Economic Valuation for Information Security Investment: *A Systematic Literature Review*

Daniel Schatz[1] and Rabih Bashroush[2*]

[1] Thomson Reuters, London, UK; email: Daniel.schatz@thomsonreuters.com

[2] University of East London, UK; email: r.bashroush@qub.ac.uk

Abstract – Research on technological aspects of information security risk is a well-established area and familiar territory for most information security professionals. The same cannot be said about the economic value of information security investments in organisations. While there is an emerging research base investigating suitable approaches measuring the value of investments in information security, it remains difficult for practitioners to identify key approaches in current research. To address this issue, we conducted a systematic literature review on approaches used to evaluate investments in information security. Following a defined review protocol, we searched several databases for relevant primary studies and extracted key details from the identified studies to answer our research questions. The contributions of this work include: a comparison framework and a catalogue of existing approaches and trends that would help researchers and practitioners navigate existing work; categorisation and mapping of approaches according to their key elements and components; and a summary of key challenges and benefits of existing work, which should help focus future research efforts.

Keywords – Information Systems; Information Security; Econometrics; Return on Security Investment; Systematic Literature Review; Managerial risk accounting.

* Corresponding Author: Dr Rabih Bashroush, University of East London, 4-6 University Way, London E16 2RD, UK; Phone: +44 208 223 6515; email: r.bashroush@qub.ac.uk.

1 Introduction

The security of information assets in organisations has been a research subject for many years (Badenhorst and Eloff, 1990, Loch et al., 1992, Blakley et al., 2001, Siponen and Oinas-Kukkonen, 2007) largely focusing on technology and technological risks. While there has been early research on the economic impact of information security risks (Ekenberg et al., 1995), academic research was rather limited until the turn of the millennium when papers by Anderson (2001) as well as Gordon and Loeb (2002) raised interest in this topic. This effort is closely aligned with research in the fast moving area of information security risks in general, which represents a challenging problem on its own right (Hoo, 2000). The situation presents a dilemma as understanding the risks involved in an investment is a key requirement to assessing the expected benefits of the investment; as Hertz (1979) states "... *the courage to act boldly in the face of apparent uncertainty can be greatly bolstered by the clarity of portrayal of the risks and possible rewards.*"

This led to a situation where security professionals tasked with the protection of information assets have to justify security investments with little access to widely adopted financial methods. This is due to the lack of a tangible return on investment since security measures aim to reduce loss and not commonly generate revenue. The result is a battle on various fronts. It involves the challenge of understanding what the current and future threats to the organisations' information assets are; prioritising those with the highest probability to be realised on the highest valued assets; and investigating appropriate countermeasures. Not only this is a highly complex undertaking based on estimates and assumptions, it is merely the preamble to a budget approval process. The security professional is faced with the challenge of transforming the identified risks into financial formulas to justify the investment in controls by showing value and priority (e.g. compared to other projects within the organisation competing for the same pot of money).

1.1 Background

Gordon and Loeb (2006) found limited evidence of the effectiveness of a cost-benefit approach in organisations but conclude "*However, on the open-ended questions, a few respondents noted the budgeted expenditure level on information security for their firms is largely driven by such items as the past year's budget, best practices in the industry, or a mustdo approach.*" Along similar lines, Hoo (2000) argues that decisions favour security only when the security advocate commands significant respect from senior management. Likewise, Moore et al. (2015) found that in certain situations calculating return on investment (ROI) is feasible, even helpful, while in other cases it is not an appropriate measure. Wood and Parker (2004) went a step further and advise against using traditional financial analysis arguing that it is difficult and counterproductive to try to apply these in the context of information security. On the other hand, investment decisions in security based on anecdotal evidence tend to backfire as security measures have a tendency to look like redundant outlay, whether they work (the lack of loss events impacts value perception of the protective measure) or not (loss occurs despite the investment). This is clearly not an ideal situation for a rapidly maturing Information Security profession. It may even raise questions about the ability of the Chief Information Security Officer (CISO) properly doing the job or, in worst case, calls for an audit to verify whether security budgets may be misappropriated (Gordon et al., 2008). Even in absence of malice or incompetence is budget allocation a cause of tension; Srinidhi et al. (2015) find that managers over-invest in specific security-enhancing assets to reduce security breaches during their tenure as it is in their best interest. Herath and Herath (2014) discuss this classical agency issue in more detail and provide guidance allowing firms to decide whether it is worthwhile to conduct an IT security audit.

