Information Security Expenditures: a Techno-Economic Analysis

Theodosios Tsiakis
Research Assistant, Dept of Logistics, Technological Institute of Thessaloniki, Branch of Katerini, Greece

Summary
Information Security is considered to be an inextricable part of companies' expenditures and there are defined amounts that are invested for its accomplishment, although it is really difficult to determine the best Security Solution. The substantive problem of information security risk is value proportion of information properties or assets. Risk analysis can be approached from two evaluation models: the qualitative and the quantitative. Quantitative analysis refers to the use of numeric calculations and statistical techniques. Qualitative analysis describes methods that consider loss in a subjective form. Without measurement and metrics of information security we will not be able to estimate and process Information Security Strategies. The aims of this paper are to gain an understanding of Quantitative and Qualitative analysis and furthermore to both evaluate and improve the use of those methods.

Key words:
Risk, Information Security, Quantitative and Qualitative Analysis.

1. Introduction

As the world becomes more connected and an increasing amount of business is transacted electronically the computer and information security will continue to grow in importance [1]. But before we step forward to the concept and means of security we need to understand that the most important characteristic of an object transacted electronically is its value. And that is because for failures to have consequences, electronic assets must have value. As Gaines and Shapiro [2] designates, value to the potential violator may result from possession of the object (knowledge of the information), or because the violator can use the object. Value may be quantifiable, generally in monetary terms, or it may be determined subjectively and thus be difficult to quantify.

Security is an intricate property that is achieved by a combination of sufficiently strong cryptographic algorithms and protocols, correct implementation of hardware and software, and appropriate assumptions about trusted authorities [3]. Security is a constant process that is strongly related to today's society evolution and not a solution [4]. Security properties describe the ability of principals to access information or resources. Key security properties include [5], [6]:

- *privacy or confidentiality*: setting principal which information are and can be revealed to authorised people
- *integrity:* detection of whether the data has not been altered, manipulated or corrupted by unauthorized parties;
- *authentication:* providence of the identity of a principal or the source of information;
- *access control:* restricting or controlling the actions of a person or entity, based upon its identity
- *non-repudiation:* preventing person or entity from denying their actions;
- *availability of service:* guaranteeing authorized persons or entities to have continuously and uninterrupted access to services.

Canavan [7] looks security as a trinity (figure 1) consisting of:

- Prevention – foundation, preventative measures over detection and response
- Detection – once measures implemented, procedures need to be placed in order to detect potential problems
- Response – identifies the appropriate response to a security breach

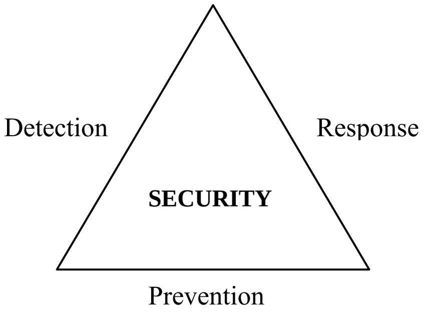

Fig. 1 The Security Trinity.

The determination of security requirements for a given system, and the selection of appropriate security mechanisms (including security policy) are a part of the risk management activity. The basic steps are value and criticality analysis, vulnerability analysis, threat identification, risk analysis, risk assessment, security safeguards selection and implementation, development of contingency plans, and effectiveness reviews [8]. The

Manuscript received April 5, 2010
Manuscript revised April 20, 2010

better the risk model, the better the security decisions that can be made using its forecasts [9]. The only thing that security policy specifies (figure 2) is what should be protected, but does not impose any measures. In simply words policy necessitate certain process on who (person or entity) has specific permission and what he can do with information. From the moment the security policy has been employed the sequential stage is to enforce it [10].

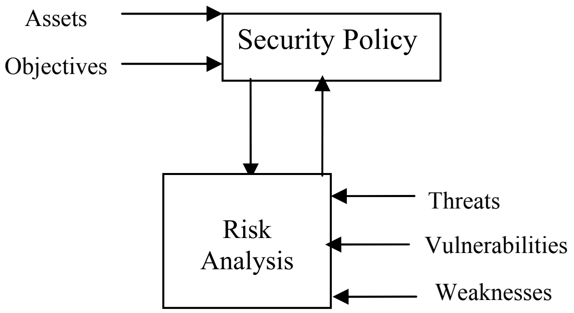

Fig. 2 Security Policy and Risk.

