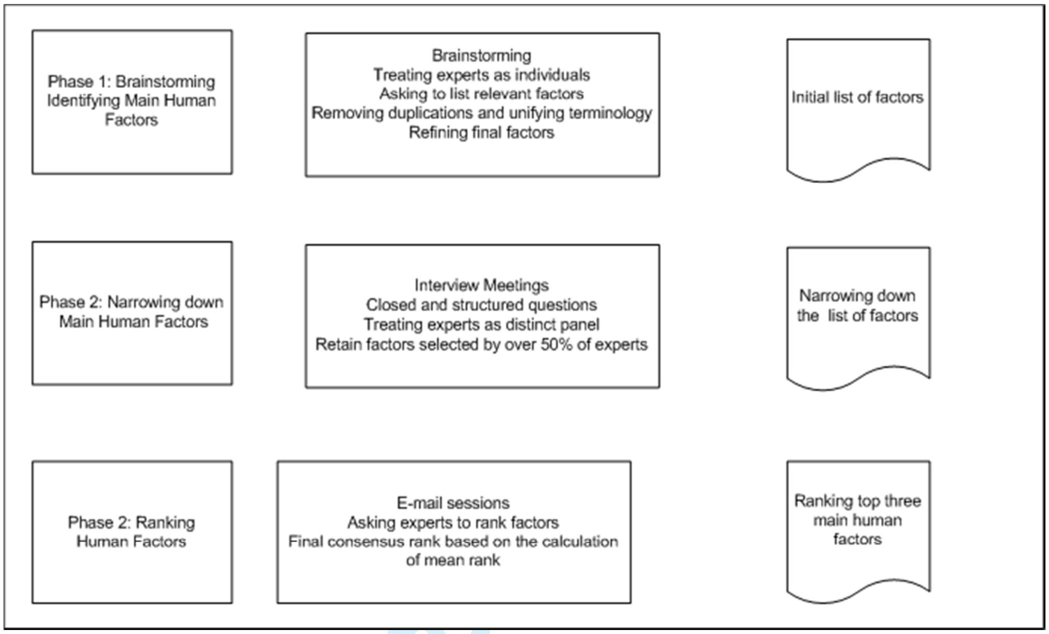
Phase 1: Brainstorming Identifying Main Human Factors
Brainstorming
Treating experts as individuals
Asking to list relevant factors
Removing duplications and unifying terminology
Refining final factors
Initial list of factors
Phase 2: Narrowing down Main Human Factors
Interview Meetings
Closed and structured questions
Treating experts as distinct panel
Retain factors selected by over 50% of experts
Narrowing down the list of factors
Phase 2: Ranking Human Factors
E-mail sessions
Asking experts to rank factors
Final consensus rank based on the calculation of mean rank
Ranking top three main human factors

Figure 5: An overview of the phases of Delphi expert panel

Phase 1: Brainstorming

In this phase, a group-brainstorming session with structured questions was conducted to stimulate main human factors as subjective data. A survey of 62 respondents belonging to 7 organisations were performed. The brainstorming sessions were run in all seven organisations separately in which all participants agreed to set of factors in their ISMS projects experiences. Table 1 provides an overview details of organisations, ISMS projects and the survey participants.

Delphi Survey Organisations Info	
Organisations Outline	Respondents were experts belonged to industry and academia
ISMS Projects	Main human and people issues related to security projects
Detail on Participants	The total of the participants was 62. They were from different layer of the organisations, including Chief Information Security officers (CISO), Chief Information Officers (CIO), IT managers, and participants from academia.

Table 1: Overview of Participants Organisations

The participants were also asked to justify the reasoning for their selection and ranking of the factors. They were given two weeks for their responses. In the first phase, 34 of 62 experts (52%) offered their assistance, generating a list of 13 human factors for ISMS that was similar to the factors in this list were established in this research through multiple methods.

The outcome of this process was the identification of 13 human factors listed in Table 2 with ranking where 1-5 are very significant whilst 5-13 having various value of significance.