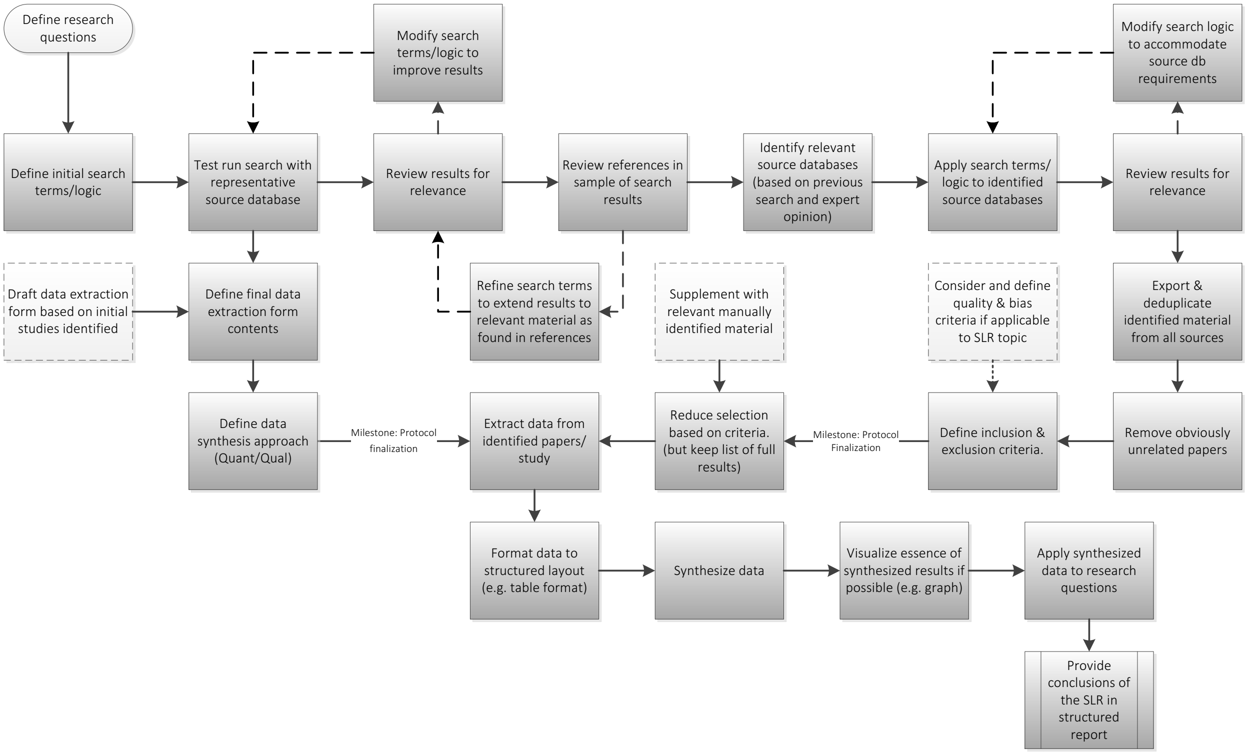
An ever increasing amount of research activity in the information security field at large makes it difficult to identify relevant research addressing the value challenge. Although various works have provided preliminary views on the topic (Kesswani and Kumar, 2015, Neubauer and Hartl, 2009, European Network and Information Security Agency, 2012, Eisenga et al., 2012), with some providing some detailed analysis (Demetz and Bachlechner, 2013, Huang and Behara, 2013), they tend to fall short of providing a comprehensive view of the literature, using a rigour approach.

In this work, we conduct a systematic literature review to identify and analyse the state-of-the-art. The paper will: provide guidance to practitioners looking to understand the current state of research; provide researchers in the field with an overview of the directions previous work has taken; and provide newcomers to this area with a good understanding of the state-of-the-art in economic assessment of information security investments in organisations.

The rest of the document is structured as follows. In section 2 the research methodology is discussed. This includes the study's research questions, search protocol as well as inclusion and exclusion criteria. Section 3 provides the data extraction and synthesis process of the primary studies identifying trends and developments in the field. Based on the data collected, the research questions are then addressed in detail in the remainder of section 3. Section 4 looks at the wider perspective of our work, section 5 discusses possible study limitations and threats to validity. Lastly, section 6 rounds off the paper with summary and conclusions.

2 Systematic Literature Review research method

Pursuing the objectives of this study, a Systematic Literature Review (SLR) approach was adopted. Systematic Literature Reviews provide a structured method for critically examining, interpreting and evaluating the entirety of current research evidence in a certain field or area leveraging a strict framework and predefined questions. For this paper, we follow guidance provided by Kitchenham and Charters (2007), Brereton et al. (2007), Biolchini et al. (2005) as well as Cronin et al. (2008) and note challenges and limitations as explained in section 5. A multiple step approach that resembles the phases described by Kitchenham and Charters (2007, p. 6) was followed to conduct the review. To aid the process, a high level flowchart was created during the protocol definition phase (Figure 1).



