SECURITY ECONOMICS MODELLER

A Document submitted for the Scientific Methods

COMP-80142

Syed Usman Shaukat (7562579)

SCHOOL OF COMPUTER SCIENCE

TABLE OF CONTENTS

Word Count excluding References and Definition of Key Terms: 1215

Background of problem:

During the last couple of decades, there has been a tremendous work in information security that people feel was because of security breaches and caused an economic impact on the organization **(Cavusoglu, 2004)**. Organisations began to learn from their past mistakes by realising failures to the business [1]. Researchers stated realisation of risks as key to the business Ross Anderson states bad incentives as one of the reasons for the failures and stresses that building awareness to address critical issues to the business helps both attacker and defender equally. More the awareness increases there are fewer chances of failures to the business [2].

Security economics has been the prime area of concern for researchers, they used security cost estimation as the way to measure the direct impact of security breaches on the business and concluded modelling risks crucial achieving business goals. (Cavusoglu,2004)

Therefore, it was needed to do more research in building up a dependable system, which addresses key functions of the business, shows the loss of earnings and developing an effective way of handling information. This research is a way forward because it addresses key areas concerned with the management for smooth business operations.

Why is this a problem?

On various occasions, it has been noticed that Economics of Information Security is a big issue for business owners because of growing number of losses because of known or unknown vulnerabilities [2][3]. Financial Service Authority on numerous occasions imposed legal fines on various large scale organisations for not taking care of public information. For example on 14th February 2007, Nationwide Building Society has been fined £980,000 for the failure of implementing security controls following theft of an employee's laptop containing customer information [9]. This makes this problem a reason to worry and this research is based on addressing cost of

a. **Security breaches**
b. **Implementing security controls**
c. **Cost of business disruption**

Could this problem be solved by?

This research tries to solve this problem by creating a framework which address all required business functions, brings resilience to the control functions and analysing problem by showing a crossover relationship between **Risks and Risk Mitigation** to create a **Modelling Tool** which takes input from each related process and forms a dependency between each component.

Therefore, tool will mitigate the loss by realisation of risks, risk mitigation strategy and by extending information maturity model.

Research Questions to address:

- How to model the information risks mitigation to the acceptable level?
- How to determine a relationship between vulnerability and level of mitigation of a security control?
- To determine a correlation between the maturity of an organisation and the mitigation of risk through the security controls.
- Measuring cost effectiveness of security controls.
- Establishing a mathematical formula
- To determine how to collect data to test it?

Moreover, to answer whether created framework or modelling tool **works technically or not?**

And does it solve this problem?

Therefore, Security Economics Modeller shows a process of implementing security in following stages

1. Creating a Framework
2. Measurement of Security Breaches
3. Economic Impact of Information Security
4. Implementing Security Controls

Aims & Objectives

Axelsson [2000] stated security measures as best effort to achieve information security when implemented in the form of controls to protect uncertainty of cost required to run the business. According to Crosby's Quality Management Grid[4] if these issues are not fixed then the chances of increase in the cost of running the business may rise and may even result in failure or closure of the business.

According to (Rescorla, 2005), "It is better for vulnerabilities to be found and fixed by good guys than for them to be found and exploited by bad guys."[5] The graph of business performance will rise towards the profit to the business as soon as researchers are able to remove defects from the system.

The objectives of Security Economics Modeller are to create an understanding of the following stages of the project:

<<<< Creating a Framework >>>>

Creating a framework is important in order to measure cost of security breaches, in order to do this we have to address various security issues related to the business especially asset identification, risk identification & mitigation, business impact analysis, maintaining state of forensic readiness and using these processes to model cost of running the business. This framework is directly or indirectly related to the cost model. ***Figure 1*** shows data flow diagram of security economics modeller.

<<<< Measurement of Security Breaches >>>>

Measurement of security threats in such a way that failure of the system does not harm the organization and brings the profit to the business. Security Economics Modeller uses different principles defined in **Crosby's Quality Management Grid** [4] primarily aimed to improve quality by removing defects from the system; by involving risk management, their classification in a way to minimise their threat level and most importantly

to improve the performance of the system and to help determining cost to the business.

<<<< Economic Impact of Security >>>>

Determining the economic impact of information security refers to calculating frequency of potential security breaches, their cost and investment to implement mechanisms. It not only minimizes these breaches but also improves performance of the process as well.

