A Budget Model for Information Security

M.T Dlamini[1,3,4], M.M. Eloff[2], J.H.P. Eloff[1,3,4] and H.S. Venter[1]

[1]Information and Computer Security Architectures Research Group
Department of Computer Science, University of Pretoria, South Africa
[2]School of Computing, UNISA, Pretoria, South Africa
[3]SAP Meraka UTD, CSIR, Pretoria, South Africa
[4]SAP Research CEC Pretoria
e-mail: {[1]eloff, [3]mdlamini, [4]hventer}@cs.up.ac.za; [2]eloffmm@unisa.ac.za

Abstract

This paper presents a model to assist in deriving a cost-effective and optimal information security budget. The derived budget focuses on an adequate mix of administrative, operational and environmental controls enabling organizations to comply with relevant regulatory mandates. The results seek to provide guidance on how decision makers can achieve optimal protection of their information assets in the face of shrinking information security budgets. A case study illustrates the implementation of the proposed model.

Keywords

Broad control categories, constraints, compliance, information security standards, information security spending

1. Introduction

An ad hoc selection of information security controls rarely contributes to a cost-effective and optimal information security investment. A cost-effective and optimal information security investment is more crucial given the global economic downturn, where organisations must strive for adequate information security at a reasonable cost (Schneier, 2007). Hence, today's organisations are required to strike the right balance between the need to secure their information assets and the need to minimise information security costs (Brink, 2008).

This paper proposes the Broad Control Category Cost Indicators (BC3I) model in a bid to determine a cost effective and optimal information security budget across different types of information security controls. The ultimate question to be considered is: How much should be invested in the different types of controls, for instance – should the focus be on administrative as opposed to environmental and operational controls, or on both?

The structure of this paper is as follows: Section 2 discusses related work. Section 3 develops and discusses the proposed BC3I model while Section 4 provides the case study. Section 5 outlines some of the limitations of the BC3I model and Section 6 concludes the paper and highlights future research.

2. Related Work

Most organisations are unable to give an indication of how much in total they really spend on information security. Even though extensive research has already been conducted to evaluate information security investments by using financial analysis tools (Wood & Parker, 2004; Sygate, 2007, Geer, 2002; Pappa, 2002) such as return on (security) investment (ROI/ROSI) and net present value (NPV); the results are still not satisfying and lack industry acceptance. Wood and Parker attribute the failure of the current financial analysis tools to the lack of reliable actuarial loss statistics and the intangible benefits and losses that are involved in quantifying information security investments (Wood & Parker, 2004). However, a major milestone in this field was achieved by the work of Gordon and Loeb (2002). Gordon and Loeb propose an economic model (which we call G&L) to determine the optimal level of information security investment. Their findings show that the optimal investment for protecting an information asset must at least be less than or equal to $1/e$ or 37% of the total loss expected of the information asset.

Tanaka, Matsuura and Sudoh (2005) conducted an extensive empirical study using the G&L model. This work investigates the relationship between information sharing and vulnerability levels and how it influences the decisions on information security investments. Liu, Tanaka & Matsuura (2007) also conducted an empirical study on the G&L model to verify the relationship between the effects of an information security investment and the vulnerability level.

Matsuura (2008) realized that the G&L model derive its economic benefit from the threat reduction. Matsuura concluded that this was not enough and then extended the G&L model to include a measure of productivity. Wang and Song (2008) provide the most relevant work in their proposed multi-objective optimisation model aiming towards an optimal information security investment strategy. However, their model does not state on what specific controls an information security investment should focus. Baryshnikov (2007) has refuted the convexity of the residual vulnerability function of the G&L arguing that it is not merely convex but it is log-convex. However, Barishnikov has confirmed that the $1/e$ rule of the G&L model holds for a very broad class of functions as long as the residual vulnerability function is log-convex (Barishnikov, 2007).

Willemson (2006) reviewed and refuted the G&L model's claim. Relaxing this model’s assumptions, Willemson provided a function that suggests an investment of up to 50% and even up to 100% of the expected loss. In a recent paper, Willemson (2010) further questions the 37% rule of the G&L arguing that the G&L model is missing a restriction on monotonicity of the remaining vulnerability as part of the original vulnerability level. Furthermore, Willemson presents a general class of functions that satisfies all the original restrictions of the G&L model (Willemson, 2010)

Reviewed literature has shown that there is a wide range of tools and models measuring information security investments. However, several main shortcomings still exist. Literature agrees that information security must be implemented on the strategic, tactical and operational levels (Eloff & Eloff, 2005); but it does not state exactly how the funds must be allocated on each level to achieve a cost-effective and optimal information security investment. In a bid to address the above, this paper adopts the work of Gordon and Loeb (2002). Knowing how much to invest in information security, the question that remains is where to focus such an investment for a cost-effective and optimal protection of information assets. The next section outlines broad control categories for information security spending.