Factors Ranking	Human Factor	Description
1	Communication (F1)	concerning exchange of messages and ideas between people inside and outside
2	Awareness (F2)	ensure that people understand their responsibilities
3	Management support (F3)	management to advocate and deliver a clear message of ISMS policy to the rest of the organisation
4	Budget (F4)	It concerns with adequate budget planning
5	Errors (F5)	Can be described as a divergence in a system that works accurately
6	Skills (F6)	Skills facilitate the function of a role
7	Experience (F7)	Concerns people background
8	Incentives/Disincentive (F8)	Reward good behaviour and punish bad attitude
9	Security Policy Enforcement (F9)	A document in which the information security procedures and rules are outlined
10	Culture (F10)	consists of values, beliefs, practices, attitudes, behaviour, reputation, and ethics
11	Stress (F11)	Individuals' stress in corporations can be caused by heavy workloads and tight project deadlines.
12	Apathy (F12)	unwillingness of employees and in their attitude toward the goals and objectives
13	Ignorance and Negligence (F13)	not pay enough attention to security policy

Table 2: Ranking of Human Factors by Importance

Phase 2: Narrowing down main human factors

Phase two of the survey study concluded of 18 open questions and 24 closed questions in the mode of questionnaire were presented to the participants. The feedback received from the brainstorming sessions were formed the questions and questionnaire to ensure the refinement of the human factors. In order to reduce any possible bias by missing factors, the participants were given an opportunity to offer feedback on the factor they wished to share.

Phase 3: Ranking main human factors

The third phase of the process consists of sending questionnaires to the entire group that included 13 main human factors identified in the previous two phases and the average importance and rating from the phase 2. This was included a reasoning of the selections. Figure 7 depicts the number of respondents at this stage and based on the percentage. Figure 6 shows the three main factors with their sub-factors.

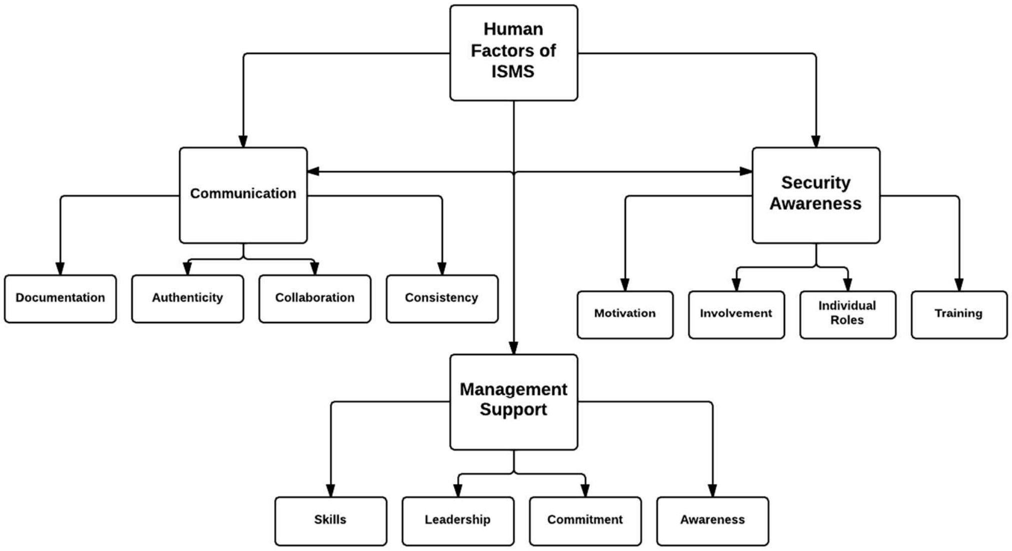

Figure 6: Three top Ranking of Human Factors with Sub-factors

- **Identification and classification of critical organisational systems and assets**

Each asset needs to be identified such as servers, applications and databases. This reference provides the foundation for managing and measuring vulnerabilities. This is important for updating the status of assets and system as often as required. In addition, assets and various systems to be grouped and classified from low, medium priority to the most critical assets that are vital to the organisation operations. The classification depends on the nature of business domain. For example, while web servers that support order process, could be the most critical devices for an Internet merchant, whilst for a manufacturer the systems that support the supply chain, could be a vital asset. The objective is to classify those assets and systems that are essential to organisational operations and success and clarifying business process.