Define research questions
Modify search terms/logic to improve results
Modify search logic to accommodate source db requirements
Define initial search terms/logic
Test run search with representative source database
Review results for relevance
Review references in sample of search results
Identify relevant source databases (based on previous search and expert opinion)
Apply search terms/ logic to identified source databases
Review results for relevance
Draft data extraction form based on initial studies identified
Define final data extraction form contents
Refine search terms to extend results to relevant material as found in references
Supplement with relevant manually identified material
Consider and define quality & bias criteria if applicable to SLR topic
Export & deduplicate identified material from all sources
Define data synthesis approach (Quant/Qual)
Milestone: Protocol finalization
Extract data from identified papers/ study
Reduce selection based on criteria. (but keep list of full results)
Milestone: Protocol Finalization
Define inclusion & exclusion criteria.
Remove obviously unrelated papers
Format data to structured layout (e.g. table format)
Synthesize data
Visualize essence of synthesized results if possible (e.g. graph)
Apply synthesized data to research questions
Provide conclusions of the SLR in structured report

Figure 1 - Systematic Literature Review workflow

2.1 Research questions

As shown in Figure 1, the SLR process starts with the definition of the research questions the study aims to answer. For this study, the following research questions were identified:

RQ 1	**What approaches are described in the literature to support decision processes for information security investments (in organisations) taking economic factors into consideration?**
	The intention is to understand which approaches are proposed to value information security investments inside organisations.
RQ 2	**Are there any common key elements across the identified approaches?**
	The intention is to understand whether there are any common elements or factors covered by the different identified approaches.
RQ 3	**What are the main issues faced by these approaches as reported in the literature?**
	The assumption is that no approach is perfect, hence, under this question we try to capture issues and limitations as reported by the authors.
RQ 4	**Who is publishing on this topic?**
	The intention is to understand the size and distribution of the research community.
RQ 5	**Is there any tendency towards the use of a specific approach?**
	The aim is to find out whether there are any favoured approaches when it comes to economically valuing information security investments in organisations.

Table 1- Review questions

2.2 Search construction

To capture relevant material, the search has been constructed with inspiration by Beecham et al. (2006) as well as further modifications to accommodate the requirements of this particular systematic literature review. The selection of keywords was based on a review of key relevant papers in the field and the authors' experience. Over the course of the protocol development phase, these keywords were refined based on preliminary search results. Test searches conducted led to the identification of more potential keywords (e.g. Return on Investment, ROI, Net Present Value, NPV…); However, these were not used to avoid potential bias based on too narrow search terms in an already sparsely researched field. Additionally, the preliminary search results with these keywords did not noticeably improve or return additional relevant material. The search has been constructed based on the keywords shown in Table 2.

Keyword list
Information Security, IT Security, InfoSec, investment, investing, economy, cost, benefit, finance, spending, analysis, analyse, analyze, framework, model, decision, justification

Table 2 - Keyword list

The keywords were relationally grouped and each group linked using Boolean logic. Clustering of terms in groups was done to allow for reduction of search strings as groups form relevant compound nouns (e.g. InfoSec investment framework). Search terms were shortened by use of wildcard (asterisk) where possible and sensible. For example - use of asterisk search with 'invest*' did not just return 'investment' and 'investing' but also 'investigation' and 'investigating' which is commonly used in relation to Computer Science but less useful in this context.

Group 1	“Information Security” OR “IT Security” OR InfoSec
Group 2	Investment OR investing OR econom* OR (cost AND benefit) OR finance* OR spend*
Group 3	Analy* OR framework OR model OR decision OR justification

Table 3 - Search groups

The search construct was tailored to suit each of the source databases following the specific search requirements / syntax of the database provider as described in Table 5.

2.3 Search scope

The search mainly utilised electronic databases to identify relevant literature. Source databases were considered based on their relevance to the field of computer science and information security. To return results from the databases mentioned in Table 4, the search function provided by each website was used.

Source	Description
EBSCOhost	http://www.ebscohost.com
Web of Knowledge	http://apps.webofknowledge.com/
ScienceDirect	http://www.sciencedirect.com
IEEE_Xplore	http://ieeexplore.ieee.org/Xplore/

Table 4 - Source databases

2.4 Inclusion and Exclusion criteria

The initial results obtained through the search process were further filtered based on the inclusion and exclusion criteria below.

Inclusion:

- **IC1**: Papers and studies investigating approaches and metrics supporting economic decision processes as it pertains to information security investments in organisations
- **IC2**: Papers and studies are available in English or German language

Exclusion:

- **EC1**: Papers and studies investigating largely or exclusively non-economic approaches of information security (e.g. purely risk or technology based)
- **EC2**: Short papers, articles or studies which do not provide sufficient new insights or ideas
- **EC3**: Papers, articles or studies that are not peer reviewed (e.g. white papers)

Where multiple papers were identified utilizing the same or very similar approach, the most representative paper (favouring the more detailed and more recent publications) was selected unless there were other major contributions reported in other papers to warrant inclusion (e.g. additional arguments supporting an approach). All search terms have been designed to capture papers and studies published in English; however, publications in German have been considered and included if returned as a search result or found as a relevant reference in a paper.

