Determining the Value of Information Security Investments
A Decision Support System

Hannah Louise Davies and Andrew J. C. Blyth
Information Security Research Group, University of South Wales, Pontypridd, U.K.

Keywords: Return on Security Investment, Multi-Attribute Utility Theory, Decision Making under Uncertainty, Multi-Criteria Decision Making, Information Security Metrics, Decision Making for Information Security.

Abstract: Advances in the technological era are making information security breaches a more common occurrence. A vital part of ensuring an organisation is well protected from these increasingly complex threats is a suitable security solution. Suitability of a security solution should not only be measured in terms of goals such as reducing down time or reducing the risk of a certain threat, but also meet stakeholder and executive goals in terms of being cost effective. Currently, cost effective is determined by calculating a return on security investment calculation, where the cost of a solution is evaluated against any savings resulting after purchasing the solution to determine whether the option is viable. The current implementation of return on security investment calculations however is often subjective and inaccurate as calculations are performed in an ad-hoc manner. When there are multiple factors to consider, with uncertain or incomplete values available, a multi-attribute decision making method that utilises uncertainty is required in order to allow the decision maker to assess all possible options in the most logical and objective manner, whilst keeping in mind the goals of the organisation. In this paper we present and evaluate a conceptual, analytical framework that, with the use of multi-attribute utility theory under uncertainty, is able to model return on security investment calculations in a novel way. This new calculation is introduced as a Value of Information Security Investment calculation. The final goal is to create a framework that allows for repeatable, predictable and mature, calculations that determine the value of an information security investment.

1 INTRODUCTION

Since the global economic crisis of 2008, justifying a decision to acquire tools, techniques and processes has become increasingly important. In this technology era, organisations are faced with building and maintaining an effective information technology infrastructure that is not only suited to the organisations objectives, but conforms to policy, addresses the alarming increase in information security threats (Al-Humaigani and Dunn, 2003) and is cost-effective.

When designing an effective security solution, an organisation requires a complete Risk Management framework to identify, measure and manage the risks present. Assessing the financial aspect of a security solution is also important and is most commonly evaluated by performing a return on investment (ROI) calculation (Pontes *et al.,* 2011). ROI calculations aim to answer the question as to which option gives the most value for money (Sonnenreich, 2006). The problem faced, however, is that security programs and solutions are often preventing losses and not delivery profit; hence calculating a standard ROI is not sufficient. Applying a security program or solution is expected to reduce the risks threatening your assets, thus a return on security investment (ROSI) calculation should be used to calculate how much loss has been avoided following the investment (ENISA, 2012). The standard ROSI methodology involves the comparison of the monetary value of the investment and the monetary value of the risk reduction. The monetary value of the risk reduction can be estimated by a quantitative risk assessment (ENISA, 2012).

With security threats becoming more sophisticated and more costly, determining the acceptable risk level and selection of an optimal cost effective solution is becoming an increasingly complex but necessary decision for information security management. As with all such decisions, expenditure to protect a system has to be fully justified in terms of a well-specified objective (Ioannidis *et al.,* 2010). Another issue that arises

Louise Davies H. and J. C. Blyth A..
Determining the Value of Information Security Investments - A Decision Support System.
DOI: 10.5220/0005170704260433
In *Proceedings of the International Conference on Knowledge Management and Information Sharing* (KMIS-2014), pages 426-433
ISBN: 978-989-758-050-5

with calculating ROSI is the lack of data concerning information security (Levy, 2005). Security breaches and incidents are still seen as a reason for embarrassment and few companies are willing or able to provide actual costs associated with security breaches (Sonnenreich, 2006). However, whilst the data itself can be improved in terms of accuracy, it is in fact the reproducible nature of the calculation that is important, this reproducible nature arises from a consistent methodology of calculating and reporting the cost (Sonnenreich, 2006).

There are multiple factors and numerous alternatives to consider when such a widely used methodology as multi-criteria decision-making (MCDM) is used. MCDM is a collection of methodologies used to compare, select or rank multiple alternatives that typically involve incommensurate attributes (Levy, 2005). MCDM can fall in to two main categories; 1) decision making under certainty and 2) decision making under uncertainty. However, in practice, it is extremely unlikely to have complete information about the future (Shah *et al.*, 2007). The values used in ROSI calculations are subject to uncertainty, primarily down to the fact that you cannot predict, with a high level of certainty, the losses caused when an event may or may not happen (Sonnenreich, 2006). Consequently, decision-making under uncertainty is the logical method to use in order to allow for realistic solutions.