<<<< Implementing Security Controls >>>>

SANS (2008) describes implementing security controls as a plan to address security deficiencies, stresses implementing critical security controls for improved effectiveness of the business. Implementation of these is an ongoing process and helps to conduct a cost benefits analysis by improved risk management strategies [10]. ISO 17799 is a legal framework that helps to implement security principles s set by the organisations. [11]

Methodologies

	OBJECTIVES	TARGET DELIVERABLE	METHOD TO BE USED
Risk Management	a. How to Model? b. How to Measure? c. How to Mitigate? d. Relationship between how much a vulnerability threatens an information system. And how much a security control can mitigate against that risk?	a. Asset discovery & registration b. Business impact analysis and data classification c. Risk assessment and treatment	a. Asset Management b. Qualitative and Quantitative Risk Identification c. Risk Analysis d. Business Impact Analysis e. Risk Classification f. Risk Estimation g. Probabilistic Risk Assessment h. ISO31000 guidelines
Security Maturity	a. Is there a correlation between the maturity of an organisation and the mitigation of risk through the security controls that it implements?	A 5-layer cost of security maturity model extending Crosby's Quality Management Grid	Information Assurance Model Crosby's Maturity Grid

Information Governance	a. Is the governance a separate control or an extension of the technical controls whose implementation it is meant to assure?	Linking these process together to form bases for cost estimation	Information Assurance
Cost Analysis	a. How can the cost effectiveness of security controls be demonstrated? b. What is the formula? c. How can data be collected to test it?	The cost of maintaining a state of forensic readiness around the asset	Cost Analysis based on Security Controls like ACL, Awareness & Training, Audit and Accountability
Testing & Audit	a. How to Audit/Improve/Test security breaches or Loopholes to the particular business? b. Is there any crossover point between these research questions or their inter-relationship?	An evaluation of the tool using selected examples of security breaches and the countermeasures which should have protected against them	CSI Survey Risk Audit

