Real Option Applications to Information Security

Pythagoras PETRATOS
Visiting Fellow, University of Buckingham

Abstract: Real options present advantages over the standard discounting methods. In this paper we analyze them briefly and examine their potential applications on information security. The applications of real options on valuation of information assets, information security investment and capital budgeting provide considerable benefits. Finally portfolios of real options and other financial products can reduce information security risk.

Key words: Real options, information security, valuation, information security investment, capital budgeting, portfolio theory, information security risk.

Introduction to real options

"A real option is the right, but not the obligation, to take an action at a predetermined cost called the exercise price, for a predetermined period of time-the life of the option" (COPELAND & ANTIKAROV, 2001, p. 5). The development of real options theory came as a response to the disadvantages of the existing valuation methods. Except the early criticism of Discounted Cash Flow (DCF) (e.g. DEAN, 1951), MYERS (1977) recognized its inability to encompass the value attached to business growth opportunities ("growth options"). Moreover MYERS (1987, pp. 6-13) emphasized the gap between finance theory and strategic planning and suggested to think of strategy in terms of firm's portfolio of real options. Although the name real might be confusing, since many regard it as synonymous to physical assets, both MYERS (1987) stated that real option value applies to growth and intangible assets, and BOER (2002) recommended that option theory can be even more important to the intangible, strategic or virtual side of capital (BOER 2002, p. 117). The real options theory was further enriched by general conceptual frameworks (MASON & MERTON, 1985; BREALEY & MYERS, 2000, etc.) and alternative conceptual real options (DIXIT & PINDYCK, 2001; TRIGEORGIS, 2001) for specific cases of capital budgeting decisions (SCHWARTZ & TRIGEORGIS, 2001).

COMMUNICATIONS & STRATEGIES, no. 70, 2nd quarter 2008, p. 15.

Real options share many similarities with financial options (COPELAND & ANTIKAROV, 2001). The wide use of financial options was triggered by the revolutionary work on option pricing theory by BLACK & SCHOLES (1973), and MERTON (1973). A simplified discrete-time approach for option pricing was later introduced by COX, ROSS & RUBINSTEIN (1979). Except these prominent publications, option pricing has been extensively researched and combined with other financial products[1]. Option theory based on arbitrage pricing methods, implies that since the value of option is derived from the underlying asset, then the value is the same in real world as in a risk neutral environment. According to SCHWARTZ & TRIGEORGIS (2001), the utilization of a risk-neutral framework in the valuation of investment projects has three major advantages. The ability to take into account all the flexibilities (options) of the project, the use of all the information in market prices, when they do exist, and finally to allow the determination of the project value as well as the optimal operating policy (SCHWARTZ & TRIGEORGIS, 2001).

Thus, a major advantage of real option is the management's flexibility to react according to evolving conditions. Managers should not only continuously consider the new information provided by the constant changes in market conditions (technical change, uncertainty, etc) but also have the valuable ability to adapt respectively the business and operating strategy. Only by possessing flexibility the management may be able "to capitalize on future opportunities or mitigate losses" (TRIGEORGIS, 1993, pp. 202-204). Therefore flexibility provides the opportunity to enhance the value of the project during its evolution. "Neglecting it [flexibility] can grossly undervalue these investments and induce a mis-allocation of resources in the economy" (SCHWARTZ & TRIGEORGIS, 2001). Some of the choices are options to defer (INGERSOLL & ROSS, 1992), time to build options (MAJD & PINDYCK, 1987), options to abandon (MYERS & MAJD, 1990), options to expand or growth (BREALEY & MYERS, 1991) and additional types, including multiple interacting options, which are combinations of the various option categories and can also interact with financial options (BRENNAN & SCHWARTZ, 1985; TRIGEORGIS 1996).

[1] Combinations such as swaptions, an option to enter into a swap derivative contract (NEFTCI, 2004).