Though there are previous applications of decision analysis to ROSI problems, the inclusion of multi-attribute utility theory (MAUT) hasn't been applied to its fullest extent. The cases of MAUT being used are restricted to a small number of attributes, such as cost and availability (Ioannidis *et al.,* 2010), (Beautement *et al.,* 2008), or cost, investment and availability (Beres, Pym and Shiu, 2010) for example. The limited use of MAUT doesn't show the full extent to which decision analysis can be used to support ROSI calculations.

2 RELATED WORK

2.1 Return on Security Investment

Performing an ROSI calculation is a method of evaluating a security investment prior to making a decision; it compares the cost of implementing and procuring a solution to the losses avoided. It is the misconception of what ROSI demonstrates, in terms of not necessarily representing a profit, which has led to its misuse.

Relatively recently, in 2002, Gordon and Loeb adopted a static optimisation model where the optimal ratio of investment in Information Security can be calculated under different assumptions of expected loss. This model relies on restrictive assumptions to calculate the optimal ratio and has sparked much debate regarding whether the relationship between Information Security Investment and vulnerability is always a monotonic function. In 2006, Hausken proposed that vulnerability be represented as a function, showing the optimal ratio cannot be supported.

An important issue is that the inputs for ROSI may be highly subjective, and consequently, companies that use the same method for calculation can arrive at extremely varied results due to different choices made about the inclusion or exclusion of costs (Sonnenreich, 2006). In addition, estimating losses from future events brings uncertainty in to the values used. Even when actuarial tables or insurance data are used, these values may not be accurate due to the "ostrich effect" (Sonnenreich, 2006) experienced when an incident occurs. Another way to collet data is to base values on competitors experiences. This could be to investigate losses incurred by competitors during incidents, or an uptake in sales within an organisation once a competitor has experienced an attack. These values of losses or gains can be added on to the ROSI analysis (Korostoff, 2003) or values based on previous experience can also be used. Finally, the variable most complex to define and evaluate is the mitigated risk. One method to consider is the use of past data, determining the expected losses due to security breaches prior, and subsequent to, implementing a solution (Arora, Frank and Telang, 2008). The avoided risk or expected benefit is then the difference between the baseline loss and residual risk. When using this approach, it must be recognised that rare events may preclude the use of past data, when such events occurred sufficiently long ago that the same conditions no longer apply.

ROSI calculations, as explained above are based heavily on estimations or perceptions of values – this makes ROSI more of an approximation and less accurate. It is the ability to manipulate these approximations to justify decisions (ENISA, 2012) that call for ROSI to be improved, in terms of reproducibility, repeatability and predictability. The biased perceptions of a decision maker should not cause differing outputs of the calculations. ROSI equations should be objective and numerical but due to insufficient definition or subjective variables, the calculations become imprecise and subjective

(Rudolph and Schwarz, 2012). Another criticism of ROSI is that the methods are complex and rely on soft data to derive hard numbers that are associated with ROSI. This takes time and therefore simple but effective methods are preferred in practice (Holoman and Kuzmeskus, 2012). This research aims to identify a more suitable method of justifying Information Security Expenditure by means of an accurate, reproducible and objective approach in order to mitigate such criticism.

2.2 Multi-Attribute Utility Theory

Concerning ROSI, most decisions are made in an environment where the eventual outcomes are unknown. It is the area of decision making under uncertainty where the methodology of ROSI and decision analysis should be performed. Decision analysis was originally developed to aid a decision-maker's evaluation of alternatives whose outcomes were uncertain (Raïffa and Schlaifer, 1961). Decision theory provides an approach to modelling uncertainty in the environment, using probability to describe the likelihood of uncertain events and using utility to model the decision-maker's attitude to risk (Belton and Stewart, 2002).

