The Use of Real Option Analysis (ROA) to assist in Security Solution Decisions

Razib Hayat Khan

Department of Telematics, Norwegian University of Science & Technology (NTNU)

Summery
Security management, security risk management and security service evaluation involve deciding on a security strategy and an appropriate set of security solutions to align with the strategy. However, as there are limited budget, time and resources available to identify, select, employ, monitor, review and maintain the set of security solutions, multiple perspectives must be taken into consideration in the decision making process. One important factor for constructing effective security solution decision is to make the decision dynamic. The nature of security risk changes day by day. As time passes old risks may go away and new risks may arise. So it is necessary to make the security decision in such a way that it can keep pace with the frequently changing security risks. The security solution decision must be satisfied with the demand of changing circumstances due to changing in time and changing in technologies so that decision maker can maintain an acceptable risk level and demolish the undesirable effect of uncertainty by providing improved risk assessment and management activities. Real Option Analysis (ROA) can be seen as a promising alternative to offer effective and dynamic security solution decision making process. It offers possibilities to improve decision making in security solution decision. This paper investigates how ROA could be used to assist in security solution decisions by integrating ROA with Security Decision Making Process (SDMP) which facilitates any organization to achieve better business continuity plan. Later the framework is tested through a simulation example. Real option thinking has been applied to several software designs and engineering concepts, such as eXtreme Programming (XP), COTS-based development, project investment analysis, decision making in software prototyping and strategic software reuse. Comparing with the software engineering issues, planning a security solution decision through ROA includes more uncertainties.

Key words:
Real option, Real option analysis, Security solution decision, Uncertainty

1. Introduction

Nowadays organizations require practical security benchmarking tools in order to apply effective security strategies. Before spending money on a product or a service, decision maker needs to be sure that the investment is financially justified. Security is no different -- it has to make business sense. What decision-makers need are security metrics that show how security expenditures impact the underneath line. There's no rationalization in implementing a solution in the organization if its true cost is greater than the risk exposure as the organizations mostly are loss-profit responsible. According to the 2005 CSI/FBI Computer Crime and Security Survey, many industries have introduced economic metrics to validate the security department expenditures by expressing them in terms of Return on Security Investment (ROSI), Net Present Value (NPV) and Internal Return on Investment (IRR) [1]. The limitation of traditional approaches, such as ROSI, NPV and IRR is that they assume investment is an all-or-nothing strategy that means there is no intermediate result between loss and profit. In an environment of rapid change and prevalent uncertainty traditional methods fail to accurately capture the economic value of investments. They do not account for managerial flexibility where security manager can alter the course of an investment decision over time when certain aspects of the security uncertainty becomes known. But the culture of flexibility options is vital for creating active decision in uncertain arena like security decisions. When new risks become visible it is important for the security mangers of the organization to be able to alter the security decision and strategy.

Real options are applicable precisely where change is most evident. Real option analysis facilitates managerial flexibility to alter the investment decisions in response to unexpected situation when new security uncertainty becomes known. It allows the organizations to customize their security solution decisions to reflect the risk aspect in the company context. Real option analysis extends beyond the valuation tasks to guide not only what strategy is chosen but also when and how the strategy gets implemented in order to maximize the likelihood of desirable outcomes. However, real option analysis is the most promising alternatives for the organization for modeling uncertainty. It recognizes the value of flexibility and the additional value associated with real options in the context of uncertainty. With the growing acceptance of real option analysis as a modern approach to investment analysis, several information researchers have tried to apply ROA to IT security investment decision making. We believe that real options will become an increasingly important tool in security analysis. So the main focus of

Manuscript received October 5, 2011
Manuscript revised October 20, 2011

this paper is to investigate how ROA could be used to assist in security solution decisions by integrating ROA with Security Decision Making Process (SDMP) into a framework.

Table 1: Related works & improvements over those

Related work	Presented criteria of related work	Improvement provided by our proposed framework
Framework presented by Johansen Bräutigan & Christoph Esche [5]	▪ Time efficient process of real option valuation ▪ Covers organizational, strategic & controlling aspect necessary to apply real option valuation	▪ Sorting of real options for a particular case ▪ Providing extensive list of uncertainties present in security solution decision
OBRiM framework done by Michel Benaroach, Yossi Lichtenstein & Karl Robinson [4]	▪ Risk-Option mapping approach for choosing a particular real option to control specific risk	▪ Considering option interaction case to reduce adverse effect of uncertainty in a more complex situation
Real option thinking to IT security in networked organization by Maya Deneva [2]	▪ Identification of several real IT options	▪ Providing a guideline about the use of real option to assist in security solution decision
Making economic security solution decision through real option thinking by Jingyue Li & Xiaomeng Su [3]	▪ Tailoring real option analysis technique to provide actual valuation of options to make security decision	▪ Identification of real option ▪ Identification of uncertainties ▪ Sorting of real options for a particular case

The main contribution of this framework is to identify available real options exist in the organization premise to model the uncertainty. Then the optimal one will be chosen among the available identified real options and to integrate the optimal one in the security decision making process to provide the flexibility in the organization to reduce the undesirable effect of uncertainty for achieving improved business continuity plan smoothly through conducting detail risk assessment and management process. In addition we also try to provide some improvements over the existing related research work through our proposed real option based framework. The paper is organized as follows: section 2 introduces our proposed framework, section 3 demonstrates the simulation example to show the applicability of our proposed framework and section 4 delineates the conclusions remarks.

2. Related work

A list of several criteria of existing related works that can be utilized through our proposed framework is presented in Table 1. We also mention several improvements provided by our proposed framework over existing related work.