The selection process entailed applying the inclusion and exclusion criteria to the title and abstract of the paper. Where this proved inconclusive, the paper was retrieved in full and reviewed.

2.5 Search process implementation

Following the SLR framework as described in Figure 1, the search and extraction process was conducted as below:

1. Define search terms and logic appropriate for the individual databases
2. Review raw results and reduce by removing obviously unrelated material
3. Export search results to reference management solution (Thomson Reuters Endnote)
4. Create subfolders for each database searched and move imported references accordingly
5. Remove duplicate papers based on author(s), year, title and reference type ignoring spacing and punctuation (Endnote functionality)
6. Apply selection criteria and move selected papers in new subfolder
7. Retrieve full paper for data extraction
8. Review references in selected studies for further relevant material

2.6 Search results

The search for papers was conducted following the protocol defined earlier. Due to differences between databases, some modifications to the search string were necessary to optimise the search results. The search construct unique to each database is shown in Table 5. Some databases provided additional refinement options that were leveraged as described in the comments section.

Source	Search details	Comments	#	Date
EBSCOhost	("information security" OR "IT Security" OR InfoSec) N90 (investment OR investing OR econom* OR cost OR benefit OR spend*) AND (analysis OR analyse OR analyze OR model OR framework OR decision OR justification)	*(Business Source Complete, Communication & Mass Media Complete, Library, Information Science & Technology Abstracts with limiters applied - Scholarly (Peer Reviewed) Journals)*	143	2014-07-03
Web of Knowledge	(("information security" OR "IT Security" OR InfoSec) NEAR ((investment OR investing OR econom* OR (cost NEAR benefit) OR spend*) NEAR (analysis OR analyse OR analyze OR model OR framework OR decision OR justification)))	*Refined by: Research Areas=(COMPUTER SCIENCE OR BUSINESS ECONOMICS OR INFORMATION SCIENCE LIBRARY SCIENCE OR OPERATIONS RESEARCH MANAGEMENT SCIENCE)* *Timespan=All Years.* *Search language=English, German* *Search scope was set to 'Topic' which includes Title, Abstract, Author Keywords and Keywords Plus®*	263	2014-07-04
ScienceDirect	("information security" OR "IT Security" OR InfoSec) W/10((investment OR investing OR econom* OR cost OR benefit OR spend*) W/10(analysis OR analyse OR analyze OR model OR framework OR decision OR justification))	*[Journals(Business, Management and Accounting,Computer Science,Economics, Econometrics and Finance)]*	281	2014-07-05
IEEE_Xplore	("Abstract":(Security OR InfoSec) NEAR (investment OR economic OR cost OR benefit OR spend) AND (analysis OR analyse OR analyze OR model OR framework OR decision OR justification))	Metadata	92	2014-07-06

Table 5 - Search constructs and results

After removing obviously unrelated papers by conducting a one pass review of the raw search results as seen in Table 5 the count of papers was reduced from 779 results found by the search construct down to 270 papers of potential relevance. These were distributed across the databases as per Table 6.

Source	Initial paper selection
EBSCOhost	105
Web of Knowledge	139
ScienceDirect	25
IEEE_Xplore	1

Table 6 - Overview of initial paper selection

Please note that having one paper attributed to the IEEE_Xplore database in Table 6 does not necessarily mean that there were no other IEEE published papers on the topic but indicates that there was only one study that was not returned by the other sources.

For the next step the results across all four databases were further consolidated and duplicate references manually checked and removed which reduced the reference count further to 261.

The selection process of the papers to be considered for data extraction included a manual step exporting the initial selection to Microsoft Excel for easier handling. Each paper has been listed with a unique ID and reference information exported from EndNote. According to the defined inclusion criteria in section 2.4 a '*single reviewer - two pass*' review was conducted to decide whether to include a paper in the review (Yes), exclude it (No) or review it in more detail (additional research required [ARR]) before making the decision. Further information was added to the fields 'Duplicate' (if the paper is a duplicate which was not identified as such by EndNote) and 'Comment' where required. The field 'Included' is defined as Boolean and either identifies the paper as included (Y) or not included (N) for the data extraction phase. After completion of this process, 22 papers were selected for data extraction. Examination of the references listed in the selected papers resulted in an additional five papers identified to be relevant. Three of these were selected for data extraction bringing the total number of primary studies to 25.