- **Identification of the threats and vulnerabilities to the systems and assets**

A highly accurate, comprehensive, and up-to-date approach is required to identify the latest vulnerabilities and misconfigurations based on timely information on the basis of security policies. A suitable defence mechanism requires for the detection of vulnerabilities. This ensures that the vulnerabilities which pose high risks are dealt with. It is essential to correlate vulnerability criticality with the business value of vulnerability systems and assets. So, vulnerability assessments should examine infrastructure against the most accurate, up-to-date threats. The classification and categorisation of vulnerabilities enable the formation of detailed metrics for different types of vulnerabilities that are relevant for measuring security awareness, program effectiveness and adherence to security policies.

- **Identifying risk mitigation strategy, risk profile, inherent and unmitigated risks**

Organisations goals and objectives are vital to consider when adapting a risk mitigation strategy, otherwise the framework may not receive investment it requires. In addition, priority should be assumed to the threats and vulnerabilities that have the potential to cause significant harm then it may not be practical to deal with all identified and inherent risks. Risk mitigation strategy must be aligning with the financial objective of an organisation therefore, it is important to consider the cost of implementing controls and also the potential costs of not doing so. The risk exposure ratings can be used to establish recommended protection controls which finally direct to formation of the risk mitigation strategy. Risk management strategies also define security incident response when a security incident such as a data breach occurs.

Activity 2: Incident Analysis

This activity consists of the description of incidents, existing control measure and estimation of losses:

- **Description of incidents**

Once the organisational entities are identified and analysed by the previous activity, this activity deals and analyses the incident that instigated by the critical human factors. When an incident happens, it is central to know what to do, how to gather proof that meets legal criterions, and how to deal with the consequent regulatory, financially and reputation issues. However, it is imperative that incidents to be reported promptly to allow the issue to be analysed and addressed in order to reduce the occurring risks. The main goal of the incident analysis process is assisting to remediate any loss that may have occurred to organisations and minimise the damage sustained by similar incidents in the future.

- **Determine the existing control measures and residual risks**

Identifying and determining current control measures for each of the identified risks helps to identify the missing controls. They require a clear documentation in which the validation of their effectiveness and performance are confirmed. The effectiveness of controls can be used to re-assess and prioritise the risks in terms of their likely impact on the capacity of the system. High priority risks may require control mechanism's alteration or upgrade to achieve security goals. This applies to the residual risks too. Residual risks are the remaining risks to the organisations' assets after control measures are applied. However, organisations should consider a mitigation process for them.

- **Estimation of losses**

The loss is associated with incidents' transactions such as assets used in business or lawsuit settlements but cost affiliates with the expenses to provide security control measures. The information assets' cost comprises tangible and intangible assets [25]. Part of the quantification of the ROISI relies on the estimation of the losses incurred in the case of SEAs when a system is exploited. Considering the severity and the possible of losses the main costs of an incident can be defined as:

- Increased insurance premium
- Administrative expenses (Extra Training, Internal cost-auditing)
- Time (availability of data and system)
- Hardware and Software cost (External cost)
- Implementation cost (customisation, consultation, training, testing and communication)

The incident profile will be completed when the control mechanisms are identified and and to be categorised against the valuation criteria and be mapped to the losses and costs. The existing control measures.

The above mechanisms can be given valuation as Effective, Ineffective, Adequate or Inadequate. The introduction of new control mechanism can be matched by above ranking.

Activity 3: Return on Information Security Investment (ROISI)

The final activity calculates the return of any SI and contributes for the enhancement of the existing ISMS practice. Therefore, we need to justify whether there is a necessity of more SI considering the occurred incident/s. The justification for new investment will follow after the calculation of the return on investment.

- **Calculation of ROISI**

The final activity calculates the return of any security investment and contributes for the enhancement of the existing ISMS practice. Therefore, we need to justify whether there is a necessity of more SI, considering the occurred incident/s. In order to quantify the cost and benefit of security measures. The expenditure which play important role in the concept of ROISI. In risk management field this is called Single Loss Expectancy (SLE) that is the cost of the single loss. In which risk exposure can be calculated:
Risk Exposure = ALE = SLE * ARO
where ALE is Annual Loss Expectancy and ARO is, Annual Rate of Occurrence.