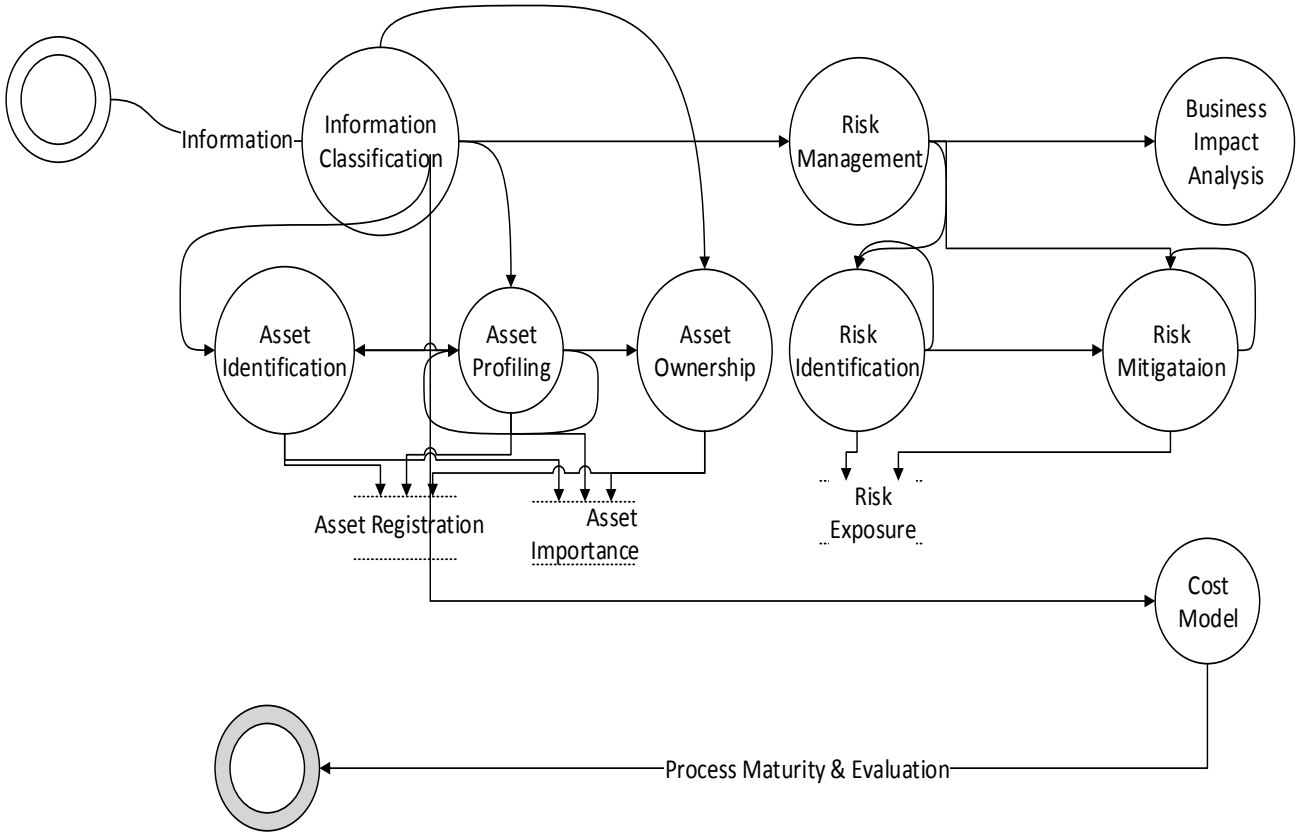

Figure 1: Basic Data Flow Diagram of Security Economics Modeller

Definition of Key Terms

Key Terms	Definition
Attacker	An individual or group(s) of individuals trying to gain access to someone's resources with wrong intentions [6].
Defender	Someone who defends people or property [6].
Risks	Risk is defined as to expose someone or something to a dangerous situation [6].
Risk Mitigation	Is defined as the reduction of exposure to potential problems in the business. From the IT perspective, risk mitigation reduces the vulnerabilities that may lead to an attack on the company's computer systems [6].
Threat	Is a statement of intent to harm or punish, or a something that presents an imminent danger or harm [6].
Vulnerabilities	Vulnerability is a weakness or some area where you are exposed or at risk[6]
Crosby's Quality Management Grid	Crosby's Quality Management Maturity Grid consists of five stages of management maturity (Uncertainty, Awakening, Enlightenment, Wisdom, and Certainty), measured against six dimensions, to complete the matrix [7]
Business Impact Analysis	Business impact analysis (BIA) is an essential component of an organization's business continuance plan; it includes an exploratory component to reveal any vulnerabilities and a planning component to developing strategies for minimizing risk [8].

References

1. J. H. P. Eloff, R. Holbein and S. Teufel (1996) 'Security classification for documents ',*Computers & Security,* 15(1), pp. 55-71 [Online]. Available at: *http://ac.els-cdn.com/0167404895000232/1-s2.0-0167404895000232-main.pdf?_tid=9fe4133c-c2b5-11e4-9ae5-00000aacb362&acdnat=1425504785_ff09d19af1e3a05fa0feee445101a250*(Accessed: 15th December 2014).
2. Ross Anderson and Tyler Moore (2008) 'Information Security Economics – and Beyond',*Information Security Summit,* (), pp. [Online]. Available at:*http://www.cl.cam.ac.uk/~rja14/Papers/econ_czech.pdf* (Accessed 28th February 28, 2015).
3. M. Eric Johnson (2009) 'Managing Information Risk and the Economics of Security',*Center for Digital Strategies, Tuck School of Business, Dartmouth College ,* (), pp. [Online]. Available

at:*http://download.springer.com/static/pdf/870/chp%253A10.1007%252F978-0-387-09762-6_1.pdf?auth66=1425873806_69b868fe12b3ab2db2530726527cdaa7&ext=.pdf* (Accessed: 08/03/2015).

4. Crosby, P. B. (1979) *Quality is free: The art of making quality certain*, 2nd edition. McGraw-Hill New York.

5. ERIC RESCORLA (2005) 'Is Finding Security Holes a Good Idea? PUBLISHED BY THE IEEE COMPUTER SOCIETY', IEEE SECURITY & PRIVACY, 3(1), pp. 14-19 [Online]. Available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1392694 (Accessed: 15th October 2014).

6. Your Dictionary, Available at: http://www.yourdictionary.com (Accessed: 14th October 2014).

7. Quality Management Maturity Grid, Available at: http://c2.com/cgi/wiki?QualityManagementMaturityGrid (Accessed: 28th February 2015).

8. Business Impact Analysis, Available at:http://searchstorage.techtarget.com/definition/business-impact-analysis (Accessed: 28th February 2015).

9. Financial Service Authority, Available at: http://www.fsa.gov.uk/pages/Library/Communication/PR/2007/021.shtml

10. Jim D. Hietala (2008) 'Implementing the Critical Security Controls', *SANS Institute InfoSec Reading Room*, (), pp. [Online]. Available at: *http://www.sans.org/reading-room/whitepapers/analyst/implementing-critical-security-controls-35125* (Accessed: 10th March 2015).

11. Ma, Qingxiong, and J. Michael Pearson. "ISO 17799:" Best Practices" in Information Security Management?." *Communications of the Association for Information Systems* 15.1 (2005): 32.

12. Hasan Cavusoglu (2004) 'ECONOMICS OF IT SECURITY MANAGEMENT: FOUR IMPROVEMENTS TO CURRENT SECURITY PRACTICES', *Communications of the Association for Information Systems*, 14(), pp. 65-75 [Online]. Available at:*https://www.utdallas.edu/~huseyin/paper/practice.pdf* (Accessed: 9th March 2015).

13. Axelsson, S.,(2000) "The Base-Rate Falllacy and the Difficulty of Intrusion Detection," ACM Transactions on Information and Systems Security