2.1. Information Security Controls

The objective of the BC3I is to derive an information security budget that focuses on an adequate set of controls and, hence, a need arises to provide information security control categorization. Several categories are found in the available literature, for example in Purcel (2007), Killmeyer (2006) and the National Institute of Standards and Technology's (NIST) special publication 800-12 (1995). Based on the above and other categorisations, this paper proposes the following broad control categories:

- Administrative controls – controls that guide the user's actions in executing duties to meet business goals and objectives.
- Operational controls – implemented through software or hardware systems.
- Environmental controls – controls that provide physical protection to information and its infrastructure.

3. BC3I Model

This section begins by outlining the BC3I model requirements. This is followed by the variables, constraints and objective function to be considered in developing the BC3I model.

3.1. Requirements for the BC3I Model

Below are the requirements for the BC3I model:

- Cognisance of the business goals of an organisation.
- A holistic approach towards the implementation of information security.
- Be flexible to accommodate different information security standards.
- Cost effective to achieve a high level of security within a minimal budget.

3.2. Variables

The section discusses the components of the BC3I model; i.e. variables, constraints and objectives.

3.2.1. Broad Control Categories

Let x_{i_j} be an information security control. Furthermore: { $\forall x_{i_j} \mid x_{i_j}$ is an element of a standard or a customised control within the organisation}.

X_1: Broad control category consisting of administrative controls

Let x_{1_l} be an administrative control. Furthermore: Let $X_1 = \{x_{1_1}, x_{1_2}, \ldots, x_{1_l}\}$ e.g. $n(X_1) = 3$, $X_1 = \{$policy, standards, guidelines$\}$

X_2: Broad control category consisting of operational controls

Let x_{2_m} be an operational control. Furthermore: Let $X_2 = \{x_{2_1}, x_{2_2}, \ldots, x_{2_m}\}$ e.g. $n(X_2) = 3$, $X_2 = \{$firewall, anti-virus, authentication$\}$

X_3: Broad control category consisting of environmental controls

Let x_{3_n} be an environmental control. Furthermore: Let $X_3 = \{x_{3_1}, x_{3_2}, \ldots, x_{3_n}\}$ e.g. $n(X_3)=3$, $X_3=\{$surveillance cameras, buildings, security guards$\}$ and $\{\forall \ x_{i_j} \mid \exists \ (x_{i_j} \in X_1 \vee x_{i_j} \in X_2 \vee x_{i_j} \in X_3)\}$.

3.2.2. The Universal Set of Broad Control Categories

Let $\mathcal{U}$ be the universal set of all information security controls over all broad control categories. Furthermore: $\mathcal{U} = \{X_1, X_2, X_3\}$ and $X_1 \bigcap X_2 \bigcap X_3 = \phi$

3.2.3. Information Security Standards

Let s_k be an information security standard. Furthermore: $S=\{s_1, s_2, s_3, s_4, \ldots\ldots, s_k\}$

Where s_k consists of the following three subsets:

$X_1^{S_k}$ denotes broad administrative controls
$X_2^{S_k}$ denotes broad operational controls and
$X_3^{S_k}$ denotes broad environmental controls

And $\{\forall \ X_1^{S_k}, X_2^{S_k}, X_3^{S_k} \mid X_1^{S_k} \subset X_1 \wedge X_2^{S_k} \subset X_2 \wedge X_3^{S_k} \subset X_3\}$ e.g. $n(S) = 2$, $S=\{$ISO 27002, BASEL II$\}$

3.2.4. Organisational View of the Weights of Importance of Information Security Standards

Let $\omega_k^{S_k}$ be the weight of importance of standard s_k as decided upon by an organisation. Furthermore: $0 \le \omega_k^{S_k} \le 1 \ \forall k$.