The SLE provides a quantitative evaluation, using the estimation of likelihood that can be used for the calculation of Annualised Lost Expectancy (ALE). Vulnerabilities would be flaws in information process that expose a system to compromise and threats are the circumstance in which an actor adversely impact information assets through unauthorised access, destruction, disclosure, modification of data, and/or denial of service [26]. ALE, which also can be considered as the annual cost of risk, is the multiplication of SLE and likelihood of threats. After implementation of any security measure, an assessment should run to evaluate the frequency of any potential incident because likelihood of threat will increase or decrease depending on the nature of threat and its security measure. For example, the frequency of natural disaster stays same but if organisations deploy new and more effective anti-virus software the likelihood of a successful malicious code attack will decrease. Lastly, the estimation of cost of security measures should be considered as accurately as possible, considering following factors:

1. The cost of acquiring of security measure
2. The cost of maintenance
3. The cost of people (fulfilling critical human factors)
4. The cost of value after commissioning the measurement

Considering all factors and inputs ROISI can be positive or negative. In order the ROISI be positive is that the reduction of risk must be much greater than total investment and cost of security measures. This also can be seen in ALE where the annual cost of security measures is less than ALE. Previous studies have developed different methods using various concepts which it was explained earlier.

Study aims to solve the described trade-off between the expected attacks losses $EA_{(L)}$, and the costs of the economical capital $CE_{(C)}$, on the one hand and the investments in information security controls $IS_{(C)}$ and the investment in insurance $I_{(I)}$ on the other hand. Thereby, the capital to be invested in information security control mechanisms will be optimised. Based on this, the total negative liquidity can be shown as:

$$NL_{(T)} = EA_{(L)} + CE_{(C)} + IS_{(C)} + I_{(I)}$$

The above concepts should be expanded to assume more details of the involved costs and losses in order ROISI to be accurate. Therefore, in order to calculate the return of the investment on information security the followings must be considered in three different stages; stage one would be the calculation of the cost of single expected attack in an incident and the stage two would be to calculate the risk exposure factor and risk reduction after security control measures and insurance are considered with the assumption that security controls and investment in insurance policy reduce the loss. The third stage would be calculation of ROISI in absolute quantity where the ROISI calculated based on annual cost of protection, insurance and other costs.

we also need to consider the preliminary expected cost from the following parameters:

- External Services Cost $ES_{(C)}$
- Purchasing Cost $P_{(C)}$
- Employee Cost $E_{(C)}$
- Administrative Cost $A_{(C)}$
- Legal Costs $L_{(C)}$
- Other Costs $O_{(C)}$

Therefore, the total expected cost of an attack $TEC_{(T)}$ would be:

$$TEC_{(T)} = ES_{(C)} + P_{(C)} + E_{(C)} + A_{(C)} + L_{(C)} + O_{(C)}$$

It is also the loss of the revenue from both existing (L_1) and potential customers (L_2) in which the Total Revenue Loss $RL_{(T)}$ can be calculated as follow:

$$RL_{(T)} = L_1 + L_2$$

Now we can look at the following parameters we mentioned earlier:

- Single Expected Attack Loss $SEA_{(L)}$
- Total Expected Cost of an Attack $TEC_{(T)}$
- Insurance Claim $IC_{(I)}$
- Revenue Loss from existing/potential clients $RL_{(T)}$
- Average Margin $AM_{(A)}$

$$SEA_{(L)}= TEC_{(T)} – IC_{(I)} + (RL_{(T)}) * AM_{(A)}$$

Whilst the single expected attack loss has been calculated then we would be able to calculate the annual expected attack loss based on the likelihood (L) of the SEA occurs. This can be done by the following formula:

$$AEA_{(L)} = SEA_{(L)} * L$$

Now we have defined the process of the calculation of ROISI, we can see how this can be applied to the case study.

- **Justification of the Investment**

Quantifying costs and benefits associated with information security in organisations very often have difficulty to be addressed in budget proposals. Senior management generally perceive information security as measures of disaster recovery rather than as a mechanism for lowering risk and for this reason, justification of the investment in information security is a problematic issue [30]. Therefore, justification seems not only necessary but quite hard to achieve and it relies heavily on the figures.

Case Study

To demonstrate the applicability of the proposed approach, the paper used a scenario. The following description is a real and successful SEA incident that happened in a financial institution within the UK and it was a very well targeted phishing attack.