An *asset* is defined as any element of an information system that possess a value [11]. It includes tangible (software, hardware, personnel) and intangible assets (plans, organization, external factors, technical factors). In risk process an object is called asset when there is an effect in objects value when risk emerges. A *threat* is defined as any possible harm to the system, including network failures and natural disasters. Vulnerability is a weak point where the system security is susceptible to attack [12], [13]. Threats need to exploit certain vulnerability in order to cause a security incident. Therefore, threats, vulnerabilities, and impacts should be combined together to provide a measure of the risk. This is given in figure 3.

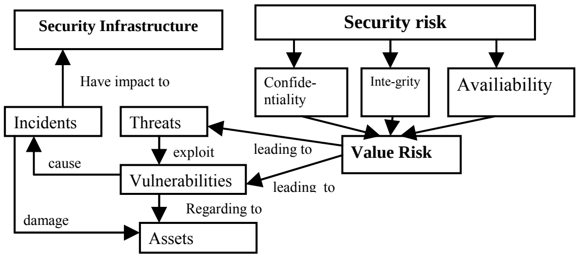

Fig. 3 The process or Risk.

By Security Architecture we mean the consideration of how a company's systems (in the widest sense) should be designed to ensure that the company meets its security objectives [14]. A security Infrastructure is the practical realization of a security Architecture in a tangible and usable form. A security objective is the contribution to security that a system or a product is intended to achieve [15]. The term security objective must not be confused with security services that are defined as "a processing or communication service that is provided by a system to give a specific kind of protection to system resources" or — with more emphasis on communication in as "a service, provided by a layer of communicating open systems, which ensures adequate security of the system or of data transfer" [16]. Therefore, security objectives are the goals that are to be achieved, while security services are means to achieve these goals.

We can picture this in the following ideogram as:

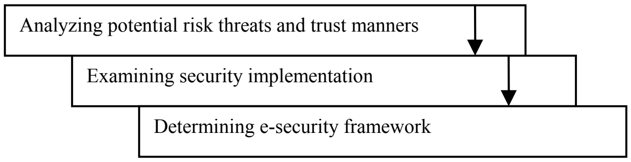
Analyzing potential risk threats and trust manners
Examining security implementation
Determining e-security framework

Fig. 4 Implementing Security.

Analyzing the security sceptic – logic we conclude in:

1. Identification of the system and its components
2. Identification of the system assets and their value to the system
3. Security objectives for the assets
4. The threats and vulnerabilities the assets face of will face
5. Valuation (financial) of security process through risk management
6. Design and establishment of security principals applicable to the organization system

2. Risk Concept

Every human endeavour involves risk [17]. The majority of people think that risk constitutes something negative or bad. But Labuschagne and Eloff [18], shows that we need to think of risk as mere opportunities, and the reason is that in most business environments, the number or size of the risks taken usually is equal to the number or size of the advantages to be gained. The reverse is also true. Risk has been studied from many perspectives. Kumar, [19] studied risk in a detailed theoretical analysis of the anatomy of risk and risk and uncertainty in the context of the value of information.

Risk (R) in the simplest form is the product between event probability P(E) and the possible damage, mostly described as an Impact (I) [20].

$$R(E) = P(E) \bullet I(E) \qquad (1)$$

Where R(E) = risk of an event, E = Event, P = Probability and I = Impact.

The scope is to replace risk with acceptable risk as Jackson and Al-Hamdani [21] formulate:

$$\text{Security Investment} \leq \text{Acceptable Risk} \geq 0 \qquad (2)$$

3. Implementing Risk Evaluation methods (measurement)

Over the last five years there is a tremendous interest to implement - apply economic analysis to information security issues [22], [23], [24], [25]. And that is due to demand to define risk quantitatively so that information security can be addressed in a consistent, predictive and repeatable way [26], [27], [28]. Furthermore economic analysis often explains security failure better from technical analysis.
Measurement of risk of an organisation can be conducted by two different measurements, Quantitative or Qualitative [29]. We use those measurement methods in order in one hand to understand and evaluate problems and in the other to predict and improve processes, products and strategies.