3. ROA & it's relation with IT security

The term "Real Options" can be traced to Myers (1977), who first identified investments in real assets as mere options [6]. "A real option allows generating different value at different time periods to undertake some business decision, typically an option to make a capital investment". [6] For example, "an opportunity to invest in the expansion of a firm's factory is a real option. In contrast to financial options a real option is not tradable - e.g. the factory owner cannot sell the right to extend his factory to another party, only he can make this decision" [6].

"The terminology "real option" is relatively new, whereas business operators have been making capital investment decisions for centuries". [6] Real option analysis is mainly introduced as a method that supports decision support for capital investments. It facilitates managerial flexibility to alter decisions in response to unexpected situation. "Companies create shareholder value by identifying, managing and exercising real options associated with their investment portfolio. The real options method applies financial options theory to quantify the value of management flexibility in a world of uncertainty". [7] It allows the decision makers to illustrate and to correspond to the strategic value of an investment project when used as conceptual tool. In an environment of quick change and ubiquitous uncertainty traditional methods (e.g. net present value) fail to accurately express the economic value of investments.

Information technology (IT) security investment helps the organization to achieve success in their regular business activities. It is always difficult to measure the effectiveness of security solution decision in financial value. One important factor here is to validate the security expenditure through appropriate cost-benefit analysis technique to measure the effectiveness of security solution decision. But risk and uncertainty presents in the security investment decision and security solution decision avoid any organization to validate the security expenditure through proper cost-benefit analysis technique. That means a useful cost benefit analysis technique is required to

reduce the undesirable effect of security risks and uncertainty to successfully validate the security expenditures. Nowadays there are several methods used by the organization to validate the security expenditure for instance net present value (NPV), return of security investment (ROSI), internal rate of return (IRR). But their problem is the inability to demolish the undesirable effect of uncertainty when validating the security expenditure and their failure to think about the changes of security investment decision over time by taking the advantage of several real options like abandon, postpone, defer or stage etc [8]. Real option analysis (ROA) approach overcomes several of these shortcomings when integrating with security decision making process. The main advantage of real option analysis technique is to take the advantage of several real options present in the organization premise. Thus it helps any organization to alter the investment decision over time when new uncertainty becomes known. As ROA considers the changing circumstances due to changing in time it does not produce any paradoxical result. ROA combining with NPV produces a tremendous result while investing in IT security solution decision as ROA incorporates option thinking in security investment decision and security solution decision. In addition ROA breaks the concept of all-or-nothing strategy, thus allows to defer, to postpone or to wait for investing in an innovative project when market condition becomes more favorable [9].

4. Proposed Real Option based security solution decision framework

When integrating real option analysis with security decision making process, calculate the value of real option through mathematical model is not the last word. Moreover incorporating real option thinking with security decision is not a stand alone process. To conduct the option incorporating security decision successfully it is necessary to find out available real option for modeling uncertainty. Here uncertainty is key value driver as organization put effort to model uncertainty through the best suited real IT option specific for an uncertainty to reduce its effect. Though real option analysis controls the uncertainty by exercising optimal real option it does not give any direction when, why and how uncertainty inherent in the organization. But to get the best output it is necessary to answer all the questions regarding uncertainties inherent in the organizational context. Bearing the above concepts we present our proposed framework in figure 1 where segments in the framework are organized in such a sequential way that conduct the overall security decision making process by giving the answer of the all the questions mentioned above. Our proposed framework consists of six segments:

1. Organizational environment valuation
2. Uncertainty modeling aspect
3. Option tailoring
4. Option valuation
5. Option exercising security decision
6. Post implementation

In our description, at first we will underline the relationship among different segments activities in a sequential way in the context of risk assessment, management and business continuity. Then detail descriptions of all segments will be given by highlighting how the activities of different segments will be achieved. One important aspect of our proposed framework is that all segments activities are glued by security solution decisions. That means the combined target of all the segment activities is to help an organization to construct a better security solution decision in the context of organizational need and according to organization's business continuity plan. The detail descriptions of the segments are presented below:

Segment1: Organizational Environment Valuation

"Since much of the value of the real-options approach comes form strategy" [5], it is essential to properly define the organizational business strategy and security policy for better understanding the organization's need. Business strategy helps the organization planned for and responds to business disruption to achieve better business continuity plan. Security policy helps the organization to put restriction when accessing organization's asset so that any external systems and unwanted intruders and hackers can not interrupt the normal business activities. The first segment mainly deals with the above information and identifies the asset in the organization on which uncertainties inherent. This identification is not limited to the present surroundings of the organization rather attempts must be made to ensure the future need.

For achieving the task of this segment, standard processes like AS/NZ 4360:2004 [10], CORAS [11] and CRAMM [12] can be used as references. Sub process 1 which is "Establish the context" for both AS/NZ 4360:2004 and CORAS has direct influence in this segment's activities. Establishing the context helps to define the boundary of the system based on which risk assessment will be conducted. This also helps to identify the most valuable critical assets of the organization on which risks inherent. Some parameters must be chosen to conduct the risk assessment successfully so that no risk is excluded from the risk assessment process. This process also takes care about the resources required to conduct the risk assessment activities. Another important factor for achieving this segments activity is to form an active management team. Because all the activities achieved through our proposed

framework will be completed with the help of active management team. The management team should be formed by hiring experts from entire departments to produce the best outcome. If the people are taken from the entire departments they can share their view regarding security investment decision and security solution decision, thus helps to achieve a concrete decision with the combination of several opinions.

Segment 2: Uncertainty modeling aspect

The segment "uncertainty modeling aspect" extensively influences the overall activities of our proposed framework as uncertainty is the main reason for integrating real option thinking with security solution decision.

