Information Asset Valuation Method for Information Technology Security Risk Assessment

Farhad Foroughi *

Abstract—**The information security strategic plan is necessarily comprehensive, including business processes, people, and physical infrastructure, as well as the information system. The Security risk evaluation needs the calculating asset value to predict the impact and consequence of security incidents. The return on security investment (ROSI) is defining the value for all invested in terms of security by determining the cost of assets that may disturb in security breaches and the cost of its impact. Knowledge is the source of many competitive advantages for businesses and it should protect against theft, misuse and disasters by adequate security controls. All elements that involved in the knowledge creation process are knowledge assets. An IPO model with a combination of Skandia and Balanced scorecard methods needs to develop a measurement system for knowledge asset value assessment. This model recognizes the role of customers and employees as the natures of knowledge and concentrates on a wide range of factors involved in organization such as processes, structures and development elements that has not been tried before. The model in addition includes structure capital variables that emphasized ICT factors those are investing knowledge into the company's competitive advantage.**

Index Terms—**Asset Assessment, Information Security, Knowledge Asset Valuation, Return On Security Investment, Risk Assessment.**

I. Introduction

Since the Cyberspace opened its doors for commercial and business related activities through the Internet and World Wide Web in 1993, it has become the focus for information security. The cyber-market via the Internet was the second step in there and companies in all markets independent of size and business revenue interested to become this new potentiality for better competition.

The skills and strategies are two key factors in the cyber market and companies require them for successful business. The information security strategy is one part of the whole strategy plan and they must concentrate on it. This was very different in the physical market.

The first step in the information security strategic planning in any form of businesses is the risk management and risk evaluation. This is necessarily broad, including business processes, people, and physical infrastructure, as well as the information system. The Security risk evaluation needs to assess the asset value to predict the impact and consequence of any dangers but it is difficult to apply this approach to systems built using knowledge-based architectures.

Knowledge is the cause of many competitive advantages for businesses and it should protect against theft, misuse and disasters by adequate security controls. This is very important related to current economic, social and political conditions.

The cyber-terrorism's target is disrupting the flow of information and knowledge assets and attacking the systems of the organization. With the growth in hacking, sniffing, spamming, viruses, and other nuisances that intercept, and destroy electronic networks; knowledge and information assets are increasingly at risk. For example, in case of documents, software code will steal or loss when an organization has poor intellectual property protection measures in place. However, cyber-terrorism is difficult to control because it works from any location on the world at any time and from almost any communication channel but protection and prevention mechanism related to knowledge management may decrease the impact of attacks or their consequences.

In case of distributed and heterogeneous environments, managing knowledge security is more difficult. The government sectors may involve e-government and e-commerce services should more attend on this point because of most valuable information provided or served but private organizations should focus on knowledge that made by human resources [1]

The Return on Investment (ROI) metric has been traditionally used in the business world to measure the effectiveness of a given investment. In terms of security management, return on security investment (ROSI) is defining the benefit of security investment by determining the value of assets that may disturb in security breaches and the cost of its impact. However, “security consumers will require understanding the variables that define ROSI and endure the discomfort of assigning cost values to quantities that currently are extremely ill-defined” [2].

This paper discusses about a ROSI method and knowledge asset valuation model to find how much investment accepted according to risk analysis. In organizations that business based on knowledge-services, the crucial is that what the knowledge asset is and how to value that. This will define in the following.

* Farhad Foroughi is with University of Sunderland

II. Security Investigation

Top executive managers and decision makers don't need to know how a security control works to protect company's knowledge. They just want to know the contribution value and cost of information security.

They want to know: [3]

- The cost of security lack in terms of business
- The consequence of a security breach on productivity
- The impact of a sudden great damage in information security breach
- The most cost effective solution
- The effect set of founded solution against breach on productivity

According to the CERT report, the cost of security breaches increases same as the number of that. The 2006 CSI/FBI Computer Crime and Security Survey revealed that 56% of respondents detected security breaches. The ROSI calculation could help to find the possibility of threats, probability of vulnerabilities and the cost impact of breaches related to information security risk analysis. In other hand, ROSI determines an approach that is based on the cost effectiveness of investment. The very important point in there is indirect estimation of cost value associated with security incidents such as the loss in the market. While loss estimates can be a useful starting point in convincing firms to deploy security technologies, they are less useful to firms in deciding which technology to install or how much money to spend [2].