3.2.5. Weights of Importance of Broad Control categories within each Standard

Let a_{ki} be the weight of importance within standard s_k of the broad control category subset $X_i^{S_k}$. Furthermore: $A_k=\{a_{k1}, a_{k2,} a_{k3}\}$ and $0 \leq a_{ki} \leq 1$ $\forall i,k$. Note: Weights of importance are determined by computing how much emphasis is placed on each broad control category by each standard s_k.

3.2.6. The Universal Set of Broad Control Category Costs

Let X_{ic} be the total cost associated with broad control category X_i. And x_{ijc} is the cost of control x_{ij}. Furthermore: $\mathcal{U}_c= \{X_{1c}, X_{2c}, X_{3c}\}$. The total cost for each broad control category is calculated as follows: $\overline{X_i^c} = \sum_{i=1}^{3} \sum_{j=1}^{l \vee n \vee m} x_{\text{ijc}}$

3.2.7. Cost Indicators

3.2.8. Let $\underline{X_i^c}$ be the cost indicator for the monetary amount to be spent on appropriate controls, as selected by an organisation from the broad control category set X_i. Furthermore: $\underline{X_i^c} < \overline{X_i^c}$ $\forall i \mid 1 \leq i \leq 3$

3.2.9. Budget

Let ***B*** be the monetary amount (budget) to be spent on the implementation of information security controls. Furthermore: $\overline{B}$ is the total budget, should all the controls within all broad control categories be implemented and is calculated as follows:

$$\overline{B} = \sum_{j=1}^{l} x_{1\,\text{jc}} + \sum_{j=1}^{m} x_{2\,\text{jc}} + \sum_{j=1}^{n} x_{3\,\text{jc}}$$

And $\underline{B}$ is the total budget for the selected controls, i.e. those controls viewed as applicable by an organisation.

3.2.10. Potential Loss

Let ***P*** be the total expected potential loss expressed as a monetary amount. However, the computation of ***P*** is outside the scope of this paper.

3.3. Constraints

The section discusses the constraints of the BC3I model i.e. budget constraints and non-negativity constraints.

3.3.1. Budget Constraints (B)

For the BC3I model the cost effectiveness of ***B*** is based on the G&L model, which stipulates that not more than 37% of the expected potential loss ***P*** should be spent on implementing controls (Gordon & Loeb, 2002). Therefore: ***B*** = (37/100) ***P***

3.3.2. Non-negativity Constraints

The model considers non-negativity constraints on a_{ki} ; $\omega_k^{S_k}$; $\underline{X_i^c}$; $\overline{X_i^c}$ such that $0 \leq a_{ki}$, $\omega_k^{S_k} \leq 1$ and $\underline{X_i^c}, \overline{X_i^c} \geq 0 \quad \forall k, i$. The next section describes the objectives of the BC3I model.

3.4. The Objective

In an ideal world, organisations would implement all the controls of all the three broad control categories. Thus: $\overline{X_1^c} + \overline{X_2^c} + \overline{X_3^c} = B$

Due to the cost and magnitude of controls available, this is an impractical scenario. Hence, organisations need to select only applicable controls. The objective of the BC3I model can thus be stated as follows: $\underline{\delta X_1^c} + \underline{\beta X_2^c} + \underline{\gamma X_3^c} \leq \underline{B}$ where:

δ, β and γ are the coefficient weights of importance of the broad control categories as viewed by an organisation. The results of the entire model rely on the coefficient weights of importance with regards to the sensitivity of the model. When you increase one of these, the results of the model will be greatly affected. This is illustrated in the case study in section 4.

3.5. Determining values for $\underline{X_1^c}$, $\underline{X_2^c}$ and $\underline{X_3^c}$

An information security budget (***B***) is dependent on $\omega_k^{S_k}$ and hence $\underline{B} \propto \omega_k^{S_k}$ **B** ($\underline{B}$ is directly proportional to **B**). For each standard s_k the unknown cost variable X_i^c is also dependent on a_{ki} and their relationship to the cost indicators $\underline{X_i^c}$ is: $\underline{X_i^c} \propto a_{ki} X_i^c$ ($\underline{X_i^c}$ is directly proportional to X_i^c)