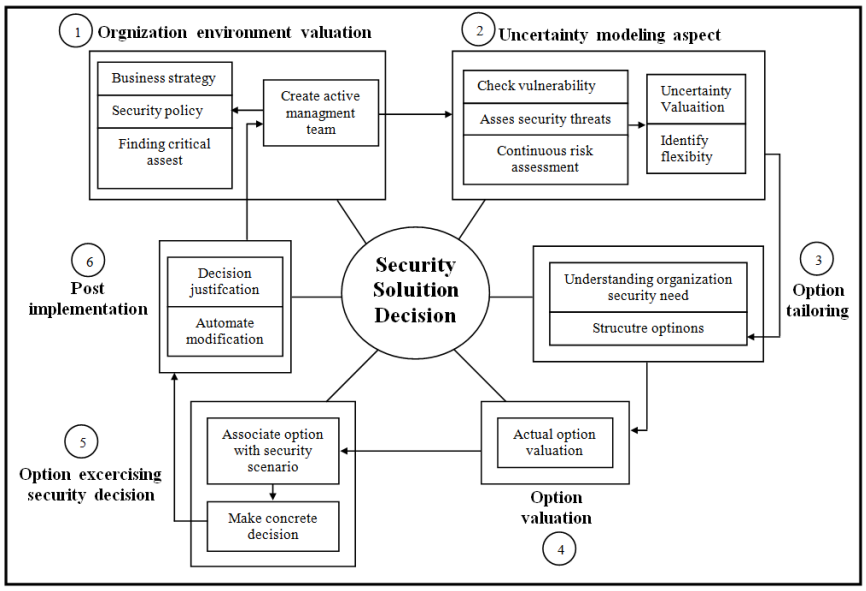

Fig. 1 Proposed Real Option based security solution decision framework

Table 2: List of Uncertainty

Uncertainty	Description
Uncertainty concerning time	Any investment decision is influenced by time. Investment on security is no different – it has relation with time & payoff.
Uncertainty concerning complexity	"A recent survey deemed this uncertainty most threatening in the context of information technology investments". [17] As we are dealing with security investment decision in context of IT threats this uncertainty has greater impact on the organization's overall business activities. Dynamic nature of security threats makes the situation complex and out of control if the security decision is not up to date and not effective
Cost uncertainty	Security manger of the organization always thinks about the cost of security solution against the expected benefit in reduction of security risks [13]. To make efficient security decision a detail list of security threats will be generated based on the severe effect on the organization's asset. According to this list, security manager takes security solution decision. Manager has to consider several aspects when making security decision including several costs like infrastructure development cost, employment cost, maintenance cost of security decisions, incident cost, cost in loss of sensitive and confidential data, cost in productivity loss. So it is indispensable to know the financial justification of investment before making the investment decision by considering the above cost.
Uncertainty about quality	Quality of the product when making security solution decision has greater impact over organization's business continuity plan. For example IDS operation is constrained by two quality factors including probability of false alarm and probability of detection. Choosing IDS for any organization the security manager must judge the two quality factors. Otherwise the organization will not get much benefit in filtering malicious background traffic. Moreover, if quality of the security product is not ensured properly the organization will face problem in achieving the future return from the security service investment.
Unknown uncertainty	A final class of uncertainties will be explained here as well. "Unknown uncertainties may be presented in almost any investment". [5] In fact, they are one of the primary causes of project failure.

However, a careful analysis of the organizational uncertainty as well as continuous assessment of the security risk is required for the appropriate valuation of real options that exist across the organization premise. Sub process 2 which is "risk identification" of both AS/NZS 4360:2004 [10] and CORAS [11] process give a better direction of how activities of this segment will be achieved. Another important task of this segment is to identify uncertainty regarding security decision and security investment decision in the organization. Uncertainty presents in the security investment may produce asymmetric payoff for the organization. There may present several uncertainties in this regard shown in Table 2[5].

The final task of this stage is to find out the options available for incorporating into the organizational security solution decision process to remove the uncertainty. The options are the following: **Postpone** - Waiting to determine whether to invest in a security mechanism, without imperiling the potential benefits. **Abandon** - Keeping security project resources relatively easily redeployed, if the project needs to be cancelled. **Scope up** - Increasing amount of security mechanisms if uncertainties are resolved favorably. **Scope down** - Cutting back on security mechanisms if uncertainties are resolved unfavorably. **Outsource** - Deciding on managed security services if the service gap is manageable and security costs are reduced. **Switch** - Keeping open to choose alternative security technologies and managed security service providers. **Stage** - Rolling out a security solution incrementally, slowly expanding to user populations. **Growth** - Taking advantage of future, interrelated opportunities due to achieved compliancy with SOX (Sarbanes-Oxley) or ISO [2].
Based on the above categories of uncertainty and option to resolve the uncertainty, the proposed framework helps the organization to produce an uncertainty-option matrix shown in Table 3 [5] [4]. **"√"** Sign indicates the particular option used to resolve particular uncertainty

Segment 3: Option tailoring

The main task of this segment is to arrange the real option for particular decision making process and for particular business need through a state model (figure 2) and revising the option integration process over time to simplify the option interaction process for resolving effect of uncertainty. This model mainly represents what particular options are available to make a decision for a particular case. As this framework is dealing with option incorporating security solution decision process here real options are modeled and sorted to facilitate the security decision making process.