The information security risk management develops the level of risk that exists within the organization and the level of acceptance risks and ignored once. This attempts to assign numeric values to the likelihood and potential damage and to components of security controls such as its cost and effectiveness. After this quantitative analysis, technical managers and security professionals may mitigate the risk up to an acceptable level by implementation of security infrastructure and security control measures. These controls categorized in preventive and detective controls.

According to this approach and after the controls selection, security policies and procedures will address required response and treatment to security breaches such as training. These responses may be executed manually or automatically depending on its cost. The Monitoring process determines whether a system works correctly and analyzes the log files and audit trails.

III. ROI/ROSI Calculation method

The selection of control which has most value with minimum cost is the fundamental point that ROI should address. That is the best way to compare alternative investment strategies. ROI may be a factor in most companies for deciding which technology or extended capability of existing technology should use [3].

The factors involved in ROI calculation are the expected returns, the cost of investment and the life of item. ROI calculated simply by following formula: [4]

$$ROI = \frac{\text{Expected Returns} - \text{Cost of Investment}}{\text{Cost of Investment}}$$

According to this formula, the following equation must use to calculate the value of ROSI : [4]

$$ROSI = \frac{(\text{Risk Exposure} * \text{Risk Mitigated } (\%)) - \text{Solution Cost}}{\text{Solution Cost}}$$

The seeking of these parameters is no simple task. There is no standard definition, model or methodology for determination of security breaches' financial risk. This is also same for valuation of security incident's cost. Likewise, finding the level of mitigating effectiveness of security controls is a complex task. Both of them should monitor in a period of time to find the answer of the above questions but the time is the most valuable things in security.

The processes of solution cost evaluation can change in terms of cases. Sometimes, it just includes hardware, software and service cots but in somewhere else, it involves with indirect overhead and constant impacts on productivity (internal costs).

A. Quantifying Risk Exposure

The accuracy and result of quantitatively measuring risk exposure depends on statistics and experiences of past years activities and consequences. This is very important to use accurate data and trustable statistics for ROSI calculation because future decisions based on that. Unfortunately, the information of previous incidents or security breaches does not exist in the beginning of information security strategic planning in the most companies or organizations. In terms of this problem, there are two approaches to use that. Firstly, ROSI is a very useful tool for comparing security solutions according to their cost and consequence. This means, it can just compare alternative solutions together for seeking the best one. The “inaccurate” information can be used in some cases when they are repeatable or consistent metrics [4]. Secondly, the "best" actuarial data found and developed by some annual surveys of businesses conducted by the Computer Security Institute (CSI) and the U.S. Federal Bureau of Investigation (FBI). This information collected from the businesses that estimated the cost impact of security breaches and incidents for a large number of groups and categories in period of one year.

According to the Sonnenreich's research [4], “risk exposure is to multiply the projected cost of a security incident (Single Loss Exposure, or SLE) with its estimated annual rate of occurrence (ARO). The resulting figure is called the Annual Loss Exposure (ALE).”

$$\text{Risk Exposure} = ALE = SLE * ARO$$

In terms of this method, if no localize data or statistics available depends on organization incident reports for SLE or ARO, these could be estimated as an average rate from CSI/FBI reports depended on real events. The most of these tables are reported by academic institutes, insurance claim data, private or government companies and independent surveys.

B. *Quantifying Risk Mitigated*

Each security control and solution has some mitigation levels but this is difficult to find the amount or degree of these levels same as the measuring of risk exposure.

Some security controls may preventative and someone may detective or corrective. The devices may be used as one of these reasons or a collection of them depends on vulnerable facts. After implementation, to represent the amount of mitigated risk, a security assessment must run in consist of a scoring algorithm. The security assessment model must capture the all implementation and installation impacts and the scoring algorithm must express the impact of time. The assessment model is based on usability and productivity, and the algorithm is based on solution effectiveness.

In terms of this assessment method, some significant problems related. These are: [4]

- Risks are not isolatable
- Security solutions do not work in
- Security solution must be effective without any unwanted effect on productivity
- Hackers are going to find new vulnerabilities in systems. Because of this, the security solutions may not be effective after a period of time

The quality and accuracy of the score for mitigated risk depend on the algorithm and method that used. The International Security Forum (ISF), the International Standards Organization (ISO) and National Institute of Standards in Technology (NIST), have guidelines for this. These are good practices for assessment. In this paper, we will not talk more about this part of calculation and just find good points related to knowledge and information assets.