Scenario

An employee received an email from one of the managers' referencing an invoice hosted on a cloud file sharing service. A few minutes later, the same employee received a phone call from another manager within the organization, instructing her to examine and process the invoice. However, the invoice was a fake and the manager who called the employee was an attacker. The apparent invoice was in fact a Remote Access Trojan (RAT) that was designed to contact and command-and-control (C&C) the server. By using the RAT, the attacker took control of the employee's computer instantly. The attacker managed to breach a part of the server as the multi-layered encrypted server prevented him from getting access to all the servers. This attacker used a socially engineered attack for financial gain. Before the attack was stopped they succeeded in getting a financial incentive in the region of £50,000.00.

Activity 1: Organisational Analysis

- **Defining Critical Human Factors**

Considering three identified critical human factors, the case study demonstrates the applicability of them. It is clear that lack of security awareness contributed to a successful planned SEA. The absent of adequate authentication process in regards to communication has also assisted the attacker to establish a false communication channel. Finally, if senior management had adequate skills and awareness then it was able to support the adequate and appropriate control measures in place.

- **Identification and classification of critical organisational systems and assets**

The first and most critical asset which compromised was part of the server of this company. Financial information were the other important assets which compromised. Both compromised assets can be categorised as high value asset.

- **Identification of the threats and vulnerabilities to the systems and assets**

The main threat to in this case study was the installation of a Malware which assists the attacker to get access to the server. The user's carelessness due to lack of adequate training was a vulnerability to the server which exploited. This created a potential risk of loss as the result of the threat exploiting the vulnerability. This clearly shows the lack of proper firewall and software security protection.

- **Identifying risk mitigation strategy, risk profile, inherent and unmitigated risks**

Studying the nature of the incident this company should define an adequate risk mitigation strategy whilst considering the cost of implementing controls and also the potential costs of not doing so. In addition, the company requires to prioritise, evaluate, and implement appropriate risk-reducing activities to address the specific risk it faces with the degree exposure of this incident.

Activity 2: Incident analysis

- **Description of incidents**

The incident rooted mainly on the exploitation of vulnerabilities in the server but factors as we described in the Activity 1 originated from critical human factors. The risks concerning to be exposed have directly impacted the company. The nature of the incident was a SEA in which a malware called (RAT) that was designed to contact and command-and-control (C&C) the server. In short, human factors and inadequately of security detection and prevention system contributed to the incident.

- **Determine the existing control measures and residual risks**

Existing control measures covers security awareness training, authentication, firewall and encryption. However, the training manuals require an update, encryption mechanism must be reviewed, authentication process should be established in all sort of communication and firewall to be updated. All of these can address the vulnerabilities and residual risks.

- **Estimation of losses**

The estimation of the losses in regards to all variables are required, otherwise the calculation of the return on investment can not be justified. The company estimated all related cost of the incident and provided them which we will be using them in the next activity for the calculation of ROISI. Comparing the estimation losses and the existing control measures shows the inadequately and ineffectively of current controls as the incident generated losses and consequently some additional costs. Given the figures for losses are provided in the next activity.

Activity 3: Calculation of ROISI

- **Return on Information Security Investment (ROISI)**

For the purpose of this study, the paper introduced the preliminary expected cost to cover the loss arising from incidents from the following parameters: External Services Cost $ES_{(C)}$, Purchasing Cost-$P_{(C)}$, Employee Cost-$E_{(C)}$, Administrative Cost-$A_{(C)}$, Legal Costs-$L_{(C)}$ and Other Cost-$O_{(C)}$. Therefore, the total expected cost of new and updating control mechanism would be:

$TEC_{(T)} = ES_{(C)} + P_{(C)} + E_{(C)} + A_{(C)} + L_{(C)} + O_{(C)}$
$TEC_{(T)}$ = 10K+5K+2K+0+1K= £18,000.00

The next step is to calculate the Total Revenue Loss $RL_{(T)}$ that would be from both existing (L_1) and potential customers (L_2). The estimation for this company based on the its business and revenue are given as:

$RL_{(T)} = L_1 + L_2$
$RL_{(T)}$ = 50k + 0 = 50K

Now we can look at the following parameters we mentioned earlier:

- Single Expected Attack Loss $SEA_{(L)}$
- Total Expected Cost of an Attack $TEC_{(T)}$
- Insurance Claim $IC_{(I)}$
- Revenue Loss from existing/potential clients $RL_{(T)}$
- Average Margin $AM_{(A)}$

$SEA_{(L)}= ((TEC_{(T)} – IC_{(I)}) + (RL_{(T)})) * AM_{(A)}$
$SEA_{(L)}$ = ((23K – 5K) + (50K) * 15%
$SEA_{(L)}$ = £30500.00

This would be total Single Expected Attack Loss $SEA_{(L)}$ considering the risk exposure just indicated at probability of the incident happens only "once a year" and by taking into consideration of the threats, vulnerabilities and existing control mechanism. Now if we apply a training program every three months which will cost £2k internally and £2k externally, and we consider an 80% reduction in the security incidents in this company with 15 employees and average cost of £22k for each employee, then the annual cost of new control protection will be £5320.00.