In the previous segment we develop a generalized list of real options to reduce the adverse effect of uncertainty. But not all the real options mentioned in the previous segment are important when making security investment decision and security solution decision. Through our proposed state model (presented in figure 2) we present only those real options that are useful and valuable for making security investment and security solution decision. According to our proposed state model suppose Company AB is going to start new e-business and wants to make security solution decision. When making security solution decision Company AB has four options at first time step for instance handling security service by the company itself, outsourcing the security solution service to a MSSP by properly defining their requirements, choosing stage option while outsourcing if they have shortage in fund or wait and see approach. In the next time step our proposed state model helps the company AB to revise the security solution decision. If company AB chooses outsourcing their security solution in previous time step they can renew the contract with specific need in the next time step or can manage the security service by the company's own IT department. Again if the company AB chooses stage option while outsourcing they can select the scope up or scope up security service option based on the organization need in the next time step. Furthermore the company AB can mange the security service by themselves after certain period of time by learning from experience. This way company AB can revise the integration of usable and valuable real option through our proposed state model.

Segment 4: Actual Valuation of options

In the previous segment all the available options are arranged and sorted according to the organization particular business need for facilitating the security solution decision making process. In this segment we will choose the most promising real options from the above sorted options using preferred mathematical model to make effective security solution decision by considering the cost, benefit and payoff of security solution services. Before giving the detail description about the option valuation it is necessary to know the category of option. There are mainly three types of options based on the time to exercise the options. According to [14] these include: **European option -** An option that may only be exercised on expiration (expiration is the date on which the contract expires). **American option -** An option that may be exercised on any trading day on or before expiration. **Bermudan option -** An option that may be exercised only on specified dates on or before expiration.

Table 3: Option – Uncertainty matrix

	Postpone	Abandon	Scope Up	Scope down	Outsource	Switch	stage
Time	√	√			√		√
Complexity	√	√	√		√		
Cost	√	√		√	√	√	√
Quality		√	√	√	√	√	
Unknown							

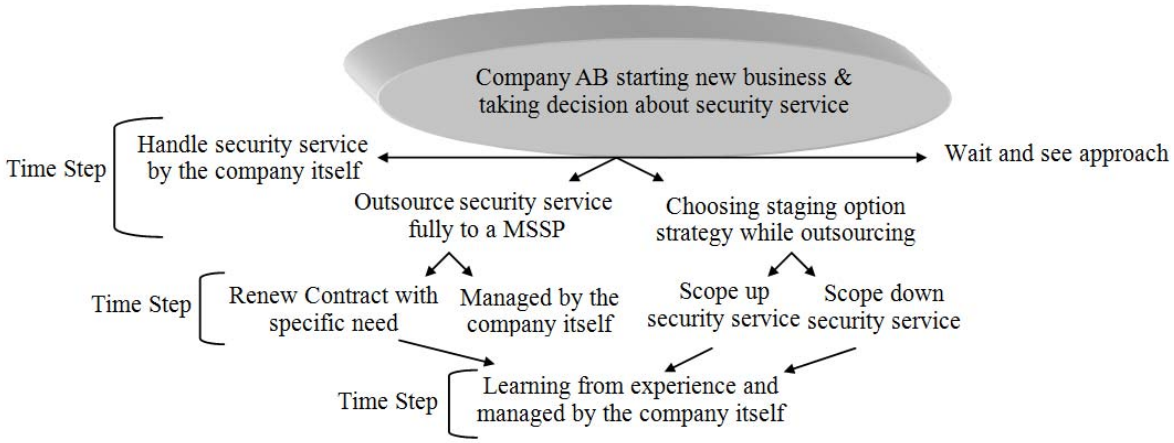

Fig. 2 Option tailoring State Model

There exist several methods that can be used to conduct real options valuation. Among them the Black-Scholes model [16] and the Cox, Ross and Rubinstein Binomial option pricing model [15] are the primary pricing models. According to [15] the Binomial option pricing model is an iterative solution that models the price evolution over the whole option validity period. The binomial model breaks down the time to expiration into potentially a very large number of time intervals, or steps between valuation date and option expiration. A tree of total prices of solution is initially developed working forward from the present to expiration date of real option. At each step it is assumed that the total price will move up or down by an amount calculated using volatility and time to expiration. This produces a binomial distribution, or recombining tree, of underlying total prices. The tree represents all the possible paths that the total price could take during the life of the option. The above features of valuing the options over time rather than in a particular time period makes this model suitable for using in the security decision making process. As nature of security risk and threats are changing day by day security decision must be consistent with this changing consequence. It is difficult to implement a security solution decision well in advance and security managers are disinclined to invest in protecting a security breach before it happens. It is not prudent to make a static security investment decision for a particular time period rather than to update the decision over time according to the nature of the security breach and organizational need. So we prefer to use Binomial option pricing model for our framework which give the opportunity to the valuation of real option particularly for long period of time to justify the optimal utilization of security investment.

The big advantage of the binomial model has over the Black-Scholes model is that it can be used to accurately price American options that allows the exercising of real option at any time during the option life [15]. This is because with the binomial model it's possible to check at every point in an option's life (i.e. at every step of the binomial tree) for the possibility of early exercise. Where an early exercise point is found it is assumed that the option holder has a chance to exercise the option if the condition remains favorable, and the option price can then be modified and adjusted.

Segment 5: Option exercising security decision

The outcome of the previous section plays an important role in this segment which gives the justification of merging real options thinking with different business scenarios for better utilization of security investment and for better management of security solution decision. Based on the viability of valuation of real options, the security managers merge real options with security solution decision making process to take the advantage of opportunity in changing consequences of security scenarios.