■ Information security and real options

The most recent Computer Security Institute (CSI) survey in 2007 has demonstrated a significant increase in average annual losses to organizations due to information security breaches, which more than doubled, from $168,000 to $350,424 (RICHARDSON, 2007). Financial fraud increased significantly and for the first time overtook virus attacks and established itself as the greatest source of financial losses; while other threats such as system penetration, denial of service, phishing and botnets retained their impact (RICHARDSON, 2007, p. 15). While there might not be a substantial increase in the number of attacks it is evident that their impact has massively risen. This is reflected in the average annual losses which do reveal an increase in the information security risk. Moreover, financial fraud as the primary threat exposes the fact, that information security attackers have augmented their sophistication driven by financial and criminal incentives. At the same time, there is a New E-Espionage Threat, resulting in appropriation of valuable information, such as industrial secrets and information on weapon systems that generate not only financial losses but create serious dangers to National Defense and Security (GROW *et al.,* 2008). In addition, incidents of cyber warfare, with the notable case of Estonia, can cause considerable damage (*The Economist*, 2007).

There are two key characteristics, especially on the last two threats. Firstly, they cannot be easily predicted and detected. Secondly, it is difficult to estimate the loss from these types of attacks, because they involve intangible goods (e.g. patents, copyrights, etc.), or impair critical infrastructure with all associated costs. Returning to the CSI survey, except the companies that did not use any measurement to justify information security expenditure, most of the companies that utilized financial metrics, employed return on investment (ROI), net present value (NPV), or internal rate of return (IRR) (RICHARDSON, 2007, pp. 8-9). A common feature of all three methods is their direct connection to discounted cash flow (DCF) approach. In the introduction we presented some of its main disadvantages. Regarding intangible assets, like projects of high-growth or in the research and development (R&D) stage, it misses them in the calculations and fails to recognize their strategic value (BOER, 2002). Particularly in the information and communications technology (ICT) industry, in which important assets include intellectual capital at R&D development stages and high-growth projects. Real options can offer an alternative to the disadvantages of these standard methods, since they can better facilitate the estimation of value and managerial strategy.

A critical factor for the application of real options in information security is the idiosyncrasies of the related market. Information security market is characterized by dynamic effects and often unforeseeable events and conditions. While in the recent years a massive attack on information systems has not occurred, there were severe attacks in the past like the Melissa (F-SECURE undated) and MyDoom (CNN.com 2004). Although the circumstances have changed, none can guarantee that similar scale attacks might not happen again, due to numerous reasons. One of them is that vulnerability, in a widely-used operating system or software, might provide the chance for a large scale attack. Especially, because the number, and more importantly the sophistication of attackers, presents an upward trend (MISHA, 2007). Moreover, new threats have arisen. For example, bots are programs silently installed to hijack computers for fraudulent online activity and "the effect on the basic worldwide network infrastructures could be disastrous" (BARROSO, 2007). In this dynamic environment management requires flexibility to deal with the changing nature of the information security market. To ensure flexibility and the achievement of optimal operating policies appropriate methods, as real options, should be implemented.

Valuation of information assets

Information asset is a broad term. It covers all valuable information. Although information is an intangible asset there are tangible assets, such as hardware involved in its protection. While physical information systems facilitate the handling of information and therefore enhance the information value chain, the burden of value remains in information *per se*. To illustrate this point, despite the fact that banks have heavily invested in information systems, it is the information on databases which has the majority of value. An attack on the ICT infrastructure could result in significant operating losses. However, an attack compromising client information would probably prove catastrophic. This is not due to the loss of information that can be recovered, but mainly because its disclosure can lead to legal action by the clients and thus financial costs[2]. Similarly, if confidentiality of R&D information is breached by targeted attacks and this information is available to other competitors, then the competitive advantage of a company is

[2] There is currently a legal framework protecting personal data as in European Union (see http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm) and related legislation with the notable example of Sarbanes-Oxley Act.

undermined. The firm's investment in R&D is exploited by others who benefit from it without paying the related costs. Therefore economic externalities are created, discouraging innovation and causing welfare losses.

In order to protect information assets investment in information security is required. To obtain a suitable amount of investment appropriate calculations are essential. An economic model that determines the optimal investment for the protection of information assets proposed by GORDON & LOEB (2002) takes into account three main factors; the monetary loss by a security breach, the probability of the threat occurring and the probability that this threat could be successfully realized (GORDON & LOEB, 2002, pp. 438-457). The first parameter depends on the value of the information assets. The more valuable the assets are, the more loss might occur, *ceteris paribus*. Therefore, a priority is to estimate the value of information assets. However, this presents considerable difficulties if it is performed using the standard discounting techniques (DCF), as it was shown above. Reminding that many information assets are intangible goods, there are suggestions (*i.e*. MEYERS, 1987; BOER, 2002) that real option have useful application in their valuation.