Quantitative risk analysis or Quantitative measures is a mathematical approach to assign numerical value in order to measure the amount of damage dome to an asset. Asset(s) values are expressed in monetary terms and threat(s) frequency in annualized expressions that represent actual expected frequency (e.g., 1/10 for once in 10 years, or 50/1 for 50 times per year) [30]; [31].

Qualitative risk analysis or measure is the simplest form of relative value assigned to a risk, for estimating potential loss using subjective measurement such ordinal ranking (low risk or value, medium risk or value, and high risk or value) in a risk-to-value matrix. As everything there is positive and negative side. So looking qualitative versus quantitative we have the following Tables (1and 2):

Table 1: Qualitative Pros & Cons

Qualitative – Pros	Qualitative – Cons
Calculations are simple	Process and metrics are subjective
No need to assign monetary value or threat frequency	No value calculation
Cost of risk does not need to estimate threat and measures	No basis is provided for cost/benefit analysis
	Not objective way to management risk and analyze impact

Table 2: Quantitative Pros & Cons

Quantitative – Pros	Quantitative – Cons
Value of information in monetary terms is objective	Calculations are complex
Return on Investment on Security implementation can be measured	A great amount of information must be gathered
Risk management can be evaluated	Common Standards lack for risk/threat.

4. Establishing Quantitative Risk Analysis

Information security management is closely related with financial decision making. The question whether we need more security (certain products), has turned to how much should we spend for added security. But spending more doesn't necessary means that we are more secure. It is true that good security costs a lot to implement [32] while on the other hand, the cost of actually detecting and responding to problems and security breaches is not as high [33].

The fact that security technology is advancing at a tremendous speed but the problem still remains indicates that the key solution to the problem is not with technology but with how people implement security technology [34].

This sceptic leads us to the reality that we need to educate people to risk management model that reducing cost without increasing risk. Information security investments concerning well established technologies such as firewalls and anti-virus software is easier because the economics of these technologies are already well understood. The problem emerges from new investments where the results are far less tangible [35]. Specific, information security managers are confronted with great difficulties evaluating and justifying security technology investments because the technology benefits are difficult to estimate and these benefits depend on attack(s) frequency expectation, damage occurrence and effectiveness of security technology to mitigate the damage(s) from an attack(s) [36].

The first simple method is estimation of Annualized Loss Expectancy (ALE) [37], [38], [39]. We need to calculate:

Asset **V**aluation (**AV**): The process that distributes every information financial value.

Exposure **F**actor (**EF**): Is expressed within a range from 0 to 100 percent that an asset's value will be destroyed by risk.

Single **L**oss **E**xpectancy (**SLE**): Is the calculation of expected monetary loss every time a risk occurs.

The Single Loss Expectancy, Asset Value(AV), and exposure factor(EF) are related by the formula:

SLE = asset value (AV) x exposure factor (EF) / SLE = AV * EF (3)

Next we find **A**nnualized **R**ate of **O**ccurrence (**ARO**): The probability that a risk will occur in a particular year.

Annualized **L**oss **E**xpectancy (**ALE**): is the annually expected monetary loss that can be expected for an asset due to a risk. It is determined by the two input values: the cost of the damage and the probability that the loss will occur. It's calculated as:

ALE = SLE * ARO (4)

The second formula is **R**eturn **O**n **I**nvestment. ROI as it names indicates simply defines how much will be received for what I have spent [40]. By spending we mean things such as equipment (Firewalls, Antivirus, etc), administration (Per hour cost of all security activities) etc. So ROSI, acronym of **R**eturn **o**n **S**ecurity **I**nvestment, as defined by Davis [41], measures how much security investment reduces the risk. The calculation of the financial return from an investment in security is based on the financial benefits and costs of that investment. Sonnenreich et al. [42] calculated ROI, as the cost of a purchase is weighed against the expected returns over the life of the item (1).

$$ROI = \frac{Expected\ Returns - Cost(Investments)}{Cost(Investments)} \quad (5)$$

A simplified example of an ALE calculation that describes the above approach is to multiply the cost of a potential exposure, times the likelihood that it will occur. In a case that we have a server that costs (has an asset value of) 20000 €, an Antivirus 1500 € and Infrastructure 1000000 € we can produce the following results (Table 3).