Segment 6: Post implementation

The post implementation segment mainly deals with and responsible for the following activities: Continuous investigation and regular update of option merged security solution decision, Automate modification with iterative process if needed and Provide continuous feedback to active management team for better understanding of the whole framework's activities

5. Application Example

In this section an application example is formulated to test our proposed real option based security solution decision framework to provide improved security solution decision. The simulation example also helps to demonstrate the activities of each segment of our proposed framework in an organizational context.

Suppose Company X is going to start a new e-business. The main target of company X is to conduct their business on the internet in a controlled and secured way to ensure confidentiality, integrity and availability when accessing to information by the business partners, customers and suppliers. Company X will conduct their business on the Internet for buying and selling products as well as serving customers and joining with other business partners. In addition Company X uses the Internet to buy different products and parts from other companies and business organization, to cooperate with each other for achieving better business activities. Moreover, Company X has to extensively use information and communication technologies to combine together their business processes and systems internally as well as to ensure different departments to work together to provide better products and faster and efficient services. To achieve success Company X has to protect their critical business activities from hackers, discontented employees, criminals and attackers. As Company X's business is connected to the internet, it's their responsibility to protect business data and information against unwanted intruders. If the protection mechanism is not properly implemented sensitive and important information such as customer details, pricing information, and personal records can all be hacked, disseminated, altered or even destroyed. Company X has to ensure that their connection to the internet must be secured when conducting their business online. To make their business secure Company X has to consider following issues: conducting business on the Internet in a secure way, virus and malware protection, firewalls, back up system, ensuring secure password and passphrase & intrusion detection system.

Now the company X will take decision about their security solution to achieve the most economical and efficient security services for their company to make their business secure. They have to make the decision to be consistent with their fixed security budget. As their budget is fixed and limited they can take the preventive measures according to the priority of security risks those have the most adverse effects on organization's asset. In addition they need to choose a mechanism for making the investment decision dynamically that allows the organization X to make any midcourse strategic corrections and to provide flexibility to alter the investment decisions when new risks become available or any uncertainty will be involved in future.

Now we will conduct and demonstrate our application example according to different segments of our proposed framework.

First segment mainly defines the several organizational aspect of X like defining the business continuity strategy, security policy and defining the assets which drives overall security solution decision of company X. This information will help to achieve second segment activities on which further risk and uncertainty assessment will be done. Detail description is given in framework's explanation section on how all the activities of this segment will be completed.

The second segment has a greater impact on the upcoming segments activities to give them a proper shape. After completing the task of the second segment company X can make a detail list of security threats inherent in organization's assets. Based on this list company X can choose security solution service to reduce the adverse effect of security threats. This segment also helps company X to figure out several uncertainties inherent in security investment decision and to make list of possible real options to demolish the effect of uncertainties to achieve better business continuity plan. Uncertainty-Option matrix may be generated for better understanding the relationship between uncertainty and option.

In the option tailoring segment organization X will try to identify and sort the particular real options for their particular business need. They will organize and sort all

the real options to be consistent with their security services. Based on this they will create a model for sorting real options like one shown in figure 2 which is nothing but a tree to graphically represent all the real options presents when making security solution decision for better decision making process. Organization X can choose two alternatives here:

- They can make the security solution decision by their own
- As they are new in this arena they can outsource the security service to a MSSP by defining their requirements if it is cost efficient for X. In this case they may chose the option of scale down or scale up security services after a certain period of time based on their security need and available budget. That means they may apply different real options at different time periods.

The previous two segment's findings play an important role here. For example: company X may choose to outsource the security service if it is financially feasible. It needs to clarify all the security requirements to MSSP so that MSSP can make a concrete security decision for company X. If company X completes the previous segment activities successfully then it will be easier for them to highlight all detail requirements to MSSP regarding their security services.

In this stage organization X contact to a MSSP for outsourcing their security service. The MSSP provides two alternatives:

1. MSSP demands $100 thousand to organization X for providing 6 security services for 5 years without giving any flexibility
2. MSSP demands $5 thousand to organization X for providing 6 security services for 5 years. In this alternative the organization X will get the flexibility to scope down or scope up security services by the half of the total security services during the contract period.

As organization X is not certain about the future security threats they may need more security services by giving extra money or they can discard some security services in future and may save some money. But to choose alternative 2 organization X has to pay more $25 thousand. Now it is time to find out the most effective and cost efficient security solution decision from the above two alternatives for the organization X. As the alternative 2 gives the organization right but not obligation to achieve some goal this is a real option for the organization. Organization X can treat the alternative 2 as a scope up or scope down option. Organization X can get the chance to apply the real option at any time during the life of the real option. So according to the definition it is an American option. Suppose here volatility (σ) 50%, risk free interest rate (r) 5%, dividend (q) 0%, 5 years contract and 5 steps for calculating the value of option (See Appendix for more information).

At first we evaluate the value of security solution when exercising scope down option and take the optimal decision based on the calculated value. The total price for the current security solution services for alternative 1 is $75 thousand and for alternative 2 is $50 thousand calculated through the traditional NPV (For the sake of NPV calculation we assume that the organization achieve cash flow of $40 thousand for each year from the security solution service).

We generate the Binomial price tree working forward from valuation date to expiration shown in figure 3. As alternative 2 is used as a real option for the organization X we start with $50 thousands (total price of the alternative 2) as value of the starting node of the price tree. At each step the price will be up or down by a factor *u* and *d* (Value of *u* and *d* is 1.687 and 0.6065; calculated from equation 1 & 2 in Appendix; where time step (t) = 1). At time step 1, value 82.435 and 30.325 is generated from multiplying 50 by 1.6487 and 0.6065. This way prices of others time steps will be generated.

