INFORMATION SECURITY – RETURN ON INVESTMENTS – AN ANALYSIS

Ganapathi Subramaniam Balasubramanian  
Director, Information Security, Flipkart Internet Pvt. Limited, India  
Email: bgansub@gmail.com

ABSTRACT

Justifying the expenditure on information security has always been a challenge for security practitioners. The few models developed in the academia have not percolated through the industry practitioners. Whether Security is an investment or not Practitioners face a battle every year during the budgeting process to justify resources – both money and people. Whilst increased regulations and breaches have changed the perception of security in the minds of the corporate directors and senior management, the battle for expenditure justification by the Security Manager has not vanished. This paper aims to discuss some of the models conceptualized in various academic research works.

Keywords: Information Security Investments; Security ROI

INTRODUCTION

Security Investments – Issues and Concerns

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 an equivalent to an anticipated reduction in potential annual expected losses.

Security Managers often complain about lack of adequate funding approvals or allocation of funding or resources; obtaining approval for making substantial investments towards security continues to remain a challenge for Practitioners.

Even some leading security practitioners do not believe information security to be an investment. Leading practitioners like Jay Heiser[2] challenge 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.

Security Managers often tend to use or are often forced to use the data/information published in the various annual information security surveys as supporting evidence justifying the expenditure.

Again, not many of these annual security survey reports 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] states that ‘it is the ability to misuse the survey results that makes it so popular’.
Do investments in Information Security lead to any additional revenue or earnings for any Company? Different models developed in the academic world allude that security investments have possible incremental revenue as outcomes of such investments 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”.

When BS7799 or the British standard on Information Security became the de-facto information security standard in the UK in the late1990s, 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. Later, many other banks appear to have achieved the certification. However neither the Co-op Bank nor the other banks appear to advertise their compliance certification to promote their secure online banking.

There have been studies [5] to identify the potential negative impact on the market value of the firms due to any security related incidents.

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

Some of the useful research undertaken by academia on optimal investment for information security such as the GLEIST™ [6] model development might not have percolated into the corporate world.

Most of the traditional / conventional methods used for measuring return on Investments may or may not be applicable to Information Security investments.

Amongst the following traditional methods of generic investments appraisal, the Discounted Cash Flow or the Net Present Value method is the most commonly used method by the industry.

- Payback Method
- Net Present Value or Discounted Cash flow method; and
- Accounting Rate of Return method.

The Accounting Rate of return method considers the average profit generated by the investment and expresses it as a percentage of the initial investment made over the lifetime of the project.

\[
ARR = \frac{\text{Average Annual Profit}}{\text{Average Investment}} \times 100\%
\]

The fundamental flaw of this method is that it takes into account the ‘accounting profit’ and not the actual ‘cash flow’ for calculation purposes.

Payback method considers the length of the time it takes for the returns (net cash flows) to equal the sum of the initial investments made. It is expressed in terms of number of years or a set time period in years. The basic flaw of Payback Method is that the cash flows beyond the payback period is completely ignored and is not taken into account for calculation of returns.

On the other hand, Net Present Value (‘NPV’) or the discounted cash flow method takes into account the various cash flows generated by the project over a period of time. The NPV or the net present value of such future cash flows is calculated using an appropriate discount rate. Net Present Value (‘NPV’) method also takes into account the time value of money.
The NPV method is also not free from its flaws and the weaknesses have been highlighted [7] as follows:

“First, the ‘operating flexibility’ available within a single project which enables management to make or revise decisions at a future time (such as, for example, options to defer, expand or abandon the project); and second, the ‘strategic’ option value of a project resulting from its interdependence with future and follow-up investments”.

The key factor that distinguishes information security investments from other investments is that it is made to prevent an occurrence of a potential loss and not with an aim to generate any additional profit, though in some cases, additional revenue is generated and some models take such revenue into account. It is again not easy to decide the rate at which the future cash flows or reduction in losses can be discounted and analysed. In addition, many of the benefits accrued are neither tangible nor quantifiable.

Certain organisations use tools like Balanced Scorecard for measuring and monitoring performance.

Balanced Scorecard is a performance measurement and management tool introduced in the nineties. Whilst the traditional performance measures were purely from the finance perspective only, Balanced Scorecard advocated [8] the use of measures from four perspectives, including finance as follows:

- “Finance – To succeed financially how should we appear to our shareholders.
- Customer – To achieve our vision, how should we appear to our Customers?
- Internal Business Process – To satisfy our shareholders and customers, what business processes must we excel at?
- Learning and Growth – To achieve our vision, how will we sustain our ability to improve and change”.

A number of alternative models [9] such as Maisel’s Balanced-Scorecard, the Performance Pyramid model, Effective Progress and Performance Measurement model are available; they resemble the original Balanced Scorecard approach and such models have been extensively reviewed.

It is pertinent to note that unless implemented properly, balanced scorecards fail to produce necessary results. Some of the key reasons for a failure include [10] “the independent or non-financial variables on the scorecard are incorrectly identified as primary drivers of future stakeholder satisfaction” and the inappropriate definition of metrics.

However, companies make investments 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 implement security controls. In India, the Reserve Bank of India has come up with security guidelines for banks. So, willingly or unwillingly, companies are forced to spend on information security, to meet regulatory requirements.