C. *Quantifying Solution Cost*

The cost of a solution is not just its price. The internal costs such as implementing, maintaining and support costs need to be taken into consideration. In other hand, productivity is an important point that affects on cost because security always comes at the cost of convenience. Some security solution may change employee routine activities or may need new jobs and responsibility in organization. With increasing of created security solutions productivity, the cost may be decreased. This occurs when a result or side effect of the solution is going to eliminate other important problem issues that is effecting productivity. For example, regarding to knowledge and information assets, training and awareness will dramatically increase the productivity of security solutions. This impact can be measured by re-running an audit and survey to estimate risk exposure. Sonnenreich [4] says "The cost of a solution must include the impact of the solution on productivity, since this number is often large enough to make or break the viability of a given solution."

IV. Knowledge Management Systems

In the meaning and calculating of ROSI, the accuracy of the asset value is so important. It would be completely challenging in terms of knowledge and information assets. Therefore, In terms of knowledge asset classification, cost factors are more considerable. These should be measurable free from outside control or directly related to the classification.

There are two serious costs. The cost of lowering high secure information as a valued intellectual property is an important issue. The impact of a security incident such as information theft may make a critical loss for system without any outcome on productivity. Likewise, the productivity loss that is the result of this security breach is another important cost. In most cases, the cost of lost of productivity is more than the information recovery or system repair cost [4].

Hamilton [5] says that "the definition of an asset is based on an associated value that is derived from any number of relationships between the asset, its producers, consumers and observers."

In the complex applications where data come from multi sources or is an integration of many resources such as knowledge and information, defining an asset is usually a process of compiling and entering meta information for a particular purpose depends on its type. However, in these conditions, the asset value is captured in the associations between that asset and other items included in the workflow.

The asset value definition depends on asset contains and properties and its relationship with other objects. This complex object has one or more sources and zero or more targets that may be a flexible relationship or fix.

Knowledge management, as a discipline, is a process to find and classify the knowledge and information assets because that is the most salient source of sustainable competitive advantages in the organizations. Depends on knowledge management approach, Value out of an asset is determined both by how it is used towards economic ends and also based on its scarcity in the marketplace. This means that an asset has some characteristics of rare, non-imitable factors and non-substitutable parameters in order to organization competition [1]. For example, if the Coca Cola Company was to create this knowledge public, opportunities are serious they would not be able to earn abnormal profits from the marketing of coke. Also, the information assets must be protected against the external world and be available and integrated in corporation for internal use. This is even more important granted current economic, social and political conditions. This is very difficult when it should be distributed in terms of business such as service-base companies.

For knowledge and information asset management, firstly, system and relationships should define. One of the most famous models to determine systems is IPO model. This model has three components: Inputs, Processes and Outputs. This model with additional feedback link will be a knowledge and information management system model with learning capability.

According to the Jennex [6] definition, a system that is processing information by humans or machines is an information system. This processing accomplished by following operations: capturing, transmitting, storing, retrieving, manipulating and displaying. These operations are a part of the information system and participated in system to accomplish a set of goals. This definition develops relationships and sources of objects according to knowledge and information assets. The consideration of the parts of the system is significant in the meaning of relationships to achieve goals. These basic considerations are:

- System Objectives including measures
- System Environment
- System Resources
- System Components, activities, goals and measures of performance
- System Management

ICT (Information and Communication Technology) system developed in organizations to support and enhance knowledge creation, constriction, identification, capturing, selection, valuation, linking, structuring, retention and maintenance [6]. This knowledge and information found in documents, organizational routines, processes, practices and norms. The element of human context, experience and interpretation is included in knowledge definition.

As a definition, "Knowledge is created through the interaction and intersection between tacit and implicit knowledge, following four different modes of conversion: Socialization, Externalization, Combination, and Internalization (SECI)" [7].

Aramburu [8] says, all elements that involved in knowledge creation process, are knowledge assets. Likewise this definition, information assets are those elements that involved in information creation processes. These may be an input, output or a moderator of this process. For example, the trust between personnel is a result of the process of information and knowledge creation in organization. These assets categorized into four different types:

1- Experiential knowledge assets consist of the tacit knowledge that is built through shared hands-on or working experience among employees. This knowledge found in coordination activities between all members, customers and suppliers and because the time is significant parameters in its creation process, that is very valuable and in terms of calculation the value, time-cost should calculate. This kind of knowledge asset in terms of intellectual capital called human capital that is usually in the minds of individuals.