The following is a generalised representation of the BC3I model:

$$\sum_{k=1}^{f} \sum_{i=1}^{3} a_{ki} X_i^c \leq \omega_k^{S_k} \boldsymbol{B}; \quad \forall i \,|\, 1 \leq i \leq 3 \text{ and } \forall f \,|\, 1 \leq k \leq f \tag{1}$$

where: *f* is the number of all the standards to be considered by an organisation.
A system of linear inequalities derived from (1) is as follows:

$$
\begin{aligned}
&a_{11} X_1^c + a_{12}\ X_2^c + a_{13}\ X_3^c \leq \omega_1^{S_1} \boldsymbol{B} \text{ for } s_1 \in \text{S} \\
&a_{21} X_1^c + a_{22}\ X_2^c + a_{23}\ X_3^c \leq \omega_2^{S_2} \boldsymbol{B} \text{ for } s_2 \in \text{S} \\
&a_{31} X_1^c + a_{32} X_2^c + a_{33} X_3^c \leq \omega_3^{S_3} \boldsymbol{B} \text{ for } s_3 \in \text{S} \\
&\quad .\ +\ .\ +\ . \qquad \leq . \\
&a_{k1} X_1^c + a_{k2} X_2^c + a_{k3} X_3^c \leq \omega_k^{S_k} \boldsymbol{B} \text{ for } s_k \in \text{S} \quad 0 \leq a_{ki} \leq 1 \quad \forall k, i .
\end{aligned}
\qquad \textbf{(2)}
$$

Taking any three (or more) standards, we can now rewrite (2)

$$
\text{as follows: } \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} \begin{bmatrix} X_1^c \\ X_2^c \\ X_3^c \end{bmatrix} \leq \begin{bmatrix} \omega_1^{S_1} B \\ \omega_2^{S_2} B \\ \omega_3^{S_3} B \end{bmatrix} \qquad \textbf{(3)}
$$

$$
\text{subject to: } X_i^c \geq 0 \text{ and } 0 \leq a_{ki} \leq 1\, \forall i, k
$$

4. Case Study

The illustration considers organisation O in the banking sector. Assuming that organisation O has chosen to implement two standards, namely ISO 27002 and PCIDSS, along with the custom-made controls specific to their business. The case study is implemented in the following five steps.

4.1. Step 1: Determine the Weights of Importance of the Broad Control Categories within Standards

The first step is to compute the weights of importance of each broad control category within each information security standard. The ISO 27002 (denoted s_1) standard consists of a total of 138 controls, of which 31% are in the X_1, 55% in the X_2 and 14% in the X_3 control category. The PCI DSS (denoted s_2) consists of 189 controls, of which 25% are in category X_1, 59% in X_2 and 15% in X_3. Organisation O has 120 custom-made controls that are specific to its business (denoted s_3), and that 35% in X_1, 30% in X_2 and 35% in X_3.

4.2. Step 2: Determine the Organisational View of the Weights of Importance of the Standards

The next step is to determine the weights of importance of each standard within the organisation. On a scale of zero to one, assume that based on their risk profile and previous information security investments organisation O weighs the standards s_1, s_2 and s_3 as follows: $\omega_1^{S_1} = 0.3$, $\omega_2^{S_2} = 0.4$ and $\omega_3^{S_3} = 0.3$ respectively.

4.3. Determine the Overall Security Budget

Assuming that organisation O identified an overall potential loss estimated to be $10 000 000. Using the G&L model, organisation O needs to spend at most 37% of this amount on its security budget. Therefore, the system of linear constraint inequalities becomes:

$$0.31\,X_1^c + 0.54\,X_2^c + 0.14\,X_3^c \leq \$1\ 110\ 000$$

$$0.25\,X_1^c + 0.59\,X_2^c + 0.15\,X_3^c \leq \$1\ 480\ 000$$

$$0.35\,X_1^c + 0.30\,X_2^c + 0.35\,X_3^c \leq \$1\ 110\ 000$$

4.4. Step 5: The Objective Function

After discovering that most breaches in their sector target business operations; on a scale of one to ten, organisation O weighs X_1, X_2 and X_3 as follows: $\delta = 2.3$, $\beta = 5.5$ and $\gamma = 2.2$ respectively. Then the overall objective function becomes:

$$2.3\,\underline{X}_1^{\,c} + 5.5\,\underline{X}_2^{\,c} + 2.2\,\underline{X}_3^{\,c} \leq 3\ 700\ 000$$

4.5. Discussion of the Results

The following are the results of applying the BC3I model.