Table 3: Example of cost Implementation

Asset	Asset Value	Threat	EF	SLE	ARO	ALE
Server	20000 €	Failure	100%	20000 €	0.35	7000 €
Antivirus	1500 €	Virus	20%	300 €	0.51	153 €
Infrastructure	1000000 €	Fire	40%	400000 €	0.07	28000 €

5. Conclusions

The goal of security is to protect the distributed information, in Information Systems and Networks from any source and type of threat. The study of the literature impose that approaches for measurement of Information Security are relied on the measurement and analysis of risk. The cost of Information Security however, can't be calculated with precise as the information and substructures have subjective value and perception. The question that arises is twofold. Firstly when the information or system is considered secure and secondly what is its price for it. The higher price-cost doesn't mean that we have the higher level of security. We proposed the risk analysis methodology that should be followed, also tried to investigate, if the adoption of security countermeasures constitutes operational cost, or value-added cost. This paper outlined the results and introduced an approach to demonstrate that investments in Information Security can be measured (Qualitative and Quantitative) and analyzed with certain methods.

References

[1] J., Johnston, Eloff P., Labuschagne, L. "Security and human computer interfaces". Computers & Security 22(8), pp. 675-684, 2003.

[2] S. Gaines, N. Shapiro, "Some security principles and their application to computer security". ACM SIGOPS Operating Systems Review 12(3), pp. 19-28, 1978.

[3] S. Older, S. Chin, "Formal Methods for Assuring Security of Protocols". The Computer Journal 45(1), pp. 46-54, 2002.

[4] M. Sandrini, "We want security but we hate it. The foundations of security technoeconomics in the social world, from control to surveillance". 2nd Annual Workshop on Economics and Information Security, 2003.

[5] T. Peltier, "Information Security Risk Analysis", CRC Press. 2005.

[6] B. Suh, I. Han, "The IS risk analysis based on a business model". Information & Management 41, pp. 149–158, 2003.

[7] J. Canavan, "The Fundamentals of Network Security". Boston: Artech House, 2001.

[8] R. Turn, "Security and privacy requirements in computing". Proceedings of ACM Fall joint computer conference, pp 1106–1114, 1999.

[9] S. Schechter, "Toward Econometric Models of the Security Risk from Remote Attacks". The Third Annual Workshop on Economics and Information Security (WEIS04), pp. 13–14, 2004.

[10] B. Decker, "Introduction to Computer Security". Lecture Notes in Computer Science 1528, pp. 377-393, 1998.

[11] E. Loukis, D. Spinellis, "Information Systems Security in the Greek Public Sector". Information Management and Computer Security 9(1), pp. 21–31, 2001.

[12] M. Myerson, "Risk Management Processes for Software Engineering Models". Boston: Artech House, 1997.

[13] Spinellis, D., Kokolakis S., Gritzalis, S. "Security requirements, risks and recommendations for small enterprise and home office environments". Information Management & Computer Security 7(3), pp. 121-128, 1999.

[14] A. Wright, "Controlling Risks of E-commerce Content". Computers & Security 20(2), pp. 147-154, 2001.