Multi-attribute utility theory seeks to reduce the complex problem of assessing a multi-attribute utility function into one of assessing a series of uni-dimensional utility functions. These individually estimated component functions are then brought together again; the glue is known as value trade-offs (Zeleny, 1982). The trade-off issue is, in essence, evaluating how much achievement, in objective 1, is the decision maker willing to give up to improve achievement, by some fixed amount, on objective 2 (Keeney and Raïffa, 1976). By determining the trade-offs that a decision-maker is willing to make, the optimal solution based on these preferences can be determined.

An important step in using MAUT is defining the objectives that an organisation has. There are 4 identified steps to develop and quantify objectives (Keeney, 1975):

- Identify objectives that the organisation considers important.
- Structure the objectives into a hierarchy so ends and means remain distinct and redundancies get eliminated.
- For clarification, define attributes for objectives, and then consequences are measurable.
- Develop a utility function to indicate value trade-offs and reflect different viewpoints within the organisation.

For the application of MAUT that is being considered here, an objective may be to reduce the vulnerability of the organisation to a specific threat agent. An attribute would then be the number of incidents in a week/month/year relating to that specific threat agent. Uncertainty would then be propagated over the variables with the use of probabilities.

The basis of MAUT is the use of utility functions; these can be applied to transform the raw performance values of the alternatives against diverse criteria, factual and judgemental, to a common dimensionless scale (Fülöp, 2005). In practice, the interval [0,1] is used, where 1 is the highest utility that can be achieved, and 0 is the lowest utility that can be achieved. Utility functions allow for the most preferred alternative to obtain a higher utility value than less preferred alternatives.

The use of utility functions also allow for more relevant criteria to contribute more substantially to the overall utility value than less relevant criteria. The actual magnitude of the utility is not important, the utility function serves as a "risk preference thermometer" that can be used for ranking lotteries according to the risk preference of an individual (Howard, 1968). We seek a utility function $U(\mathbf{z})$, such that alternative a is preferred to alternative b if and only if the expectation of $U(\mathbf{z}^a)$ is greater than $U(\mathbf{z}^b)$, that is:

$$E[U(\mathbf{z}^a)] > E[U(\mathbf{z}^b)] \qquad (1)$$

Where $\mathbf{z}^a$ and $\mathbf{z}^b$ are the random vectors of attribute values associated with alternatives a and b respectively. This is the Expected Utility Hypothesis (Løken, 2007). Establishing the existence of a utility function is a non-trivial process, even for the single attribute case. It is within this context that von Neumann and Morgenstern (1947) first developed utility theory.

2.2.1 Additive Utility Model

The additive utility function is the best-known form of multi-attribute utility functions because of its relative simplicity and application to real world problems (Raïffa and Schlaifer, 1961). The additive utility function should be considered firstly as a possible solution as it is the simplest form of a utility function. There are a number of conditions that need to be shown to be satisfied in order for the additive form of multi-attribute utility model to be valid. However, when it is not possible to prove all of the additivity assumptions hold for every case, strong evidence suggests that even when complete independence isn't established, the additive model can still provide close approximations to "pure" additive utility functions (Yoon and Hwang, 1995).

3 INTRODUCING THE VALUE OF INFORMATION SECURITY INVESTMENT AS A CONCEPT

For any organisation, there are a number of questions relating to Information Security investments. Organisations are interested in the amount of investment that should be made, selection of the measures that should attract investment and the effectiveness of any potential investments (Zhang and Li, 2005). All of these questions can be addressed via the implementation of a decision support system that utilises multi-attribute utility theory under uncertainty. Due to the fact that the "return" of Information Security investments doesn't usually come from increased revenues, decreased costs or other monetary values, this decision support system avoids the use of the word "return" but rather determines the value of Information Security Investments – not just as a monetary value – by determining the value added to any attributes, such as process maturity, time saving or peace of mind for stakeholders. Hence, we introduce an alternative method for justifying Information security expenditure in the form of a Value of Information Security Investment (VISI) Calculation.

3.1 Risk Management Process

ROSI is best incorporated into a full Risk Management (RM) process, hence, VISI is also best utilised in a full RM framework. Pontes et al. (2011) propose a Comprehensive RM framework that purposely incorporates an ROSI phase. The phases identified in the RM framework are; plan, risk appreciation, ROSI, risk treatment, closing. The RM framework proposed by Pontes et al., 2011 could therefore be extended to include a VISI calculation phase in place of ROSI.