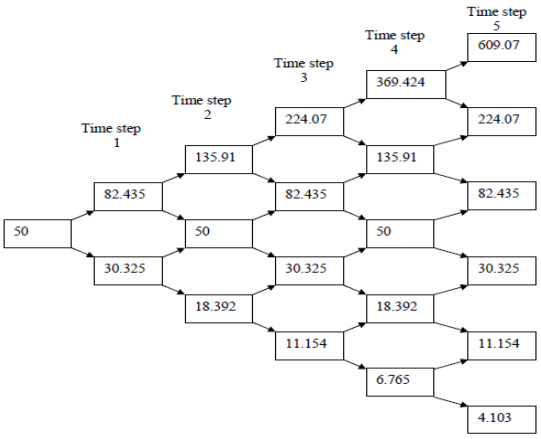

Fig. 3 Binomial price tree for alternatives 1 & 2

Then we evaluate the value of security solution service when exercising scope down option (shown in figure 4). This is a progressive calculation at each earlier node starting from the terminal node and ending at the fist node of the tree (the valuation date). At each node the organization will take the value which gives the most benefit. For example: If scope down (reducing security services by half) option is exercised at terminal node 1 (figure 4) the value of the security solution service will be equivalent to: 0.5 X $609.07 + $62.5 = $367.035 thousand (as the result is equivalent to half of its existing operation

plus saving of $62.5 thousand). As the option exercising value is less than $609.07 (which is spot price of the underlying asset) the organization X will take maximum profit generating value $609.07 thousand for the terminal node 1.

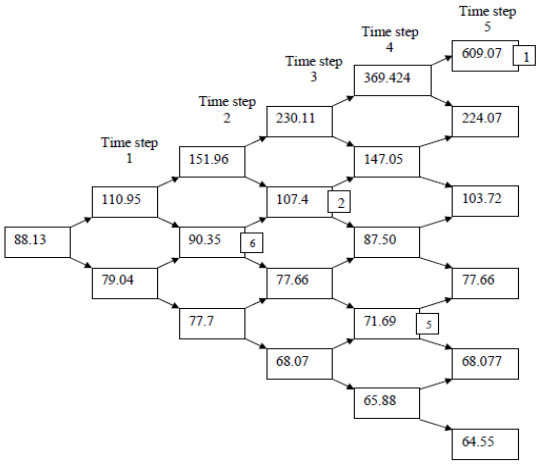

Fig. 4 Calculated value of option at different time steps for alternative 1

For each of the intermediate node, Option exercising security solution value and Binomial value will be calculated and the maximum value between these two values will be taken as value of the following intermediate node. This value generates the maximum profit for the organization. Binomial value for each intermediate node is calculated from equation 3 (Shown in Appendix):

$$\text{Binomial Value} = [p \times \text{Option up} + (1\text{-}p) \times \text{Option down}] \times \exp(-r \times t)$$

For example: Binomial value for node 2 is (in figure 4) is: $[0.4267 \text{ X } \$147.05 + 0.5733 \text{ X } \$87.5] \text{ X } e^{-0.05 \text{ X } 1} = \$107.4$ thousand (where probability p = 0.4267; calculated from equation 4 in Appendix) and if the scope down option is exercised at node 2, the value of security solution at node 2 will be: 0.5 X $82.435 + $62.5 = $103.72 thousand (as the result is equivalent to half of its existing operation plus saving of $62.5 thousand). As the option exercising value is less than Binomial value, the organization X will take maximum profit generating value $107.4 thousand for the intermediate node 2.

From the figure 4 it is shown that the value of the first node is $88.13 thousand which is the value of the security solution when exercising scope down security services option. The value is more than the value $75 thousand which is the total price for security solution without any flexibility for alternative 1. So it will be profitable for organization X to choose security solution decision with scope down option.

Now we evaluate the value of the security solution when exercising scope up option and take optimal decision based on this calculated value. Here we use the same Binomial price tree as the previous one (shown in figure 3) as values of the variables for conducting the calculation are same for both cases. After generating the price tree we will evaluate the value of security solution with exercising the real option starting form terminal node and working back to the first node of the tree (the valuation date). For example: If scope up option (increasing security services by half) is exercised at terminal node 3 (in figure 5) the value of the security solution service will be: 1.5 X $609.07 - $62.5 = $851.11 thousand (as the result is equivalent to one and half of its existing operation and more $62.5 thousand cost). As the option exercising value is greater than $609.07 (which is the spot price of the underlying asset) the organization X will take maximum profit generating value $851.11 thousand for the terminal node 3.

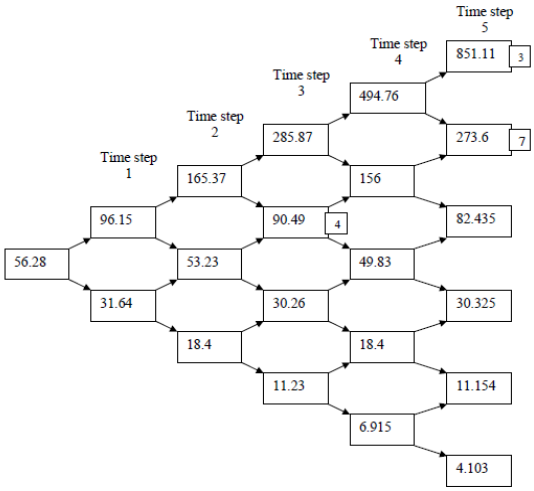

Fig. 5 Calculated value of option at different time steps for alternative 2

For each of the intermediate node, Option exercising value and Binomial value is calculated from equation 3 (in Appendix) and the maximum value between these two values is taken as value of the following node. This value generates the maximum profit for the organization X. For example: Binomial value for node 4 (in figure 5) is: $[0.4267 \text{ X } \$156 + 0.5733 \text{ X } \$49.83] \text{ X } e^{-0.05 \text{ X } 1} = \$90.49$ (where probability p = 0.4267; calculated from equation 4 in Appendix) thousand and if the scope down option is exercised at node 4, the value of the security solution at node 4 will be: 1.5 X $82.435 - $62.5 = $61.15 thousand (as the result is equivalent to one and half of its existing operation and more $62.5 thousand cost). As the option exercising value is less than Binomial value, the organization X will take maximum profit generating value $90.49 thousand for the intermediate node 4. From the