3 Data extraction and synthesis

The data extraction process was conducted on 25 papers as described in section 2.6. Table 7 lists all extracted details under various headers, as follows:

- 'ID' represents a unique numeric identifier assigned to each primary study
- 'Reference' provides the citation of the paper
- 'Publication outlet' provides information on the publication outlet where the primary study was published
- 'Approach' provides a short description of the area of research as reported in the primary study
- 'Approach details' provides a short description of the approach itself as highlighted in the primary study
- 'Key elements' lists the key elements of the approach as reported in the primary study
- 'Reported benefits' lists the approach advantages as reported in the primary study
- 'Reported challenges' lists the approach challenges as reported in the primary study

ID	Reference	Publication outlet	Approach	Approach details	Key elements	Reported benefits	Reported challenges
13	Arora et al. (2004)	IT Professional	Risk-based return on investment	RROI measures how effectively resources are used to avoid or reduce risk	• Net bypass rate for all security solutions • Incident risk, residual risk and baseline scenario	• Easier to use than Net Present Value (NPV) • Appropriate for identifying amount of investment	• Not appropriate to compare value between alternative solutions • Obtaining true cost (observed damages) • Estimating bypass rates • Interaction impact between deployed solutions • Representing catastrophic losses
23	Bistarelli et al. (2007)	Formal Aspects in Security and Trust	Strategic games on defence trees	Game theory strategies based on defence trees enriched with economic indexes as payoffs (utility)	• Return on Security Investment (ROSI) • Return on Attack (ROA) • Defence trees	• Identification of security countermeasure investment level up to marginal returns boundary	• Lack of reliable statistical data to use in a quantitative analysis • Ambiguity around calculation for the 'Risk Mitigated' attribute
28	Bodin et al. (2005)	Communications of the ACM	Analytic Hierarchy Process	Using the ratings method variant of the AHP to determine optimal budget allocation for maintaining	• AHP criteria tree • Fixed budget	• Supports multi-criteria decision problems involving both quantitative and qualitative criteria	• Does not consider quantitative concerns • Strong dependency on proper criteria definition and weighting

				and enhancing security		• Valuable tool for decision making and option ranking	
31	Bojanc and Jerman-Blažič (2008)	International Journal of Information Management	Combined use of multiple indexes	Calculating multiple indexes for each investment option and consolidate the results for decision support.	• Risk metrics • Return On (Security) Investment • Net Present Value • Internal Rate of Return	• IRR is particularly useful for multi-year investments • NPV describes cash value of expected returns	• Each index used individually does not present an appropriate solution. • ROI/IRR are not project magnitude indicator • ROI does not consider the time value of money
41	Cavusoglu et al. (2004).	Communications of the ACM	Game tree based on solution quality parameters	Game theory strategies based on security solution quality parameters in terms of risk mitigation	• Damage cost estimate • Mitigation quality parameters • Threat parameter estimates	• Understand how parameters affect optimal investment/cost • Assess marginal effect of decrease or increase of one parameter on total cost.	• Uncertainty on parameter estimates used for the model
43	Cavusoglu et al. (2008)	Journal of Management Information Systems	Decision-Theoretic and Game-Theoretic	Comparing results of sequential and simultaneous game theory approaches and decision theory approach	• Threat parameter estimates • Vulnerability parameter estimates • Sequential games • Simultaneous games • Strategy decisions	• Game theoretic approach achieves superior result over decision theory in most cases	• Uncertainty on parameter estimates used for the model, particularly for game theoretic approach • Game theoretic approach is assumed to be more complex • High levels of uncertainty reduce payoff's from game theory approach • Only relevant for targeted attack scenarios
54	Davis (2005)	Network Security	Practical Return on Security Investment	Set a policy defining the use of ROSI and adopt a consistent approach calculating it	• Cost of controls • Cost of incidents • Financial benefits • Definition/Policy when to use ROSI	• Clear view of value and benefits of security initiative • Making information security more accountable and transparent	• Quality of data estimates used for the model • Calculations can be too complex • ROSI is not well understood in businesses