3.2 Proposed Architecture

The main underlying concept of the proposed solution is to produce a decision support model that is able to evaluate multiple attributes, multiple alternatives, ROSI calculations and trade-offs under uncertainty to identify an optimal security solution for any particular organisation. The purpose of this approach is to create a standard method for calculating VISI and making an informed decision based upon these VISIC results.

Multi-attribute utility theory will initially form the analytical core of this system. The multi-attribute utility model will be fed with data that defines the objectives of the organisation, the attributes to be considered in the decision process and the alternatives. If the number of attributes is denoted as n and the number of alternatives denoted by m, then the proposed architecture is designed to be able to consider n attributes across m alternatives. This approach allows more sophisticated methods of dealing with the uncertainty present in VISI calculations. The initial proposed architecture is shown in Figure 1.

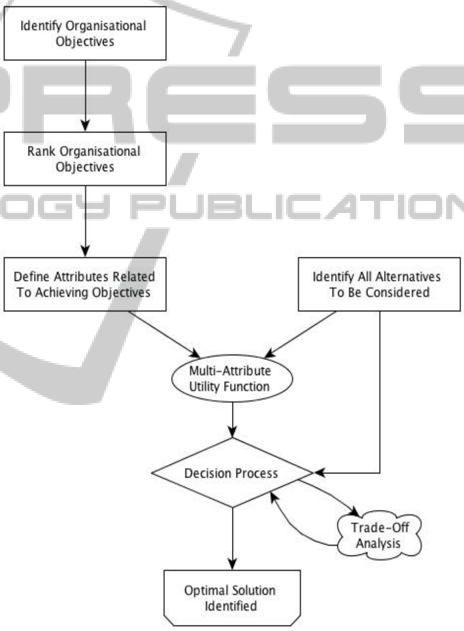
Identify Organisational Objectives
Rank Organisational Objectives
Define Attributes Related To Achieving Objectives
Identify All Alternatives To Be Considered
Multi-Attribute Utility Function
Decision Process
Trade-Off Analysis
Optimal Solution Identified

Figure 1: Initial Proposed Architecture.

3.3 Proposed Validation

In order to validate the decision support model that is being proposed, a series of realistic and appropriate case studies need to be considered. The case studies also need to be reliable and able to replicate real world behaviour and decisions. The case studies will be hypothetical, although these will be validated by the use of industry experts. The case studies will initially start with a simple, small decision problem to demonstrate that the solution is viable. The model complexity will then be increased to demonstrate applicability of the solution to real world problems that are currently being encountered. Yin (2009), characterises case study research as an empirical inquiry that:

- Investigates a contemporary phenomenon within its real life context; when
- The boundaries between phenomenon and context are not clearly evident.

As the VISI calculation is extremely complex, comprising of alternatives, objectives, attributes and their interrelationships, a case study design was warranted. As stated by Yin (2009), case studies have at least four different applications, perhaps most importantly, the explanation of causal links in the VISI calculation, and to provide enlightenment to situations in which the VISI calculation being evaluated has no clear, single set of outcomes. The case study approach also allows for the use of data from multiple sources.

3.4 Initial Case Study

This hypothetical case study looks at a medium sized organisation that is concerned about the safe use of its sensitive data. As the insider threat is still identified as a serious threat for organisations (Pricewaterhouse Cooper, 2014), this case study will consider the threat agent to be an insider with direct access to the system and the alternatives available to be preventive measures that will deter or prevent the insider from extracting sensitive data. The psychological reasons for insiders acting maliciously towards a present or previous employer are outside the scope of this paper.

Three alternatives available to the organisation are identified. These include off the shelf software to prevent unauthorised storage devices being connected to the network, implementation of a tracking software that track activity and raise alerts to suspicious activity and finally the use of database monitoring software to monitor access to certain restricted data by insiders.

The organisation is concerned with the following attributes that it will use to evaluate the decision. These attributes are cost, lifetime and maturity. As can be seen, these attributes are measured in different units and are defined in monetary and time units as well as a scale. These incommensurate attributes are just one issue that is met when trying to perform a VISI calculation to justify information security expenditure.