figure 5 it is shown that the value of the first node is $56.28 thousand which is the value of the security solution with scope up security service. The value is less than the value $75 thousand which is the total price for security solution without any flexibility for alternative 1. So it will be profitable for organization X to continue security solution decision without scope up security service.

Based on outcome of the previous segment Organization X will make the real option incorporating security decision. That means now organization X can choose the security decision which would be the cost effective and gives the most benefit. The manager of organization X can make any midcourse strategic changes of the security solution decision. For example in figure 4 the binomial value of node 5 is $68.65 thousand and value of the security solution after exercising real option for corresponding node is $71.69 thousand. According the decision rule (defined in Appendix) if organization X exercises the option of scope down the security services it will give the maximum profit. Again in figure 4 the binomial value of node 6 is $90.35 thousand and value of the security solution after exercising real option for the same node is $90.35. So according to the decision rule (defined in Appendix) if organization X continues the existing security services rather than exercising scope down option it will generate maximum profit for the organization X. Moreover in figure 5 value of security solution with exercising scope up option in terminal node 7 is $273.6 thousand which is greater than value $224.07 thousand. So it is wise to scope up the security service for maximizing the profit.

Real option analysis gives the direction about how to calculate the value of the security solution with exercising real option. In addition this technique ensures the optimal exercise of real options in perfect time but it doesn't provide any guideline about when and why new risk becomes visible and exposed. So it is necessary to conduct incessant investigation by company X for getting the best result from option incorporating security solution services.

5. Conclusion

In the following paper we mainly integrate a new technique Real Option Analysis (ROA) with security solution decision to make the decision efficient, cost effective and dynamic. To make the integration successful, we generate an extensive real option based security solution decision framework. Moreover the effectiveness of the proposed framework is shown by using simulation based experiment. The simulation based experiment also helps us to establish the superiority of ROA by reducing the limitations of other traditional methods like NPV, IRR and ROSI. To develop the framework, we try to identify some criteria through literature study (presented in table 1). The identified criteria for developing the framework characterize our main contribution by identifying uncertainty when making security decision, by identifying real options, by developing an uncertainty-option matrix and by sorting the real options for particular business cases for reducing the uncertainties. The above mentioned activities are achieved by the first three segments of our proposed framework. The presented uncertainty-option matrix helps to make the option interaction process simpler. The remaining three segments of our proposed framework provide a guideline for customizing real option analysis technique to apply in security solution decision. Risk assessment and management activities play an important role when making security solution decision by providing improved business continuity plan. So several risk assessment and management standards are also investigated while setting up criteria for our proposed framework. The identified criteria also helps us to provide some improvements over the existing related work. Moreover to test the framework activities towards the identified criteria we draw a simulation based example. The test material for the simulation was taken from the existing related research. Simulation example for supporting and validating the proposed framework activities provides a suitable way and guidelines of how security managers will take the profit maximizing security investment decision while optimally utilizing their fixed budget. Simulation example is presented in a way that each segment's activity is demonstrated as a part of the whole evaluation process in the organizational context. The overall target is to achieve a dynamic and up-to-date security solution decision and security investment decision which is the result of the combined approach of all the segments activities of our proposed framework. The simulation example also demonstrates an effective way to simplify the options interaction process in a complex case when making security solution decision.

References

[1] L. A. Gordon, M. P. Loeb, W. Lucyshyn, and R. Rochardson, "2005 CSI/FBI computer crime and security survey", Technical Report, Computer Security Institute, 2005.

[2] Maya Daneva, "Applying Real Options Thinking to Information Security in Networked Organizations" Technical Report, University of Twente, ISSN 1381-3625, 2006

[3] Jingyue Li, Xiaomeng Xu, "Making Cost Effective Security Decision with Real Option Thinking", International Conference on Software Engineering Advances (ICSEA 2007), 25-31 Aug. 2007, Page(s):14 – 22.