80	Gordon and Loeb (2002)	ACM Transactions on Information and Systems Security	Optimal investment amount to protect a given set of information.	Leveraging information sets with security breach probability functions to calculate optimal investments in information security	• Breach loss • Threat probability • Vulnerability probability • Cost of control	• Considers how vulnerability and loss affect optimal security investment • Supports decision at what vulnerability level to focus investments • Provides upper limit for optimal investment	• Not intended to cover catastrophic events/loss • Uncertainty on threat, vulnerability and loss estimates • Principal/Agency cost not considered
95	Hausken (2006a)	Journal of Accounting and Public Policy	Income, interdependence, and substitution effects affecting incentives for security investment	Optimal strategies regarding security investment taking income effect, interdependence and substitution between attacker and defender as well as among defenders into consideration	• Asset value • Inefficiency factor • Attackers resources • Average levels of attack • Multi stage games	• Rate of return from security investment (Marginal Rate of substitution) • Appropriate investment based on identified attacker • Appropriate investment based on substitution & interdependence effect among firms	• Time factors not considered • Assumptions made on key parameters
99	Herath and Herath (2008)	Journal of Management Information Systems.	Real Options Analysis with Bayesian Post-audit	Real options model for information security investments using Bayesian inferences for valuation and post-auditing	• Total cost • Expected benefits • Volatility parameter	• (Bayesian) Revised parameter estimates lead to reduction of upward bias and the incorporation of up-to-date information • Reduces the possibility of a biased forecast • Shows how to integrate security-specific features properly in valuation • Incorporates available information into the decision-making process in a systematic manner.	• Focused decision theoretic approaches/situations • Focuses on technical dependence, not market dependence • Difficult to obtaining prior estimates of mean and standard deviation sample data
107	Iheagwara et al. (2004)	Information and Software Technology	Cascading Threat Multiplier tied into Return on Security Investment	Use a standard risk analysis framework and extend it by introducing the Cascading Threat Multiplier to arrive at accurate ROI calculations	• Asset Value • Exposure factor • Rate of occurrence • Underlying exposed assets • Secondary exposure factor	• Assists in formulate the analytical framework for asset valuation and risk calculations • A more comprehensive valuation methodology that includes intangible factors into AV variable calculation	• Cascading threat multiplier is ‘somewhat’ subjective

114	Jingyue and Xiaomeng (2007)	2007 International Conference on Software Engineering Advances	Real option theory	Apply the real option theory to make right security investment decisions	• Binomial Options Pricing Model • Underlying volatility	• Comprehends uncertainty and responds to dynamics of business needs • When and how to implement in order to maximize the likelihood of desirable outcomes • Determines the most value-adding strategy	• Assumes profit-maximizing decisions • Key parameters need to be estimated or simulated based on historical data
123	Khansa and Liginlal (2009)	European Journal of Operational Research	Security Process Innovation incorporating real option theory	Model of invest-to-learn and switching options generated upon early investment in flexible SPI	• Volatility estimate • Intensity of malicious attacks • Switching cost • Binominal lattice	• Value definition of switching solutions decision • Invest-to-learn option	• Considers switching between only two solutions • Competitor impact not included in the model
165	Purser (2004)	Computers & Security	Total Return on Investment	Risk mitigation is included as factor in the Return on Investment calculation	• Revenue • Cost saving • Value of change in risk	• Includes the financial impact of the change in risk	• Requires strategic approach and careful planning • Must be business driven
186	Sheen (2010)	Proceedings of the 9th WSEAS International Conference on Instrumentation Measurement Circuits and Systems (IMCAS 2010). Instrumentation, Measurement, Circuits and Systems	Fuzzy Economic Decision-models	Net Present Value (NPV), and discounted Return on Investment (dRoI) models leveraging fuzzy values for cost-benefit analysis	• Triangular Fuzzy Numbers • Net Present Value • Discounted Return on Investment • Interest rate • Inflation rate • Operating cost/revenue	• Considers 'Opportunity cost of capital' • Eliminates the need for complicate sensitivity analysis studies associated with input parameter variations • Takes degree of confidence of the decision-makers' opinions into consideration	• n/a
191	Shirtz and Elovici (2011)	Information Management & Computer Security	Decision-support methodology for allocating information security remedies based on the end-effect perspective	Calculate the optimal subset of remedies for a given budget and the most cost-effective subset of remedies that comply with the organization's policy	• List of end-effects • Potential damage • Protection level for each end-effect • Cost and performance of remedies	• Does not use probabilities of undesired information security events • Comply with set budget constraints and the desired security level for each end-effect	• Only mutually exclusive end-effects considered

213	Tatsumi and Goto (2010)	Economics of Information Security and Privacy	Real Option Theory	Analytically modelling continuous real options applied to information security	• Volatility estimate • Drift factor • Total expected benefits • Intensity threat	• Guidance on investment timing	• Difficulties predicting threat timing/occurrence • Difficult to formulate attacker's objective function
237	Willemson (2010)	Proceedings of the Fifth International Conference on Availability, Reliability, and Security (ARES 2010)	Extending on Gordon & Loeb	Extending on G&L by restricting the class of possible remaining vulnerability functions and generalize by stating simple functional constraints	• Gordon and Loeb model	• New family of remaining vulnerability functions satisfying all conditions • Generalizing all the currently known example function families	• n/a
244	Yong Jick et al. (2011)	Decision Support Systems	Financial economics based value-at-Risk methods and operational risk modelling	Profit optimization model for customer information security investments based on value-at-Risk methods and operational risk modelling from financial economics.	• Value at risk • Profit at risk • Revenue • Total costs • Loss estimates	• Decision-making process using operational riskmanagement and value-at-risk methods in financial economics • Risk-return trade-offs for information security enhancement investments.	• Classes of risks that cannot be estimated (Black Swan) • Considers only quantity of added services, not cost • Uncertainty on estimates of the frequency and magnitude of future losses
252	Zikai and Haitao (2008)	2008 IEEE International Conference on Networking, Sensing and Control (ICNSC '08)	Flexible optimal IS investment strategy	IS risks are transformed into opportunity cost then a multi-object optimization model is build up based on opportunity cost and direct IS investment.	• Opportunity cost loss of C,I,A • Direct cost • Impact factor	• Helps to make more confident justifications for security spend	• Data loss is hard to estimate using equations • How to combine uncertainty in this model
254	Huang and Behara (2013)	International Journal of Production Economics	IS fixed budget investment allocation	Investment model defending against concurrent heterogeneous attacks taking budget constrains into consideration	• Breach probability based on scale-free networks concept • Potential loss of class • Cross-over coefficient	• Considers budget constrains • Incorporates concurrent attacks • Adopt concept of scale free networks • Considers cross over effects of investments	• Uncertainty on assumptions for variables & functions • Attack category classification can be imperfect • Total budget consumption