Moreover, real options valuation in R&D projects has gained growing attention and its pragmatic character has enabled several applications in consulting and business, which will gain even more importance in the future (PERLITZ *et al.,* 1999, pp. 256-269. In practice, real options commonly occur and determine how decision makers regard an investment (BUSBY & PITTS, 1997, pp. 169-186). The ICT sector is research intensive. Thus the application of real options in R&D valuation plays a leading role in defining the value of information security assets. Many authors advocated that real options can be also be applicable to virtual organizations. The use of inappropriate valuation methods (i.e. DCF calculations, inappropriate metrics, etc.) during the internet boom, led to overvaluations [this is a rather complicated issue that I much simplified. The "comparables" for DCF valuations were similar internet companies. So the growth rates of cash flows were following the wrong paradigm, and at the same time intellectual capital valuation "needed to be stretched very far to explain the huge valuations" (BOER, 2002). This leads to more complicated analysis that I tried to avoid with, of course, the cost of being misunderstood]. Consequently it generated the "dot-com" bubble, which when eventually burst caused substantial financial losses. Such phenomena can be avoided with the suitable use of valuation methods. Companies like Amazon.com survived the bubble since they had embedded options, depicting strategic value, while other companies that did not use real options, such as eToys, went out of business[3]. MUM (2005) supports that the use of real options in valuation of e-business strategic projects can provide great insights and value (MUM, 2005). Finally, in valuing internet projects with real options significant value is added (COPELAND & ANTIKAROV, 2001).

Investment in information security and capital budgeting

In the previous part of the analysis the application of real options in the valuation of information assets was demonstrated. Real options can better define the value of assets compared to DCF, which is widely used in information security assessment. Especially in the case of virtual organisation and R&D projects there is strong empirical evidence supporting this statement. In the Gordon and Loeb model, monetary loss is treated as a fixed amount estimated by the firm as the present value of future losses. Nevertheless it is recognised and investigated by the authors that the loss depends on the use of information by participants (e.g. the firm, the hackers and competitors), and would change over time (GORDON & LOEB, 2002, pp. 438-457). However, the systemic caveat still remains the exercise of discounting methods to obtain the present value. In addition, the interactions among participants are neglected. KUNREUTHER & HEAL (2003) proposed the concept of interdependent security, in which the actions of decision makers are interrelated (KUNREUTHER & HEAL, 2003, pp. 231-249). Therefore a strategic planning based on game theory is required to comprise the interdependence of security levels and avoid suboptimal investments. In order to achieve management flexibility and attain an optimal strategy, real options can be of immense importance.

Information technology investments constitute a main part of capital expenditure budgets in several firms. A considerable proportion of the IT expenditure is often dedicated to information security. While the Gordon & Loeb model recommends that the optimal level of investment accounts for approximately 36.8% of the expected loss from a security breach, HAUSKEN (2006, pp. 338-349) suggests alternative solutions resulting in different figures (WILLEMSON, 2006) disproved the GORDON & LOEB conjecture by constructing an example of 50% required investment and even 100% when relaxing the original requirements (WILLEMSON, 2006, pp. 87-98). Except the discounting disadvantages of these models enormous

[3] The examples are described in BOER (2002) p. 117.

variations do exist[4]. The application of real options can assist in the management of information technology investments. The benefits are dual. More precise information security investment figures might result, and the management would have the ability to react to changing market conditions according to the available options.

A formal and practical methodology considers investment as a way to create business capabilities, facilitated by real options, in order to better cope with uncertainty (BALASUBRAMANIAN *et al.,* 2000). An extension of this model can be formed for information security investment. Investing appropriately in operating capabilities can enhance the firm's future cash flows. Investment in information security can ensure that these operating drivers would not be disrupted by attacks and therefore operating profits would be retained. Furthermore, it can be combined with business decisions, aligning the business views with technological aspects. Senior managers would be able to conduct investments in information security technology according to the changing trends of security attacks. Decision trees provide the ability to choose different strategic paths in regard to both business conditions and security threats. By having various decision nodes management is capable to react to increasing or decreasing security risks (i.e. new threats, such as new viruses, worms, botnets, e-espionage etc.)[5]. At the same time business decisions can be further related to other decision models such as game theory (i.e. Nash equilibria) of interdependent security and attack trees (SCHNEIER, 1999). The outcome is better decision making, using real options, which is likely to increase value.