This case study will use an additive utility function U. This form of multi-attribute utility theory includes individual utility functions U_i for each attribute x_j, usually scaled from 0 to 1 that reflect the decision-makers trade-offs among the attributes.

$$U(x_1,x_2,x_3) = w_1U_1(x_1)+w_2U_2(x_2)+w_3U_3(x_3) \quad (2)$$

Where

$$w_1+ w_2 + w_3 = 1 \quad (3)$$

Weights may be specified directly, or found using a swing-weight procedure. Individual utility functions are assessed using the range of attribute values across the alternatives being considered in the decision problem.

In this example, the cost has a unit of GBP, the lifetime is the expected number of years that the product will last or be useful and the maturity is a value given by a third party organisation.

Table 1: Decision Attributes and Alternative 1.

Attribute	Alternative 1
Cost	£3000
Lifetime	3 years
Maturity	Low

Table 2: Decision Attributes and Alternative 2.

Attribute	Alternative 2
Cost	£9000
Lifetime	5 years
Maturity	High

Table 3: Decision Attributes and Alternative 3.

Attribute	Alternative 3
Cost	£6000
Lifetime	5 years
Maturity	Medium

The individual utility for each attribute shall be assessed in the following way:

Table 4: Individual Utilities for each attribute.

Attribute	
Cost	U(£3000) = 1, U(£9000) = 0, linear
Lifetime	U(3 years) = 0, U(5 years) = 1, linear
Maturity	U(Low) = 0, U(Medium) = 0.6, U(High) = 1

These assessments for each attribute will allow for the individual utility for each alternative to be found below in Tables 5-7.

Table 5: Individual Utility for Alternative 1.

Attribute	Alternative 1
Cost	1.0
Lifetime	0.0
Maturity	0.0

Table 6: Individual Utility for Alternative 2.

Attribute	Alternative 2
Cost	0.0
Lifetime	1.0
Maturity	1.0

Table 7: Individual Utility for Alternative 3.

Attribute	Alternative 3
Cost	0.5
Lifetime	1.0
Maturity	0.6

The trade-offs assessment is more difficult to make. One method is to assess weight ratios. In this example, the decision maker identifies that cost is twice as important as lifetime. This may be interpreted to mean that the change in overall satisfaction corresponding to a change in cost from £9000 to £3000 is twice the change in overall satisfaction relating to a change in lifetime from 5 years to 3 years. Similarly, for maturity, the decision-maker may judge that the £6000 decrease in cost is 1 and half times as satisfying as a change from a high to low rating. These ratios are used to identify the weights for each attribute in Table 8.

Table 8: Weight Assessments.

Weights	
Cost	0.462
Lifetime	0.231
Maturity	0.307

These weights are then used to identify the overall utility value for each alternative. These are shown in Table 9 below.

Table 9: Overall Utilities.

Alternatives	Utility Value
1	0.462
2	0.538
3	0.6462

Hence, the maximum utility is that of alternative 3. Hence, the approach that should be adopted is that of the database monitoring software. In order to assess the VISI calculation of this decision, we first need to identify the cost to the organisation of not choosing any of these solutions. This is vital to ensure that the amount of expenditure is below the potential losses. The organisation suspects that if a large-scale breach were to occur that the cost would exceed £20,000, in the lowest case the cost of the incident is estimated at £10,000. This shows that even the minimum cost is higher than that of the expenditure. When evaluating the expenditure over the lifetime of the product we see that the expected losses are still much higher than that of the expenditure required for alternative 3.

This relatively simple, initial case study shows the viability of using multi-attribute utility theory to assess information security expenditure decisions. So far, the decision has been investigated in terms of just the attributes cost, lifetime and maturity. However, information security decisions for expenditure need further justification. We propose this comes in the form of a VISI calculation. The purpose of the VISI calculation is to show the value of the expenditure. The cost to the organisation if a major incident occurs is £20,000. The organisation also identifies the probability of a major incident occurring to be 0.05 and the probability of a minor incident occurring to be 0.2. In order to identify the VISI for each alternative, we need to evaluate the savings and costs in order to identify the best possible solution. For alternative 1, the savings are potentially £17,000; alternative 2 provides a potential saving of £11,000; alternative 3 provides a potential saving of £14,000. This should also be included in the utility theory process, however the uncertainty present in reality of these potential losses doesn't allow for a linear utility function. We identify the decision-maker to be risk averse and hence the utility function now will be concave shaped. In the case of a risk seeking decision-maker, the utility function would be convex shaped.

