# An Analysis of Information Security ROI models

Ganapathi Subramaniam Balasubramanian
University of Salford, UK – bgansub@yahoo.com

## Abstract

*Justifying the expenditure on information security has always been a challenge for security practitioners. Whilst a number of models have been developed in the academia, they not percolated through the industry practitioners. This paper presents a synopsis of the major Security ROI models and analyses them from a practitioner's point of view. Furthermore, the author lists out the attributes of an ideal ROI model from a practitioner's perspective, highlighting the need for a joint academic-industry approach.*

## 1. Introduction

'We are condemned to choose', wrote Jean-Paul Sartre. To choose, however, one needs rationale. Perfect knowledge of information is rare, so our reasons for exercising a certain choice involve faith.

Unshrink – Max Mckeown & Philip Whiteley

*In the context of information security investments, the word 'faith' in the above quote could have been replaced with 'fear, uncertainty and doubt'. It is well-known fact that traditionally 'fear, uncertainty and doubt' ('FUD') determined the level of security investments. In the absence of perfect knowledge of information relating to potential threats, likelihood and the vulnerabilities, the question is how do practitioners make decisions on information security investments?*

Whilst a number of useful and interesting models have been developed in academia on information security return on investments ('ROI'), industry practitioners, in the author's opinion, are oblivious of them.

Every commercial conference on information security definitely has at least one session of practitioners discussing Security ROI. The author has not come across any commercial conference speaker discussing the Security models developed by the academic world and a gap definitely exists between industry and the academic world.

This paper aims to analyse, from a practitioner's point of view, the models developed in academia and to indicate what a practitioners dream Information Security ROI model would consist of.

## 2. Information Security Investments – Key Questions

The key question is whether information security expenditure constitutes an investment or is a mere overhead. What constitutes an investment? Phil Holmes [1] defines investment as 'any act which involves the sacrifice of an immediate and certain level of consumption in exchange for the expectation of an increase in future consumption'. In the context of information security, we could conveniently interpret the 'expectation of an increase in future consumption' as equivalent to a reduction in potential annual expected losses.

Security Managers often complain about lack of adequate allocation of resources and hence substantial outlay towards security is completely out of the question. The quantum of such expenditure is not substantial and hence irreversibility is not an issue.

Even some leading security practitioners do not believe information security to be an investment. Leading practitioners like Jay Heiser[2] decry the very concept of Security ROI. 'Nobody tries to quantify the ROI of air-

conditioning. So, why try with Security?' he asks. He further states that 'Security is overhead, just like automatic fire sprinklers and air-conditioning in the server room. Face it: it is necessary evil''.

It is true that not all practitioners may share or subscribe to Jay Heiser's view.

Whether Security is an investment or not, the poor practitioners face a battle every year during the budgeting process to justify resources – both money and people. Whilst September 11 has changed the perception of security in the mindset of the corporate directors and senior management, the battle for expenditure justification by the Security Manager has not just vanished. Security Managers often tend to use or are recommended to use the data/information published in the various annual information security surveys as supporting evidence justifying the expenditure.

Auditing firms like PriceWaterhouse Coopers and Ersnt &Young and bodies like Computer Security Institute publish surveys on an annual basis, dishing out information such as the average annual loss due to security incidents is X000 dollars or so. These surveys are very popular in the industry and both the security product / services vendors and the buyers try to make the best use of the survey information to their advantage.

Again, not many of these surveys render appropriate and useful information. Kevin Soo Hoo [3] could not get realistic results from his security ROI model due to inadequate data. Again, according to Jay Heiser, "the creators, respondents and the recipients of the study have not-so-hidden agenda" and such surveys lack 'statistical and scholarly rigor' [4]. Jay Heiser [4] further quotes one of the surveying body Computer Security Institute's Editorial Director Richard Powers' views that the numbers are potentially misleading and the number of respondents wasn't what the CSI would have liked and further complains about the misuse of survey's data. Jay Heiser[4] states that 'it is the ability to misuse the survey results that makes it so popular'.