[4] Benaroch, Lichtenstein, Robinson, "Real options in IT risk management: an empirical validation of risk-options relationship", Forthcoming in MIS quarterly, 2006
[5] Johannes Bräutigam, Christoph Esche, Anett Mehler-Bicher, "Uncertainty as a key value driver of real options", Seventh annual real option conference, July 10-, 2003, USA
[6] http://en.wikipedia.org/wiki/Real_options_analysis, retrieved January 2008
[7] Real-Options.org, "Real options in theory and practice", http://www.real-options.org/, retrieved January-2008
[8] Paul P. Tallon, Robert J. Kauffman, Henry C. Lucas, Andrew B. Whinston, Kevin Zhu, "Using Real Options Analysis for evaluating uncertain investments in information technology: insights from the ICIS 2001 debate", Communications of the Association for Information Systems (Volume 9, 2002).
[9] Kambil, A., C. J. Henderson and H. Mohsenzadeh (1993) "Strategic Management of Information Technology Investments", in Banker, R., R. J. Kauffman and M. A. Mahmood (eds.) Harrisburg, PA: Idea Group Publishing,
[10] Australian/New Zealand Standards, AS/NZS 4360:2004 Risk Management, 2004
[11] K. Stølen, F. den Braber, T. Dimitrakos, R. Fredriksen, B. Gran, S. Houmb, Y. Stamatiou, and J. Aagedal., The CORAS Approach to Identify Security Risks, pages 189.207. Kluwer, 2002
[12] B. Barber and J. Davey., "The Use of the CCTA Risk Analysis and Management Methodology CRAMM in Health Information Systems", Proceedings of MEDINFO'92, pages 1589-1593. North Holland Publishing, 1992.
[13] Gordon, Lawrence A. (ED), "Information Security Expenditures and Real Options: A Wait-and-See Approach" Computer Security Journal, Vol. 19, Nr. 2, pp. 1-20, 2003
[14] http://en.wikipedia.org/wiki/Option_finance, retrieved February 2008
[15] Victor Podlozhnyuk, "Binomial Option Pricing Model", http://developer.download.nvidia.com/compute/cuda/sdk/website/projects/binomialOptions/doc/binomialOptions.pdf, April 2007, retrieved 2008
[16] Option Pricing Models and the "Greeks", http://www.hoadley.net/options/bs.htm", retrieved January 2008
[17] Jiang, J. J. and Klein, G. (2001), Software project risks and development focus. Project Management Journal, 32(1)

Appendix: Binomial Option Pricing Model

Option valuation using this method is, as described, a three step process: (1) price tree generation (2) calculation of option value at each final node (3) Progressive calculation of option value at each earlier node; the value at the first node is the value of the option.

1. The Binomial price tree generation: The tree of prices [53] is produced by working forward from valuation date to expiration. At each step, it is assumed that the price will move up or down by a specific factor (*u* or *d*) per step of the tree (where, by definition, $u \geq 1$ and $0 < d \leq 1$). So, if *S* is the current price, then in the next period the price will either be $S_{up} = S \cdot u$ or $S_{down} = S \cdot d$

The up and down factors are calculated using the underlying volatility, σ and the time duration of a step, *t* (measured in years). From the condition that the variance of the log of the price is $\sigma^2 t$, we have:

$$u = e^{\sigma\sqrt{t}} \quad \ldots\ldots\ldots (1)$$

$$d = e^{-\sigma\sqrt{t}} = \frac{1}{u}. \quad \ldots\ldots\ldots (2)$$

$$(u.\ d = 1)$$

This method ensures that the tree is recombinant, i.e. if the underlying asset moves up and then down (u, d), the price will be the same as if it had moved down and then up (d,u) — here the two paths merge or recombine. This property reduces the number of tree nodes, and accelerates the computation of the option price.

2. Calculation of option Value at each final node: At each final node of the tree i.e. at expiration of the option — the option value is simply its intrinsic, or exercise, value.

Max [(S – K), 0], for a call option
Max [(K – S), 0], for a put option; where K is the Strike price and S is the spot price of the underlying asset

3. Calculation of option value at earlier node: Once the above step is completed, the option value is then found for each earlier node, starting at the penultimate time step, and working back to the first node of the tree (the valuation date) where the calculated result is the value of the option. The steps are as follows:

(1) Expected value is calculated using the option values from the later two nodes (*Option up* and *Option down*) weighted by their respective pseudo-probabilities -- "probability" p of an up move in the underlying, and "probability" (1-p) of a down move. The expected value is then discounted at **r**, the risk free rate corresponding to the life of the option which is the annual interest rate of bonds or other "risk-free" investment. Any amount P of dollars is guaranteed to be worth $P \cdot e^{rT}$ dollars T years from now if placed today in one of theses investments or in other words, if an asset is worth P dollars T years from now, it is worth $P \cdot e^{-rT}$ today. The following formula is applied at each node:

Binomial Value = [p × Option up + (1-p) × Option down] × exp (- r × t), or

$$C_{t-1,i} = e^{-rt}(pC_{t,i+1} + (1-p)C_{t,i})$$

…… (3)

Where $C_{t,1}$ is the option's value for the i^{th} node at time step t,

$$p = \frac{e^{(r-q)t} - d}{u - d} \quad \ldots\ldots\ldots\ldots\ldots (4)$$

q, is the dividend corresponding to the life of the option.

The formula is derived from the assumption that over a period of dT the underlying asset yields the same profit as a riskless investment on average, so that if it is worth S at time t, then it is worth $S \cdot e^{r.dT}$ at time $t + dT$. This provides following equation:

$$S.\, e^{r \cdot dT} = (\mathrm{p}.\, u.\, S + (1 - p).\, d.\, S)$$

(2) This result is the "Binomial Value". It represents the fair price of the derivative at a particular point in time (i.e. at each node), given the evolution in the price of the underlying to that point. It is the value of the option if it were to be held — as opposed to exercised at that point. If exercise is permitted at the node, then the model takes the greater of binomial and exercise value at the node.
(3) Depending on the style of the option, evaluate the possibility of early exercise at each node: if (a) the option can be exercised, and (b) the exercise value exceeds the Binomial Value, then (c) the value at the node is the exercise value.

Razib Hayat Khan is doing his PhD at Department of Telematics, Norwegian University of Science and Technology (NTNU), Norway. He completed his M.Sc. in Information & Communication Systems Security from KTH, Sweden in 2008. He worked as visiting researcher, Duke University, NC, USA. He worked under VRIEND project (http://vriend.ewi.utwente.nl) as part of his M.Sc. thesis and also worked as research engineer, Multimedia technologies at Ericsson Sweden. He received his B.Sc. degree in Computer Science and Information Technology from Islamic University of Technology (IUT), Gazipur, Bangladesh in 2004.