We define VISI as follows:

$$\text{VISI} = \emptyset S - I \qquad (4)$$

Where $\emptyset$ represents the breach probability, S represents the potential savings and I represents the investment cost of the alternative. This cost should be considered in a singular unit of time, which is annually, monthly or weekly for example.

Including this VISI value in to the utility theory process as another attribute further validates the expenditure being considered. We are trying to achieve the highest VISI and hence, the highest value will be assigned the value of 1, and the lowest the value of 0 for the assessment of each alternative. The potential savings and cost of the solution elements require a pre-determined set of values to include. By providing a set of values to include in this process, the calculation will be repeatable and reproducible as well as comparable across departments and organisations.

The savings and costs to be included are:

- Monetary losses due to downtime.
- Monetary losses due to loss of business.

- Losses in terms of productivity of employees.
- Cost of software, hardware, maintenance and licencing costs.
- Training costs.

This list of savings is currently under review and will be extended and adapted as required.

4 CONCLUSIONS

This paper has demonstrated that the current state of the art methods in ROSI calculations for information security possess deficiencies in producing repeatable, predictable and reproducible results. Due to the rapid increase in the number of breaches organisations now encounter, protecting an organisation is an important aspect. This solution should not only meet the criteria in terms of protection of assets and critical systems but should also be viewed as cost-effective to stakeholders and executives.

The expansion of ROI calculations to security is not viable, due to the nature of security solutions preventing losses and not generating profit, thus a specific ROI calculation for security needs to be used. Due to inaccurate data and inconsistent methods of calculating and reporting losses, many ROSI calculations are estimations at best, and only provide insight when the methodologies are kept constant – by a single organisation for example. The current best practice methods are simple calculations, however these calculations are unable to deal with hard to define and complex metrics.

This paper presents a multi-attribute utility theory method instead of using ROSI calculations. This method allows for decision-making under uncertainty to be carried out in a logical way even when considering multiple objectives, attributes and alternatives. This consistent methodology allows for repeatable and predictable results that are reproducible when supplied with the organisational data and method. This proposed, novel solution is defined as a Value of Information Security Investment calculation.

This paper presents the initial solution framework and an initial case study. The idea of the initial case study is to show the viability, and ease of the VISI calculation.

Future work with the VISI calculation will involve refinement of the calculation method and the application to more complex, real world decision-making problems that are encountered in large, security or government organisations. Also, the RM framework needs to be expanded to include the VISI calculation to provide organisations with a complete picture of their information security position. Sensitivity analysis also needs to be carried out on VISI calculations, both coarse and fine, for sensitivity to large and small changes to the ratios identified, in order to investigate how these changes affect the identified solution in terms of the overall utility.

ACKNOWLEDGEMENTS

This work has been partly funded by ESII, contract number 3000134902/TIN/21.

REFERENCES

Al-Humaigani, M., and D.B. Dunn. 2003. “A Model of Return on Investment for Information Systems Security.” In Circuits and Systems, 2003 IEEE 46th Midwest Symposium on, 1:483 –485 Vol. 1. doi:10.1109/MWSCAS.2003.1562323.

Arora, Ashish, Steven Frank, and Rahul Telang. 2008. “Estimating Benefits from Investing in Secure Software Development.” Build Security In.

Beautement, A., *et al.*, 2009. “Modelling the Human and Technological Costs and Benefits of USB Memory Stick Security.” In Managing Information Risk and the Economics of Security, edited by M. Eric Johnson, 141–63. Springer US.

Belton, Valerie, and Theodor J. Stewart. 2002. Multiple Criteria Decision Analysis: An Integrated Approach. Springer.

Beres, Yolanta, David Pym, and Simon Shiu. 2010. “Decision Support for Systems Security Investment.” Manuscript, HP Labs.

European Network and Information Security Agency (ENISA). 2012. “Introduction to Return on Security Investment : Helping CERTs Assessing the Cost of (lack Of) Security.”

Fülöp, János. 2005. Introduction to Decision Making Methods. Laboratory of Operations Research and Decision Systems. Computer and Automation Institute, Hungarian Academy of Sciences.