2- Conceptual knowledge assets consist of explicit knowledge articulated through images, symbols and languages. These assets usually held by customers and employees. The time-cost is important here too but the period of that is shorter than time period in experiential knowledge assets. The customer relationships, brands and trademarks are some example of this type of assets. According to intellectual capital, this kind of assets called Relationship Capital.

3- Systemic knowledge assets consist of systematized and packaged explicit knowledge. This kind of knowledge sometimes called information asset. For example, technologies, manuals, documents, information about customers and suppliers and product specifications are some kind of that. The intellectual property is meaning in this part of knowledge and legally should protect by licenses and patents. These assets are very valuable and in calculation of value should attend on business competition parameters and advantages. The security risk of these assets is high because most of them are visible and tangible.

4- Routine knowledge assets. This type of asset consists of the tacit knowledge that is embedded and regulated in the actions and practices of a firm. This may include the culture, practices and organization's procedures. The processes, information systems and databases are some example of this. The time of life for this kind of assets may short or long because some of these will expire very soon such as day-to-day procedures and others may need long time to re-create such as organizational culture. In terms of intellectual capital this kind of assets called Structural Capital that is left after employees go home after work-hours.

V. KNOWLEDGE ASSET VALUATION

A. Asset Valuation Method

There are too many classification methods available. One of these methods is to classify assets regarding to law. These are protected as intellectual property and cover trade-marks, patents, copyrights, licenses. This is important to develop a group of measures for using in assess progress during the classification process [9]. These measures according to Skandia that presented in figure 1 are as follows:

- **Financial:** income per employee, market value per employee etc.
- **Customer:** number of customer visits, satisfied customer index, lost customers
- **Process:** administrative error rate, IT expense per employee
- **Renewal and Development:** training per employee, R&D expense/administrative expense, satisfied employee index
- **Human:** leadership index, employee turnover, IT literacy.

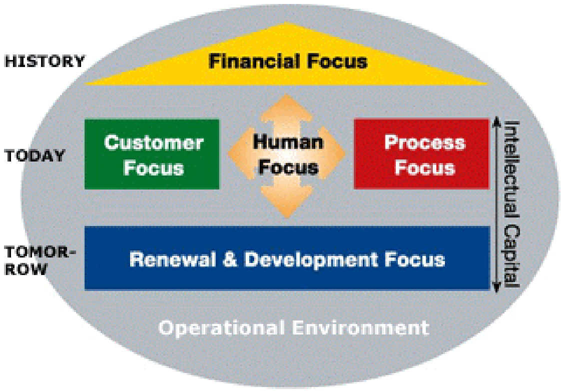

Figure 1: Skandia measures. [10]

These measures should be a part of BSC (balanced score-card) method which developed by Kaplan and Norton and adds non-financial measures to the traditional financial measures. This method should involve in IPO model. To keep score we should develop a measurement system by using above measures appropriate to each business unit. This means the base method is BSC and the measures will come from Skandia. A sample table is as follow:

Table 1: Sample of Skandia measures. [10]

Financial Focus	• revenues / employee ($) • revenues from new customers / total revenue ($) • profits resulting from new business operations ($)
Customer Focus	• days spent visiting customers (#) • ratio of sales contacts to sales closed (%) • number of customers gained versus lost (%)
Process Focus	• PCs / employee (#) • IT capacity – CPU (#) • processing time (#)
Renewal and Development Focus	• satisfied employee index (#) • training expense / administrative expense (%) • average age of patents (#)
Human Focus	• managers with advanced degrees (%) • annual turnover of staff (%) • leadership index (%)

This model is particularly impressive in recognizing the role of customers and employees as the natures of knowledge in calculation of cost value. This also concentrates on a broad coverage of organizational structural and process factors and development contributions that has not been attempted before.

Lynn [11] points out that this uses proxy measures of intellectual capital to track trends in the assumed value added and follows a balance sheet approach in knowledge and information assets measurement.

Finally, more than a method for intangible assets, ICT factors included in structure capital variables emphasized as creators of true value because contribution of employees and their computers and networks end up investing knowledge into the company's competitive advantage.

B. Success Factors And Guidance

Following significant points should be attended during knowledge asset assessment for better accuracy and quality of calculation [12].

Firstly, the organizations should develop a program of awareness for the nature of intellectual capital and knowledge role understanding. In this way, creating a common language that is more widely diffused within their companies should be attended.

Secondly, Managers should identify suitable illuminating indicators and determine a measurement model in a relational framework. Introducing measurement systems, including the accompanying management processes is the next level that guide and reward managers.