[15] S. Röhrig, K. Knorr, "Security Analysis of Electronic Business Processes" Electronic Commerce Research 4(1-2), pp. 59-81, 2004.
[16] D. Abrams, S. Jajodia, J. Podell, J. " Information security: an integrated Collection of essays". IEEE Computer Society Press, 1995.
[17] J. Chapman, "Effectiveness of working group risk identification and assessment techniques. International Journal of Project Management 16(6), pp. 333-43, 1998.
[18] L. Labuschagne, J. Eloff, "Electronic commerce: the information-security challenge". Information Management & Computer Security 8(3), pp. 154-157, 2004.
[19] R. Kumar, "Managing risks in IT projects: an options perspective". Information & Management 40(1), pp. 63–74, 2002.
[20] W. Böhmer, "Evaluation of the Quality of an Information Security Management System (ISMS) or how secure is secure?". Guest lecture at the Gjovik University College, 2006.
[21] L. Jackson, W. Al-Hamdani, "Economic acceptable risk assessment model". Proceedings of the 5th annual conference on Information security curriculum development, pp. 36-39, 2008.
[22] R. Anderson, T. Moore, "The Economics of Information Security", Science Magazine 314, pp. 610-613, 2006.
[23] G. Lawrence, M. Loeb, "The economics of information security investment". ACM Transactions on Information and System Security, 5(4), pp. 438– 457, 2002.
[24] D. Huang, H. Qing, B. Ravi, "An economic analysis of the optimal information security investment in the case of a risk-averse firm". International Journal of Production Economics 114(2), pp. 793-804, 2008.
[25] K. Campbell, L. Gordon, M. Loeb, L. Zhou, "The economic cost of publicly announced information security breaches: empirical evidence from the stock market". Journal of Computer Security 11, pp. 431–448, 2003
[26] A. Drake, "Security and Regulatory Compliance: A Quantitative Risk Management Approach.". Water Conditioning & Purification, pp. 32-34, 2004.
[27] A. Munteanu, "Information Security Risk Assessment: The Qualitative Versus Quantitative Dilema". 6th IBIMA conference, 2006.
[28] J. Shah, M. Murtaza, M. "Information Systems Risk Assessment Methods". Annual Meeting of the Southwest Decision Sciences Institute, 2006.
[29] G. Bornman, L. Labuschagne, "A comparative framework for evaluating information security risk management methods". In proceedings of the Information 3rd Annual ISSA Conference, 2004.
[30] W. Ozier, " Risk Metrics Needed For IT Security". At http://www.securitypronews.com, 2003.
[31] McAfee Foundstone, "Information Security Metrics Using FoundScore to assign metrics and measure enterprise risk". White Paper, 2006.
[32] Schneier, B. (2004) Secrets and Lies: Digital Security in a Networked World. New York: Wiley
[33] B. Lampson, "Computer security in the real world". Computer 37, pp. 37-46, 2004.
[34] F. Tabba, "Why Computer Security Fails – An Economic View". Technical Report, 2005.
[35] D. Taylor, "Economic Models for Information Security". SC Magazine, at http://www.scmagazineus.com/Economic-Models-for-Information-Security/article/30614, 2002.
[36] S. Butler "Security Attribute Evaluation Method: A Cost-Benefit Approach". International Conference on Software Engineering, 2002.
[37] C. Lin, W. Yu, K. Lin, "Apply Cost-Benefit Analysis Methods to Information Security Assets in Taiwanese Local Government --- An Initial Study". Proceedings of the 13th Asia Pacific Management Conference, Melbourne, pp. 1076-1080, 2007.
[38] S. Bistarelli, F. Fioravanti, P. Peretti, "Defense trees for economic evaluation of security investments". Proceedings of the First International Conference on Availability, Reliability and Security (ARES'06), 2006.
[39] J. Beachboard, A. Cole, M. Mellor, S. Hernandez and K. Aytes, "Improving Information Security Risk Analysis Practices for Small- and Medium-Sized Enterprises" A Research Agenda, Proceedings of I^{n}SITE, 2008.
[40] K. Lucas , "Economic Evaluation of a Company's Information Security Expenditures". Infosec Writers at (http://www.infosecwriters.com), 2005.
[41] A. Davis, "Return on security investment – proving it's worth it". Network Security 11, pp. 8-10, 2005
[42] W. Sonnenreich, J. Albanese, B. Stout, "Return On Security Investment (ROSI) - A Practical Quantitative Modell". Journal of Research and Practice in Information Technology 38(1), pp. 45-56, 2006.

Theodosios Tsiakis received the B.S. degree in Economics from Dept of International and European Economic and Political Studies and Ph.D. in Information Security Economics from Dept of Applied Informatics in University of Macedonia (Greece) respectively. Presently he is Research Assistant at Dept of Logistics in Technological Institute of Thessaloniki (Greece). His areas of interest include Information Systems, Information Security Economics, Risk Management and Human Factors in Security.