Gordon, Lawrence A., and Martin P. Loeb. 2002. “The Economics of Information Security Investment.” ACM Trans. Inf. Syst. Secur. 5 (4): 438–57. doi:10.1145/581271.581274.

Hausken, Kjell. 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 (5): 338–49. doi:10.1007/s10796-006-9011-6.

Holoman, Kathy, and Aaron Kuzmeskus. 2012. The Evolution of Return on Security Investment (ROSI). White Paper WP-SEC-SECURITY ROSI-A4.BU.N. EN.01.2012.0.01.CC. Schneider Electric.

Howard, R.A. 1968. "The Foundations of Decision Analysis." IEEE Transactions on Systems Science and Cybernetics 4 (3): 211 –219. doi:10.1109/TSSC.1968. 300115.

Ioannidis, C. *et al.,* 2009. "Investments and Trade-Offs in the Economics of Information Security." In Financial Cryptography and Data Security, edited by Roger Dingledine and Philippe Golle, 148–66. Lecture Notes in Computer Science 5628. Springer Berlin Heidelberg.

Keeney, Ralph L., and Howard Raïffa. 1976. *Decisions with Multiple Objectives: Preferences and Value Tradeoffs*. Wiley.

Keeney, Ralph L, and Howard Raiffa. 1993. Decisions with Multiple Objectives : Preferences and Value Tradeoffs. Cambridge [England]; New York, NY, USA: Cambridge University Press.

Keeney, Ralph Lyons. 1975. Examining Corporate Policy Using Multiattribute Utility Analysis. IIASA.

Korostoff, Kathryn. 2003. "The ROI of Network Security." Network World. http://www.networkworld. com/techinsider/2003/0825techinsiderroi.html.

Levy, Jason. 2005. "Multiple Criteria Decision Making and Decision Support Systems for Flood Risk Management." Stochastic Environmental Research and Risk Assessment 19 (6): 438–47. doi:10.1007/ s00477-005-0009-2.

Løken, Espen. 2007. "Use of Multicriteria Decision Analysis Methods for Energy Planning Problems." Renewable and Sustainable Energy Reviews 11 (7): 1584–95. doi:10.1016/j.rser.2005.11.005.

Pontes, Elvis, Adilson E., Anderson A. A. Silva, and Sergio T. 2011. "A Comprehensive Risk Management Framework for Approaching the Return on Security Investment (ROSI)." In *Risk Management in Environment, Production and Economy*, edited by Matteo Savino. InTech. http://www.intechopen.com/ books/risk-management-in-environment-production-and-economy/a-comprehensive-risk-management-framework-for-approaching-the-return-on-security-investment-rosi-.

Pricewaterhouse Cooper. 2014. "2014 Information Security Breaches Survey." *PwC.*

Raïffa, Howard, and Robert Schlaifer. 1961. Applied Statistical Decision Theory. Division of Research, Graduate School of Business Adminitration, Harvard University.

Rudolph, Manuel, and Reinhard Schwarz. 2012. "A Critical Survey of Security Indicator Approaches." In 2012 Seventh International Conference on Availability, Reliability and Security (ARES), 291 – 300. doi:10.1109/ARES.2012.10.

Shah., N.H., R.M. Gor, and H. Soni. 2007. Operations Research. PHI Learning Pvt. Ltd.

Sonnenreich, W. 2006. "Return on Security Investment (ROSI): A Practical Quantitative Model." Journal of Research and Practice in Information Technology 38 (1).

Von Neumann, J, and O Morgenstern. 1947. Theory of Games and Linear Programming. 2nd Edition. New York: Wiley.

Yin, Robert K. 2009. Case Study Research: Design and Methods. 4th ed. Applied Social Research Methods, v. 5. Los Angeles, Calif: Sage Publications.

Yoon, K. Paul, and Ching-Lai Hwang. 1995. *Multiple Attribute Decision Making: An Introduction*. SAGE.

Zeleny, Milan. 1982. Multiple Criteria Decision Making. New York [etc.]: McGraw-Hill.

Zhang, Jin-Ping, and Shou-Mei Li. 2005. "Portfolio Selection With Quadratic Utility Function Under Fuzzy Environment." In Proceedings of 2005 International Conference on Machine Learning and Cybernetics August 18-21, 2005, Ramada Hotel, Guangzhou, China, 2529–33. Piscataway, NJ: IEEE.