Finally, information security risk managers should use objective impartial consultants and surveys with an active communication and involvement to carry out key aspects of the measurement process.

VI. Conclusion

The risk management is the first stage of information security strategic planning and security control selection. In this area, cyber-terrorism attacks to information and knowledge assets specially those distributed or placed in heterogeneous environments.

To define a good security policy and develop adequate control to mitigate security risks, most value with minimum cost is the fundamental approach. ROSI calculation is the best way according to do this because it can compare the cost of control implementation against the impact's cost of security incident. In the calculation of this, risk exposure is the combination of single loss exposure and annual rate of occurrence. In terms of single loss exposure, the cost of assets is the major point. This means the accuracy of the asset value is very significant and would be completely challenging for knowledge and information assets. Therefore, In terms of knowledge asset classification, cost factors are more considerable. These should be measurable free from outside control or directly related to the classification.

In this approach, knowledge and information assets classified to four categories those are the experiential knowledge, the conceptual knowledge, the systemic knowledge and the routine knowledge [13]. According to this classification, Skanadia Navigator method used to assign cost and weight to the assets by their contents. These contents categorized into five groups. The financial capital, the customer capital, the process capital, renewal and development capital and human capital are these groups. This method should be used with combination of balanced scorecard method which developed by Kaplan and Norton. With these two methods, we can measure both financial and non-financial value of knowledge assets [14].

As a result and according to the reasons that presented in this paper, the method that defined is the unique understanding of which knowledge and information asset is truly valuable for the organization to choose which assumption is most valid and identify appropriate metrics.

References

[1] K. Desouza & G. Vanapalli. (2005, 01, 06) Securing Knowledge Assets and Processes: Lessons from the Defense and Intelligence Sectors. *Proceedings of the Proceedings of the 38th Annual Hawaii International Conference on System Sciences*, vol. 1.

[2] H. Cavusoglu, B. Mishra, & S. Raghunathan. (2004, 07) A model for evaluating IT security investments. *Communications of the ACM*, vol. 47, no. 7.

[3] S. Dray, C.M. Karat, D. Rosenberg, D. Siegel & D. Wixon. (2005, 04) Panels: Is ROI an effective approach for persuading decision-makers of the value of

user-centered design?. *CHI '05 extended abstracts on Human factors in computing systems.*

[4] W. Sonnenreich. (2005, 04, 06) Return On Security Investment (ROSI): A Practical Quantitative Model. *SageSecure, LLC.* [Online]. Available: http://www.infosecwriters.com/text_resources/pdf/ROSI-Practical_Model.pdf

[5] G. Hamilton. (1999, 10) CataLogger: A Framework for Building Asset Management Solutions. *Proceedings of the 23rd International Computer Software and Applications Conference*.

[6] M. Jennex. (2006, 01) Classifying Knowledge Management Systems Based on Context Content. *Proceedings of the 39th Annual Hawaii International Conference on System Sciences***. v**ol. 7, pp. 156b.

[7] S. Chou & M. He. (2004, 01, 08) Facilitating Knowledge Creation by Knowledge Assets. *Proceedings of the 37th Annual Hawaii International Conference on System Sciences,* vol. 8, no. 8.

[8] N. Aramburu, J. Sáenz & O. Rivera. (2006) Fostering innovation and knowledge creation: the role of management context. *Journal of Knowledge Managemen,* vol. 10, no. 3, pp.157-168.

[9] H. Chivers & J. Jacob. (2005, 06, 10) Specifying Information-Flow Controls. *Proceedings of the Second International Workshop on Security in Distributed Computing Systems (SDCS),* vol. 02.

[10] N. Bontis. (2001, 03) Assessing knowledge assets: a review of the models used to measure intellectual capital. *International Journal of Management Reviews,* vol. 39, no. 1, pp.41-60.

[11] L. Lynn. (1998) *The Management of Intellectual Capital: The issues and the practice.* Society of Management Accountants of Canada. Ontario: Hamilton.

[12] T. Stewart. (1997) *Intellectual Capital: The New Wealth of Organizations*. New York: Doubleday/Currency.

[13] A. Kadam. (2002, 12) Identifying and classifying assets. *Network Magazine India.* [Online]. Available: http://www.networkmagazineindia.com/200212/security2.shtml

[14] L. Yan & P. Baldasare. (2006, 08) Industrial and government applications track posters: Beyond classification and ranking: constrained optimization of the ROI. *Proceedings of the 12th ACM SIGKDD international conference on Knowledge discovery and data mining.*