257	Capko et al. (2014)	2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)	Cash flow analysis & Internal rate of return	Practical application of cash flow analysis for information security solutions	• Initial investment • Opportunity cost of capital • EoL value & depreciation method • Tax considerations • Working capital considerations	• CFA model be used to calculate NPV, IRR and RoC	• Determining input parameters esp. avoided cost/damages • Cannot be used to analyse investment in multiple solutions
M1	Cremonini (2005).	n/a	Return-On-Attack (ROA)	Improve ROI-based evaluations by integrating them with index Return-On-Attack (ROA), aimed at measuring the convenience of attacks	• Attackers gain • Attackers efficiency (or EFF) • Cost of attack	• Identify solution that mostly discourage attackers in their intrusion attempts • Able to consider time factor	• n/a
M2	Faisst et al. (2007)	Zeitschrift für Betriebswirtschaft	Dynamic security investment calculation	Model offering decision support for dynamic security investment calculations based on Net Present Value considerations	• Reduction in expected damages • Reduction of opportunity cost • Operating cost • Interest rates	• Despite uncertainty of key factors a statement on investment benefits can be arrived at • Optimal time of investment • Takes budget and equity capital constraints into consideration	• Interdependency between security controls and assets not considered • Difficult to estimate frequency and scale of malicious events • Operational budget/cost not sufficiently considered
M4	Matsuura (2009)	Managing Information Risk and the Economics of Security	Extending on Gordon & Loeb by productivity spaces	Optimal security investment considering Gordon Loeb and productivity spaces (vulnerability and threat reduction)	• Gordon-Loeb model components • Security threat probability function	• Identify security investment based on value of productivities	• Failure in assessing the threat-productivity can lead to wrong choice • Uncertainty on estimates of key variables

Table 7 - Extracted data of selected papers

3.1 Result review question (1)

In the items listed under ‘Key elements’ as shown in Table **7** are those which were considered to be the important elements the primary study is highlighting, relying on or proposing as novel, crucial or providing key contributions to the respective approach. Likewise the items listed under ‘Reported Benefits’ are those which the primary study is listing as benefits particular to the proposed approach. Following the data extraction process we aligned each approach described in the primary study in nine high level approach categories. We summarized both, elements and benefits, into a wider elements category and repeated the same with the reported challenges. The categories were then used as basis to answer the research questions as defined in Table 1. Figure 2 shows a simple relationship diagram.