There is a definite need for credible and meaningful survey data and I believe that such credible information can only be produced by the academic world with both statistical rigor and no vested interest from any of the commercial entities.

Does information security investment lead to any additional revenue or earnings? Different models developed in the academic world recognise that security investments lead to possible incremental revenue and have built in variables to account for such revenue in their models. Again, not many practitioners share this view. To quote Jay Heiser [2] again, ''Firewalls don't increase network bandwidth. VPNs don't increase throughput. Changing passwords every 60 days does not make users more efficient".

BS7799 or the British standard on Information Security became the de-facto information security standard in the UK. A number of companies, including banks and financial institutions, achieved compliance and got certified as BS7799 compliant. The Co-Op Bank UK, one of the first Internet banking firms in the UK, was a pioneer in achieving BS7799 certification. Recently, the Royal Bank of Scotland appears to have achieved the certification. However neither the Co-op Bank nor the Royal Bank of Scotland appear to advertise their BS7799 compliance to promote their secure online banking.

Whilst there have been studies [5] to identify the potential negative impact on the market value of the firms due to any security related incidents, the author is not aware of any study that has identified specific incremental benefits derived by the firms due to increased security investments.

Another key question facing the practitioners today is how much should they invest in information security? What is the optimal level of investment worries practitioners whilst determining their annual budgets. It is common knowledge that the law of marginal returns tends to operate in the information security arena as well as any other, and any investment more than an optimal investment is bound to render negative returns.

Whilst the author is aware of some of the useful research undertaken by academia on this issue such as the GLEIS™ [6] model development, he is not so sure as to whether the corporate world has been bought into such studies.

However, companies do spend on information security to meet some legal and regulatory requirements. For example, the Financial Services Authority ('FSA') in the UK has recently devised regulations that require companies to achieve BS7799 compliance, although not necessarily certification. So, willingly or unwillingly, companies are forced to spend on information security, to meet regulatory requirements.

## 3. Models developed in Academia

A number of models have been developed by academics to help measure Security ROI or to determine the optimal level of security investments.

The models are illustrated and analysed as follows from a practitioner point of view.

### 3.1 Huseyin Cavusoglu model

Huseyin Cavusoglu [7] advocates the game theory approach to determine the optimal level of information security investments. Huseyin views the companies that try to protect their assets against unauthorised access and the hackers who are determined to break the security as two different players of a typical game. Their respective payoffs and utilities, if any, are taken into account to determine the value of the game. Huseyin also takes into account the utility derivable by the hacker if he/she were to hack. The model is effective when there are both preventive and detective controls in place and the payoffs of both the company and the hacker are definable.

This model appears to have a number of limitations.

• One of the key assumptions of Game Theory is the players adopt a very 'rationale' approach. Avinash Dixit and Susan Skeath [8] explain rational behaviour as follows: "Much of the game theory assumes that players are perfect calculators and flawless followers of their best strategies. This is the assumption of rational behaviour. Thus rationality has two essential ingredients: complete knowledge of one's own interest, and flawless calculation of what actions will best serve those interests."

The problem is hackers are not always rational and do not necessarily or have to adopt a flawless approach. In 2000, there was a major denial of service attack on popular sites such as Yahoo, Amazon etc. Regular customers of those websites were not able to conduct normal business and this was caused, allegedly, by a 15 year old Canadian juvenile. Whilst not all hackers are teenage troublemakers, a number of hackers belong to that age group, who undertake hacking "seeking the thrill of publicity" [9]. Many of these hackers, due to their flawed approach and miscalculations, leave trails of their entry in hacked websites, exposing them to the law of the land.

• Huseyin considers only two players in the game – the hacker and the company being hacked. In the author's opinion, there are more than two players in a typical situation. Cathy Cronkhite & Jack McCullough [9] illustrate a hacking incident where "the British banking giant, HSBC, experienced the defacement of four of its websites. The hacker, alias Herbless, did this to protest the fuel prices in the United Kingdom. His defacement included an activist statement and guidelines for other Hacktivists."