**OBJECTIVES OF THE PAPER:**

The objectives of the paper are as follows:

1. To Discuss the need to compute the return on Information Security investments;
2. To outline the challenges behind computing the return on Information Security investments faced by Security Practitioners;
3. To analyse the merits and possible improvements for certain sample models developed by the academia.
REVIEW OF VARIOUS SECURITY EFFECTIVENESS MEASUREMENT MODELS

Huseyin Cavusoglu Model- Huseyin Cavusoglu [11] 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.

For the Companies’ point of view, the payoffs result from one or more of the following:

- Losses from undetected intrusions;
- Losses from detected intrusions; and
- Cost of monitoring

From a hacker’s point of view, the payoffs include the expected utility that he / she derives from the attack and the expected cost payable, if the hacker were ever to be caught.

Payoffs and utilities for both the hackers and the hacked Companies are taken into account to determine the value of the game. Huseyin Cavusoglu model is useful and effective only when there are both preventive and detective controls in place and the payoffs of both the company and the hacker are identifiable in simple terms.

This model appears to have a few shortcomings, such as the following:

- One of the key assumptions of Game Theory is the players adopt a very ‘rationale’ approach. Avinash Dixit and Susan Skeath [12] 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.”

- Whilst not all hackers are teenage troublemakers, a number of hackers belong to that age group, who undertake hacking “seeking the thrill of publicity” [13]. Many of these hackers get exposed to the Law Enforcement if they were to adopt a flawed approach.

- Huseyin appears to consider only two key players in the game – the hacker and the company getting hacked. In the author’s opinion, there are more than two players in a typical situation. Cathy Cronkhite & Jack McCullough [13] 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 a hacker were to hack into Company X’s website running ABC’s Operating System, the interest of ABC would also be at stake. ABC would also incur a penalty, but such penalties appear to have been ignored in Huseyin’s model, assuming that they are calculable to some extent.

- Whilst discussing a framework for Cyber-insurance, Gordon [14] illustrates a situation where insurance companies charge extra premiums for the use of specific software which can be deemed vulnerable; there are also occasions where they offer a discount in premium payable for the use of certain other products, deemed more secure. Relating the above example to the insurance issue would mean that other companies using a commercial 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 the commercial operating system used regularly. Thus, we can see the existence of more than two players and payoffs exist for all of them, which the model does not appear to take into account.
Huseyin’s model appears to 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 [15] defines information security as follows:

“Information Security is characterized here as the preservation of:

- Confidentiality: ensuring that information is accessible only to those authorised to have access;
- Integrity: safeguarding the accuracy and completeness of information and processing methods;
- 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 have limitations.

**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, that 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 [16] feels that Gordon and Leob’s model does not appear 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. It appears that there is no discounting done over the lifetime of the security investment made.

Gorden and Leob’s model has adopted a binary approach towards security breach – in other words, it assumes situations where either there is an occurrence of breach or there is no breach. The possibility of multiple breaches has not been taken into account and equally occurrence of partial loss has not been considered too. The model does not consider any time factor, because the model is basically a single period analysis only and not otherwise. For high loss and low breach probability events, according to the model, the investment will be zero, thereby making the investment meaningless.

**Kevin Soo Hoo Model** - Kevin Soo Hoo [3] adopts a decision theory approach to identify / determine the optimal level of IT Security investment. He collects and collates various security controls and translates them into a set of security policies; he suggests a cost-benefit analysis for each of the security controls to be implemented. According to Kevin, the benefits derived from the investments are the difference between the Annual Loss Expectancy (ALE) Value before and after the implementation of controls. The key variation is that he takes into account potential / possible gains generated due to specific security controls implementation as a variable in his model.

In order to compute ALE and make it more pragmatic and real, his model takes into account the reduction of frequency of incidents as an outcome of implementation of security controls. In addition, his model also takes into account marginal reduction in probable loss due to the occurrence of possible security incidents or security breaches.
The biggest advantage of the model is that it is simple to follow and easy to understand. However, the model has its own limitations.

Huseyin Cavusoglu [11] critically reviews Kevin Soo Hoo’s model as follows:

‘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’.

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

In addition, since in Kevin’s model the group of controls are aggregated together, the relative weight of individual controls gets lost and does not get captured adequately and appropriately.

Roger Adkins Model- Unlike the other models developed in the academia, which are based on measuring the benefits as an outcome of investments made, Roger Adkins adopts an insurance based approach.

His model aims to identify the maximum loss as a potential outcome of security incidents for a particular time period or horizon. Many conventional models treat the rate at which the expected future cash flows are discounted as a ‘constant’ value; however, Roger Adkin’s model treats it as a variable within the model design.

Using Real Options based approach and Probability Theory, Roger’s model treats the losses which occur as an outcome of security breaches to be random following a distribution pattern with known expected losses, compared to some other models which always treat loss as a known constant.

However, Roger’s model is based on ‘rationality’ approach, which is in total contradiction with Prospect Theory. Prospect Theory “purports that organisations adopt a risk loving stance in the presence of losses though preferring uncertain higher losses than a certain lower losses”[17].

CONCLUSION

There are multiple approaches to security investments and many models continue to emerge. Each of them has its own merits and limitations.

The challenge to the Security Practitioners is which model is ideal to use.

REFERENCES


9. ISO/IEC 17799, “information Technology – Code of Practice for information security management”, British Standards Institute, UK


11. Jay Heiser, “Go Figure: Can we trust info security surveys?” Information Security, April 2002


15. Phil Holmes: Investment Appraisal, 1999