The total New Single Expected Attack Loss $NSEA_{(L1)}$ after new control mechanism taking into consideration by:

$NSEA_{(L1)} = SEA_{(L)}$ * (100- % reduction of $SEA_{(L)}$) = £6100.00

Then the Annual Lost Expectancy based on one-year risk exposure would be:

ALE = $NSEA_{(L1)}$ * Frequency (annually) = £24,400.00

Therefore, the Risk Reduction, $R_{(r)}$ can be calculated with:

ALE = $SEA_{(L)}$ – $NSEA_{(L1)}$ = 6100.00

Eventually, if the ROISI is positive this means the investment has been returned with justification and if it is negative then investment can not be justified.

ROISI = $R_{(r)}$ – Annual cost of protection (£5320.00) = £780.00
ROISI = $R_{(r)}$ / (£5320.00) * 100% = 14.66%

- **Justification of the Investment**

The new investment is justified and it can be presented to the executive board for action.

Discussion

Applying the RIDIM model in a real case study shows the model can be applied and used in other incidents and more importantly to the incidents which critical human factors are a grave concern of organisations. The importance of providing a financial justification is clearly highlighted and provided for seeking investment in information security.

4. Study Limitation

The model presented by us in this paper, overcomes some of the limitations in respect to reasoning critical human factors for the economy of the scale. However, this study also has its own limitations. One of the major limitations of this model is that it supports incident based investment, only. This creates some sort of difficulties to presented to the executive board. Secondly, due to the nature of human factors, quantification does not exactly reflect the monetary value of the factors.

5. Conclusion

This paper introduces a risk-driven investment model in information security that enables organisations to analyse the risks and return of the investment in security controls to deal with security incidents. The process makes use of secure tropos, requirements engineering and risk management concepts. Using security, risk, business and SEA concepts allows us to model and reason the role of critical human factors in quantification method in regards to risk and investment. Therefore, risks, business domain, security incidents and investment concepts in an organisational perspective are not left unexamined by using our model. The proposed process leads to define a clear relationship between risks, incidents and investment and allows organisations to calculate them based on their own figures. Nevertheless, this model does not guarantee that organisations will fully able to calculate the return of their investment in the security controls. This is because most of incidents are related to critical human factors which makes it hard for organisations to put a figure against them. However, RIDIM supports the organisations in achieving a numerical quantity of all relevant costs to the incidents. In addition, as future work, we intend to propose methods that will further support organisations for validating the control mechanism even more accurately. In addition, to expand our understanding of critical human factors.

References

[1] Reddick, C. G. 2009. Management support and information security: an empirical study of Texas state agencies in the USA. Electronic Government, an International Journal, 6, 361-377.

[2] Kraemer, S. & Carayon, P. 2006. An Adversarial Viewpoint of Human and Organisational Factors in Computer and Information Security: Final Report. Wisconsin-Madison, University of Wisconsin-Madison & Information Design Assurance Red Team (IDART), Sandia National Laboratories.

[3] Cyberthreat, 2006. http://www.pwc.co.uk/en_UK/uk/assets/pdf/olpapp/uk-information-security-breaches-survey-technical-report.pdf. (Accessed 10 May 2012)

[4] Zhang, Y., Vaishnavi, V.K., Vandenberg, A., and Duraisamy, S. 2009. Towards design principles for effective context- and perspective-based web mining. DESRIST '09: Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology. ACM, New York.

[5] Stamp, M. 2011. Information Security: Principles and Practice, John Wiley & Sons.

[6] Yeh, Q.-J. and Chang, A. J.-T. 2007. Threats and countermeasures for information system security: A cross-industry study. Information & Management, 44, 480-491.

[7] Versteeg, G. and Bouwman, H. 2006. Business architecture: A new paradigm to relate business strategy to ICT. Information Systems Frontiers, 8, 91-102, 1387-3326.