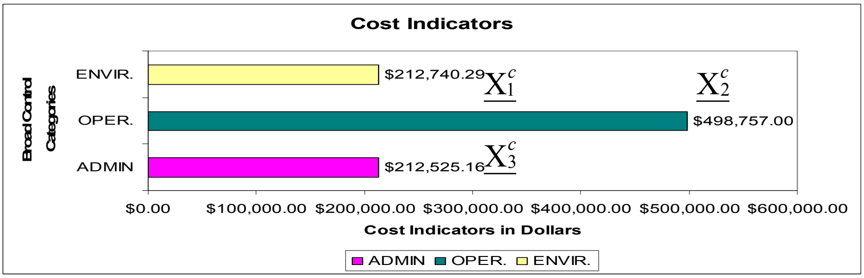

Figure 1: Cost indicators for each of the broad control categories

Figure 1 shows that the operational controls take the bigger share with $498 757.00, followed by administrative controls with $212 740.29 and environmental controls with $212 525.16. However, this is before taking into consideration the coefficient weights of importance for each broad control as viewed by the organisation. This illustrates the sensitivity of the model towards the coefficients' weights of importance. The latter is a critical factor, considering the fact that organisations (depending on their line of business and preferences) place different emphasis on different controls types.

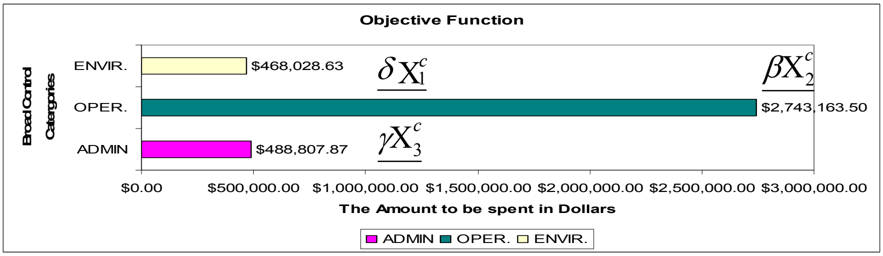

Figure 2: The proportional amounts to be spent on each of the broad control categories

After applying the weights of importance as viewed by the organisation, operational controls still take a bigger share of the budget at $2 743 163.50 This is now followed by administrative controls at $488 807.87 instead of environmental controls, which now come in last at $468 028.63. According to the results, organisation O puts more emphasis on operational than on administrative and environmental controls. This is to show that the weights of importance of the broad control categories as viewed by the organisation can contribute significantly when information security managers make decisions on the budgets of their organisations based on the BC3I model. The next section outlines some of the limitation of the BC3I model.

5. Limitation

The authors fully acknowledge the limitations of the BC3I model. Firstly, the BC3I model does not address the interdependences, interactions and sequence of and between the broad control categories. It considers broad control categories as independent variables, yet controls classified under one category could be argued to overlap to other categories. Secondly, the BC3I model uses results of the G&L model of an optimal information security investment, yet this is not necessarily an optimised information security budgeting strategy, but only a guide towards one. Thirdly, the model puts more emphasis on compliance mandates, yet "compliance" does not guarantee "security". Compliance is just a good starting point but not enough to achieve the illusion of perfect security. The last notable limitation is based on the subjectivity of selecting, categorising and weighting of the broad control categories. Further research could extend this research by addressing the identified limitations.

6. Conclusion

The BC3I model demonstrates how to arrive at a cost-effective and optimal information security budget across multiple standards and/or regulations. Acknowledging and taking full cognisance of its limitations, the BC3I model can be argued to have succeeded in answering the questions of how much to spend and where to spend it. It clearly reflects how and where specifically to focus information security budget. What remains is to implement the BC3I model in a real-world organisation, following the outlined steps. This could be part of the future work which includes addressing the identified limitations to extend this work.

7. Acknowledgments

The support of SAP Research Pretoria and SAP Meraka UTD (CSIR) towards this research is hereby acknowledged. Opinions expressed and conclusions arrived at are those of the authors and not necessarily to be attributed to the companies mentioned.

8. References

Anderson, R. and Moore, T. (2007), "The Economics of Information Security", *The Sixth Workshop on Economics of Information Security (WEIS 2007)*, Pittsburgh PA, 7-8 June 2007, www.cl.cam.ac.uk/~twm29/science-econ.pdf, (Accessed 27 November 2007).

Anderson, R. and Moore, T. (2007), "The Economics of Information Security: A Survey and Open Questions", *The Fourth Bi-annual Conference on the Economics of the Software and Internet Industries*. January 19-20, 2007: Toulouse, France.