For example, if an hacker were to hack into Company X's website running Microsoft's Windows Operating System, the interest of Microsoft would also be at stake. Microsoft would also incur a penalty, but such penalties are ignored in Huseyin's model, even if they were calculable.

• Whilst discussing a framework for Cyber-insurance, Gordon [10] illustrates a situation where insurance companies charge extra premiums for the use of specific software and also occasions where they offer a discount in premium for the use of certain other products. Relating the above example to the insurance issue would mean that other companies using Microsoft's Operating System would also incur a penalty and the insurance companies would stand to gain because of further increases in premiums due to new vulnerabilities being identified in Microsoft's Windows. Thus, there are more than two players and payoffs exist for them, which the model does not appear to take into account.

• Huseyin's model views security purely from a hacking perspective, thereby taking a fractional approach of security's definition. Information security is more than an access control or confidentiality issue and encompasses integrity, non-repudiation and availability of information. The international standard ISO/IEC 17799 [11] defines information security as follows:

'Information Security is characterized here as the preservation of:

a. Confidentiality: ensuring that information is accessible only to those authorised to have access;

b. Integrity: safeguarding the accuracy and completeness of information and processing methods;

c. Availability: ensuring that authorised users have access to information and associated assets when required.

• If the systems were to become non-available due to possible natural causes such as fire, flood or electricity where the player 'nature' has nil payoffs, the current model developed by Huseyin may not be very effective.

### 3.2 Gordon and Leob model

Gordon and Leob [6] have developed a model to determine the optimal level of an IT Security investment. According to them, the optimal level of investment in information security is only a small fraction of the expected loss associated with a firm's risk exposure. Their model, now known as the GLEIS™ model, predicts that the greatest payoffs for

investments in information security occur where the probability of a security breach is in the intermediate zone (i.e., where the probability of a security breach is not very close to zero or one).

Kanta Matsuura [12] feels that Gordon and Leob's model fails to incorporate information security insurance in it and identifies the following limitations:

*'The loss is treated as a constant. This suggests that the investment studied in the model is restricted to hardware/software technologies and management services of information security. The investment variable in the model is continuous and hence the investment subjects are treated not as discrete pieces but as a whole'.*

Gordon's approach, in the author's opinion, has further limitations.

There is no discounting done over the lifetime of the investment.

The model adopts a binary approach towards security breach – in other words, it assumes situations where there is a breach or no breach. The possibility of multiple breaches is not taken into account, nor is partial loss. The model also ignores the time factor, because it is basically a single period analysis. For high loss and low breach probability, according to the model, the investment would be zero, rendering the investment implausible.

### 3.3 Kevin Soo Hoo Model

Kevin Soo Hoo [3] adopts a decision theory approach to decide the optimal level of IT Security investment.

Huseyin Cavusoglu [7] explains Kevin Soo Hoo's model and critically reviews it.

'*Hoo provides a decision analytic framework to evaluate different policies for IT Security. He develops a risk modelling technique for selection of safeguards, which utilise influence diagrams as a common graphical language that maps relationships between key variables. Instead of comparing all security controls on an individual basis, his model groups controls into baskets of safeguards, or policies. Then he makes a cost-benefit trade-off for each policy.*

*His model considers not only the cost of security controls and expected loss from security breaches but also additional profits expected from new opportunities associated with security investment when making cost and benefit calculations.*

*Though intuitive, decision analysis approach for evaluating IT Security investment treats security technology as a black box. This technique does not provide managers any insights into how the different variables of an IT Security infrastructure affect the risk, expected loss and the likelihood. For example, it cannot answer questions such as how does the firewall affect the likelihood of a security breach or the expected loss, or what is the trade-off between preventive, such as a firewall, and detective, such as an Intrusion Detection System. They also ignore the strategic nature of the security management problem'.*

It is true that security investments result not only in cost savings, but also could possibly generate additional revenue and both cost savings and revenue generated are incorporated in Kevin's model. For example, customers may join a particular bank, if they perceive that it offers secure online banking. However, it may not be feasible to attribute or assign a percentage of any organisation's profit as those generated because of security controls.