Information security investment is part of a broader investment process known as capital budgeting. Except the fact that modern finance theory allocates capital according to discounting (NPV) rules, these rules provide no guidance for internal capital allocation (HARRIS & RAVIV, 1996, pp. 1139-1174). Under condition of imperfect markets and uncertainty managers are required to maximise the firm's market value. In order to achieve this aim, financial executives need criteria to choose between alternative time patterns of share price within the planning horizon (MAO, 1970, pp. 349-360). This is conducted from an operational, viewpoint. Thus, management should optimise its operational performance via a suitable

[4] All of the described models build upon the model of GORDON & LOEB (2002).

[5] BULASUBRAMANIAN, *et al.* (2000) use decision trees (pp. 51 - 52) to account for factors as product demand and connect them to project and business uncertainty. Similar models can be created for information security by implementing demand for security and the potential losses or benefits that this might have on cash flows.

strategy. Real options significantly assist in obtaining an optimal operating strategy. More importantly they can also provide the necessary criteria for an effective internal allocation resource mechanism. Implementing numerous factors in decision trees, which are interrelated, can indicate the best options to maximise operating profits and consequently market value. Operational capabilities are connected to investments and also investments between each other. Therefore managers have the option to pick the best mix of investments that maximises operating profits.

One of the key parameters for successful decision making is perfect information. During the life of the project market conditions might change radically. Information security is a dynamic market in this respect. In an investment decision using the standard discounting approaches only the information in the present time is taken into account. If during the progress of the project more and better information is available, it cannot be incorporated in the investment decision and capital budgeting of the project. On the contrary real option applications consider information at various stages of the life of the project. Hence, information asymmetries can be avoided and managers have the real options (to expand, abandon etc.) to use this information and gain value (TRIGEORGIS, 1993, pp. 202-224). Lastly, this is essential if quick and flexible investment decisions should be taken to avoid catastrophic losses, as for example targeted e - espionage that undermines the competitive position of the corporation.

■ Real options, financial flexibility and financial engineering

In the previous parts of the analysis we showed the applications of real assets in information security. More precisely the use of real options on information asset valuation and information security investment and capital budgeting was examined. In the course of the analysis their combination was presented with other theoretical concepts as interdependent risk, related game theory models and asymmetric information. (TRIGEORGIS, 1993) commenting on these theoretical extensions, notices numerous applications as Bayesian analysis, Agency Theory and venture capital implementations that are likely to increase financial flexibility (TRIGEORGIS, 1993, pp. 202-224). In that sense real options might have additional applications in several aspects of finance. A notable case is diversification. The use of options constitutes a portfolio of a variety of investments.

Managers have the choice to exercise the most valuable option according to the market conditions, in our case derived by information security. Furthermore they can hedge against security threats. Diversification can reduce risk (MARKOWITZ, 1991).

While the analysis concerned mainly investment projects in information security, there are additional financial products, which can be combined with real option analysis and create an effective diversified portfolio, to reduce information security risk. Cyberinsurance is probably the most common, since it allows companies to reduce remaining risks, even after the implementation of technical information security measures (RICHARDSON, 2007). It can also provide incentives for security investment that reduce risk (BAER & PARKINSON, 2007, pp. 50-56). Moreover, the evolution of information security market could generate demand for more financial products as information security derivatives (PETRATOS, 2007, pp. 54-57).

Unfulfilled demand in information security market could trigger innovation and creation of information security derivatives (e.g. financial options) or other complex information security financial products. Financial engineering therefore can provide significant solution. An appropriate selection and inclusion of such products in portfolios along with real option facilitating strategic management can effectively protect against information security threats and create significant value.

Conclusions

Real options have important applications in information security. They can be used in information asset valuation, investment in information security and capital budgeting. The flexibility provided creates value and facilitates the implementation of an optimum operating policy and in this context optimum information security policy. As the information security market evolves, more financial products are likely to be developed. Portfolios of real options and their combinations with these products can significantly reduce information security risk.