Barishnikov, Y. (2007), "IT Security Investment and Gordon-loeb's 1/*e* rule", http://ect.bell-labs.com/who/ymb/ps/cyber.pdf, (Accessed 19 July 2010).

Brink, D. (2008), "Unified Threat Management: What's in, What's Next and Why?" *Aberdeen Group, A Hart-Hanks Company*, http://www.aberdeen.com/summary/report/benchmark/4872-RA-unified-threat-management.asp, (Accessed 10 November 2008).

Eloff, J.H.P. and Eloff, M.M. (2005), "Information Security Architecture", *Computer Fraud & Security Journal*, Vol. 2005, No. 11, pp. 10-16.

Geer, D. (2002), "Making Choices to Show ROI", *Secure Business Quarterly,* Vol. 1, No. 2, pp. 1-5.

Gordon, L.A. and Loeb, M.P. (2002), "The Economics of Information Security Investments", *ACM Transactions on Information and System Security*, Vol. 5, No. 4, November 2002, pp. 438-457.

Huang, C.D., Hu, Q. and Behara, R.S. (2006), "Economics of Information Security Investment in the Case of Simultaneous Attacks", *The Fifth Workshop on the Economics of Information Security (WEIS 2006),* 26-28 January 2006, Robinson College, University of Cambridge, England.

Killmeyer, J. (2006), "Information Security Architecture", Second Edition, Auerbach Publication Taylor & Francis Group, Florida, USA, ISBN: 0-8493-1549-2.

Liu, W., Tanaka, H. and Matsuura, K. (2007), "Empirical-Analysis Methodology for Information-Security Investment and Its Application to Reliable Survey of Japanese Firms", Regular Paper, *IPSJ Digital Courier*, Vol.3, pp. 585 – 599.

Matsuura, K. (2008), "Productivity Space of Information Security in an Extension of the Gordon-Loeb's Investment Model", *The Seventh Workshop on the Economics of Information Security,* 25-28 June 2008, Hanover, USA.

National Institute of Standards and Technology (NIST) (1995), "An Introduction to Computer Security: *The NIST Handbook Special Publication 800-12"*, http://csrc.nist.gov/publications/PubsSPs.html, (Accessed 27 November 2007).

Pappa, A. (2002), "Effective ROI – A Guide for Decision Makers", *Fujitsu August 2002 Whitepaper*, http://www.fujitsu.com/nz/whitepapers, (Accessed 27 November 2007).

Purcell, J. (2006), "Security Control Types and Operational Security", http://www.giac.org/resources/whitepaper/operations/207.php, (Accessed 29 November 2007).

Schneier, B. (2007), "Managed Security Monitoring: Network Security for the 21st Century", *BT Counterpane*, UK, http://bt.counterpane.com/msm.pdf, (Accessed 26 June 2008).

Sygate (2007), "Is Return on Security Investment Impossible? Until Now Open Networks defeat all ROI-based Security Investments", http://whitepapers.techrepublic.com.com, (Accessed 27 November 2007).

Tanaka, H., Matsuura, K. and Sudoh, O. (2005), "Vulnerability and Information Security Investment: An Empirical Analysis of e-local Government in Japan", *Journal of Accounting and Public Policy*, Elsevier, Vol. 2005, No.24, pp. 37 -59.

Tsiakis, T. and Stephanides, G. (2005), "The Economic Approach of Information Security", *Computers & Security Journal*, Vol. 24, No. 2, pp. 105-108.

Wang, Z. and Song, H. (2008), "Towards an Optimal Information Security Investment Strategy", *The Proceedings of the IEEE International Conference on Networking, Sensing and Control*, Vol. 2008, 6-8 April 2008, pp. 756-761.

Willemson, J. (2006), "On the Gordon and Loeb Model for Information Security Investment", *The Fifth Workshop on the Economics of Information Security* (WEIS 2006), University of Cambridge, UK, (2006), http://www.ut.ee/~jan/publ/economics.ps, (Accessed 27 November 2007).

Willemson, J. (2010), "Extending the Gordon and Loeb Model for Information Security Investment," *International Conference on Availability, Reliability and Security* (ARES 2010), pp. 258-261.

Wood, C.C. and Parker, D.B. (2004), "Why ROI and Similar Financial Tools are not Advisable for Evaluating the Merits of Security Projects", *Computer Fraud & Security Journal*, Vol. 2004, No. 5, pp. 8-10.