In addition, since in Kevin's model a group of controls are aggregated together, the relative weight of individual controls does not get captured and is lost.

## 4. A Practitioner's dream model

The following are, in the author's opinion, as a practitioner, the attributes of an ideal model.

• The model should help Security Managers to undertake a meaningful risk assessment within any organisation and thereby enable the calculation of a realistic Annual Loss Expectancy value.

• The model should incorporate metrics relating to the specific security controls; by selecting the appropriate controls, Security Managers should be able to compute the relative reduction of any potential loss. Extrapolating this attribute further, it should be theoretically possible to evaluate the merits of two or more complementary security products, in terms of their returns. Because the model has actuarial type of information on security losses, the computation would be objective and not on a subjective basis.

• The model should incorporate both the time value of money and the discount rate. Steven E. Phelan [13] views that each idiosyncratic investment technically requires its own discount rate. He further argues that the "ability to misestimate risk-adjusted rates of return and the reluctance of Managers to alter hurdle rates clearly qualifies the treatment of risk for novel projects as a hard investment evaluation problem".

• The model should provide ways and means of identifying the specific gains derived by the implementation of security controls such as additional revenue, similar to those used by companies to identify revenue generated by say, a special advertisement campaign.

• Similar to the 'value at risk' concept of the banking industry, the model should be able to take into account the new threats and vulnerabilities that get identified on an ongoing basis, as well as the changing value of the information itself, thereby enabling the Security Manager to either increase the investment by deploying additional resources or decrease it by possible redeployment.

## 5. Conclusion

Whilst a number of useful and interesting models, albeit with a few limitations, have been developed by academia, in the author's opinion, they are yet to percolate through to the industry practitioners.

Combined efforts between industry practitioners and academia can alone make the development of an ideal, practical and pragmatic model feasible and thereby ensure that FUD factors do not any more determine investments on information security.

## References


1 Phil Holmes: *Investment Appraisal*, 1999

2 Jay Heiser, "Security Through ROSI-colored Glasses", *Information Security*, July 2002

3 Kevin J. Soo Hoo, "How much is enough? A risk management approach to computer security", *Working paper*, CRISP, Stanford University, June 2000

4 Jay Heiser, "Go Figure: Can we trust infosecurity surveys?" *Information Security*, April 2002

5 Cavusolglu, H., Mishra, B., and S.Raghunathan, "The Effect of Internet Security Breach Announcements on Shareholder Wealth: Capital Market reactions for breached firms and Internet Security Developers," Working Paper, UT-Dallas, 2002.

6 Gordon, L and Loeb, M. "The Economics of Information Security Investment", *ACM Transactions of Information and Systems Security*, November 2002.

7 Huseyin Cavusoglu, "The Economics of Information Technology Security", *PhD Dissertation*, University of Texas at Dallas, August 2003.

8 Avinash Dixit and Susan Skeath, "*Games of Strategy*", W.W. Norton & Company, Inc. 1999

9 Cathy Cronkhite & Jack McCullough, "*Access Denied*", Osborne/McGraw-Hill, 2001.

10 Gordon, L, Loeb. M. and Tashfeen Sohail, "A Framework for Using Insurance for Cyber-Risk Management" , Communications of the ACM, March 2003.

11 ISO/IEC 17799, "information Technology – Code of Practice for information security management", British Standards Institute, UK

12 Kanta Matsuura, "Information Security and Economics in Computer Networks: An Interdisciplinary Survey and a Proposal of Integrated Optimization and Investment", Working Paper, University of Tokyo.

13 Steven E. Phelan, "Exposing the illusion of confidence in financial analysis", *Management Decision*, 35/2, 1997