Reference

BAER W & PARKINSON A. (2007): "Cyberinsurance in IT management", *IEEE Security and Privacy*, Vol. 5, no. 3, pp. 50-56.

BARROSO D. (2007): "Botnets the Silent Threat", *ENISA Position Paper no. 3,* ENISA.

BOER P. (2002): *The Real Options Solution. Finding Total Value in a High-Risk World,* John Wiley & Sons, Inc. Hoboken, NJ.

BULASUBRAMANIAN P., N. KULATILAKA & J. STORCK. (2000): "Managing Information Technology Investments Using Real-Options Approach", *Journal of Strategic Information Systems*, 9, pp. 39-62.

BUSBY J. & PITTS C. (1997): "Real Options in Practice: an Exploratory Survey of How Finance Officers Deal with Flexibility in Capital Appraisal", *Management Accounting Research*, Vol. 8, no. 2, pp. 169 - 186.

CNN.com (International) (2004): "Security Firm: MyDoom Worm Fastest Yet", January 28, http://edition.cnn.com/2004/TECH/internet/01/28/mydoom.spreadwed/

COPELAND T. & ANTIKAROV V. (2001): *Real Options. A Practitioner's Guide*, TEXERE, New York - London.

(The) Economist (2007): "Cyberwarfare is Becoming Scarier", May 24th.

F-SECURE (undated): F-Secure Virus Descriptions: Melissa. See: http://www.f-secure.com/v-descs/melissa.shtml [2 June 2008].

GORDON & LOEB (2002): "The Economics of Information Security Investment", *ACM Transaction on Information and System Security,* Vol. 5, no. 4, pp. 438-457.

GROW B., K. EPSTEIN & C.-C. TSCHANG (2008): "The New E-Espionage Threat", *Business Week*, Cover Story, April 10th. See: http://www.businessweek.com/magazine/content/08_16/b4080032218430.htm?chan =top+news_top+news=index_businessweek+exclusives [2 June 2008].

HARRIS M. & RAVIV A. (1996): "The Capital Budgeting Process: Incentives and Information", *The Journal of Finance*, Vol. 51, no. 4, pp. 1139-1174.

HAUSKEN K. (2006). "Returns to Information Security Investment: The Effect of Alternative Information Security Breach Functions on Optimal Investment and Sensitivity to Vulnerability", *Information Systems Frontiers*, 8, pp. 338-349.

KUNREUTHER H. & HEAL G. (2003): "Interdependent Security", *The Journal of Risk and Uncertainty*, 26:3, pp. 231-249.

MISHA G. (2007): "Boom-Time for Mafias", *The World in 2007*, *The Economist*, London, United Kingdom.

MAO J. (1970): "Survey of Capital Budgeting: Theory and Practice", *The Journal of Finance*, Vol. 25, no. 2, pp. 349-360.

MUM J. (2005): *Real Option Analysis. Tools and Techniques for Valuing Strategic Investment and Decision*, John Wiley & Sons, Inc. Hoboken, NJ.

MYERS S. (1987): "Finance Theory and Financial Strategy", Midland Corporate, *Finance Journal*, Issue 5, no. 1, pp. 6-13.

NEFTCI S. (2004): *Principles of Financial Engineering*, Elsevier Academic Press, New York.

PETRATOS P. (2007): "Weather, Information Security, and Markets", *IEEE Security and Privacy*, Vol. 5, no. 6, pp. 54-57.

PERLITZ M., T. PESKE & SCHRANK R. (1999): "Real Options Valuation: the New Frontier in R&D Project Evaluation?", *R&D Management*, 29, 3, pp. 256-269.

RICHARDSON R. (Ed.) (2007): *2007 CSI Computer Crime and Security Survey*, Computer Security Institute.

SCHNEIER B. (1999): "Attack Trees", *Dr Bobb's Journal*, December Issue.

TRIGEORGIS L. (1993): "Real Options and Interactions with Financial Flexibility", *Financial Management,* Vol. 22, no. 3, pp. 202-224.

WILLEMSON (2006): "On the Gordon and Loeb Model for Information Security Investment", The Fifth Workshop on the Economics of Information Security (WEIS 2006), Cambridge, UK, 26-28 June, 2006; University of Cambridge, 2006, 87-98.