[8] Guo, J., Hu, Z., Chan, C.K., Luo, Y. & Chan, C. Document-oriented heterogeneous business process integration through collaborative e-marketplace. 2008. ACM, 39, 1605580759.

[9] Alavi, R., Islam, S., Jahankhani, H. and Al-Nemrat, A. 2013. Analyzing Human Factors for an Effective Information Security Management System. International Journal Of Secure Software Engineering (IJSSE) 4, 50-75.

[10] Alavi, R., Islam, S., Mouratidis, H. 2014. A conceptual framework to analyze human factors of information security management system (ISMS) in organizations. In: Tryfonas, T., Askoxylakis, I. (eds.) HAS 2014. LNCS, vol. 8533, pp. 297–305. Springer, Heidelberg.

[11] Corporation, S. 2013. Ponemon and Symantec Find Most Data Breaches Caused by Human and System Errors [Online]. Symantec Corporation. Available: http://www.symantec.com/about/news/release/article.jsp?prid=20130605_01 [Accessed 20/07/2013 2013].

[12] Brecht, M. and Nowey, T. 2013. A Closer Look at Information Security Costs. In: Bohme, R. (ed.) The Economics of Information Security and Privacy. Springer Berlin Heidelberg.

[13] Faisst, U., Prokein, O. and Wegmann, N. 2007. Ein Modell zur dynamischen Investitionsrechnung von IT-Sicherheitsmaßnahmen. Zeitschrift für Betriebswirtschaft, 77, 511-538.

[14] Brotby, W. K. 2009. Information Security Management Metrics, NW, Auerbach Publications.

[15] (ISO), I. O. F. S. 2013. ISO/IEC 27001 - Information security management. Online International Organization for Standardization (ISO).

[16] Hovav, A. and D'arcy, J. 2005. Capital market reaction to defective IT products: The case of computer viruses. Computers & Security, 24, 409-424.

[17] Janczewski, L. and Fu, L. 2010. Social Engineering-Based attacks: Model and New Zealand perspective. Computer Science and Information Technology, 847-853.

[18] Hadnagy, C. and Wilson, P. 2010. Social Engineering: The Art of Human Hacking, Wiley.

[19] Solutions, V. E. 2014. 2014 Data Breach Investigations Report (DBIR).

[20] Siponen, M., Pahnila, S. and Mahmood, M. A. 2010. Compliance with Information Security Policies: An Empirical Investigation. Computer, 43, 64-71.

[21] Greitzer, F. L., Strozer, J. R., Cohen, S., Moore, A. P., Mundie, D. and Cowley, J. Analysis of Unintentional Insider Threats Deriving from Social Engineering Exploits. Security and Privacy Workshops (SPW), 2014 IEEE, 17-18 May 2014 2014. 236-250.

[22] Peter, K., Guttorm, S. and Raimundas, M. 2012. Comparing Misuse Case and Mal-Activity Diagrams for Modelling Social Engineering Attacks. International Journal of Secure Software Engineering (IJSSE), 3, 54-73.

[23] Jagatic, T. N., Johnson, N. A., Jakobsson, M. and Menczer, F. 2007. Social phishing. Communications of the ACM, 50, 94-100, 0001-0782.

[24] Shakarian, P., Shakarian, J. and Ruef, A. 2013. Introduction to cyber-warfare: A multidisciplinary approach, Newnes.

[25] Brykczynski, B. and Small, R. 2003. Reducing internet-based intrusions: Effective security patch management. Software, IEEE, 20, 50-57.

[26] ENISA. 2014. Information Security Glossary [Online]. European Union Agency for Network and Information Security (ENISA). Available: http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary#G11 [Accessed 15/02/2014 2014].

[27] Okoli, C. and Pawlowski, S. D. 2004. The Delphi method as a research tool: an example, design considerations and applications. Information & management, 42, 15-29, 0378-7206.

[28] Mulligan, P. 2002. Specification of a capability-based IT classification framework. Information & Management, 39, 647-658. 0378-7206.

[29] Maitland, N. B. and Osei-Bryson, K.-M. 2014. Hybrid VFT/Delphi Method to Facilitate the Development of Information Security Strategies in Developing Countries.

[30] Westby, J. R., 2004. International Guide to Privacy. Chicago, ABA Pub.