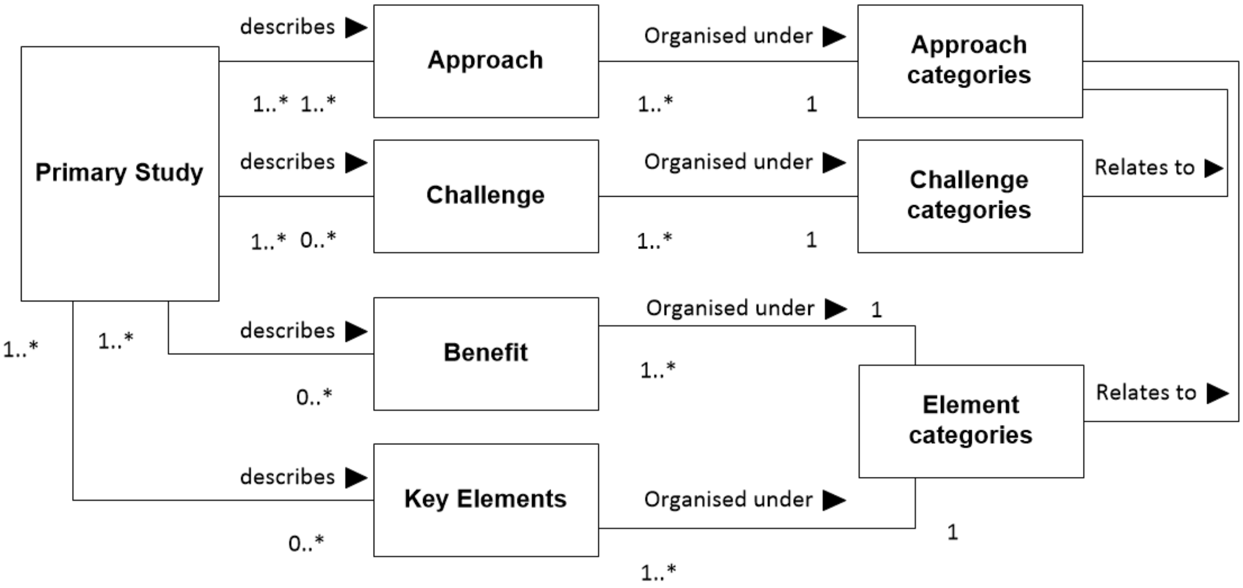


Figure 2 - Overview of extracted data and relations

Analysing the data extracted, it was clear that there were a number of approaches discussed in current research. Although fewer primary studies were identified than initially expected, the breadth of approaches covered was noteworthy. An attempt was made to categorise each paper according to its approach in top-level approach categories to be able to construct a simplified overview. After careful consideration nine top level approach categories were identified that accommodate the individual approaches described in the primary studies. These categories were assumed to strike a balance between being too constraining on the variety of approaches described in the primary studies and avoiding too many approach categories which would hinder a meaningful summarization. The nine approach categories are described in Table 8.

Approach category	**Description with reference**
AHP	The Analytic Hierarchy Process is a structured method to break down complex problems with the goal to aggregate sub problem solutions into a conclusion (Saaty, 1994).
DSS	Decision Support Systems present a structured method to understand and improve decision process and support the decision maker to make decisions more effectively. (Keen, 1980, Alavi and Henderson, 1981)
Game Theory	Game Theory describes the study of strategic decision making in situations of competition or conflict leveraging mathematical models. (Neumann and Morgenstern, 1964)
NPV	Net Present Value is a valuation formula that calculates the present value of future cash flows of an investment (Ross, 1995)
ROA	Return on Attack is an extension to Return on Investment where an attacker’s gain as well his cost (losses) are considered in the model. (Cremonini, 2005)

ROI	Return on Investment is a valuation formula that evaluates the efficiency of an investment based on cost and expected benefit. (Phillips and Phillips, 2010)
ROI, NPV	Papers which utilise a balanced mix of Return on Investment and Net Present Value to provide guidance on economic information security decisions
ROT	Real Options Theory describes a quantitative means to evaluate the flexibility inherent in the decision-making process (Miller and Park, 2002)
UM	Utility maximization describes a concept in which a subject attempts to derive the greatest possible value from an investment (Strotz, 1955)

Table 8 - Category explanation

In Table 9 an overview of the categorisation for each primary study is provided.

ID	**Author(s)**	**Year**	**Approach Category**
13	Arora, A., Hall, D., Piato, C. A., Ramsey, D., Telang, R.	2004	ROI
23	Bistarelli, S., Dall'Aglio, M., Peretti, P.	2007	Game Theory
28	Bodin, L. D., Gordon, L. A., Loeb, M. P.	2005	AHP
31	Bojanc, R., Jerman-Blažič, B.	2008	ROI, NPV
41	Cavusoglu, H., Mishra, B., Raghunathan, S.	2004	Game Theory
43	Cavusoglu, H., Raghunathan, S., Yue, W. T.	2008	Game Theory
54	Davis, A.	2005	ROI
80	Gordon, L. A., Loeb, M. P.	2002	UM
95	Hausken, K.	2006	UM

99	Herath, H. S. B., Herath, T. C.	2008	ROT
107	Iheagwara, C., Blyth, A., Kevin, T., Kinn, D.	2004	ROI
114	Jingyue, L., Xiaomeng, S.	2007	ROT
123	Khansa, L., Liginlal, D.	2009	ROT
165	Purser, S.A.	2004	ROI
186	Sheen, J.N.	2010	ROI, NPV
191	Shirtz, D., Elovici, Y.	2011	DSS
213	Tatsumi, K.-i., Goto, M.	2010	ROT
237	Willemson, J.	2010	UM
244	Yong Jick, L., Kauffman, R. J., Sougstad, R.	2011	DSS
252	Zikai, W., Haitao, S.	2008	DSS
254	Huang, C. Derrick, Behara, Ravi S	2013	UM
257	Capko, Z., Aksentijevic, S., Tijan, E.	2014	NPV
M1	Cremonini, M.	2005	ROA
M2	Faisst, U., Prokein, O., Wegmann, N.	2007	NPV
M4	Matsuura, K.	2009	UM

Table 9 - Category mapping by paper

Figure 3 shows how the approaches discussed in the 25 primary studies are mapped to nine approach categories.

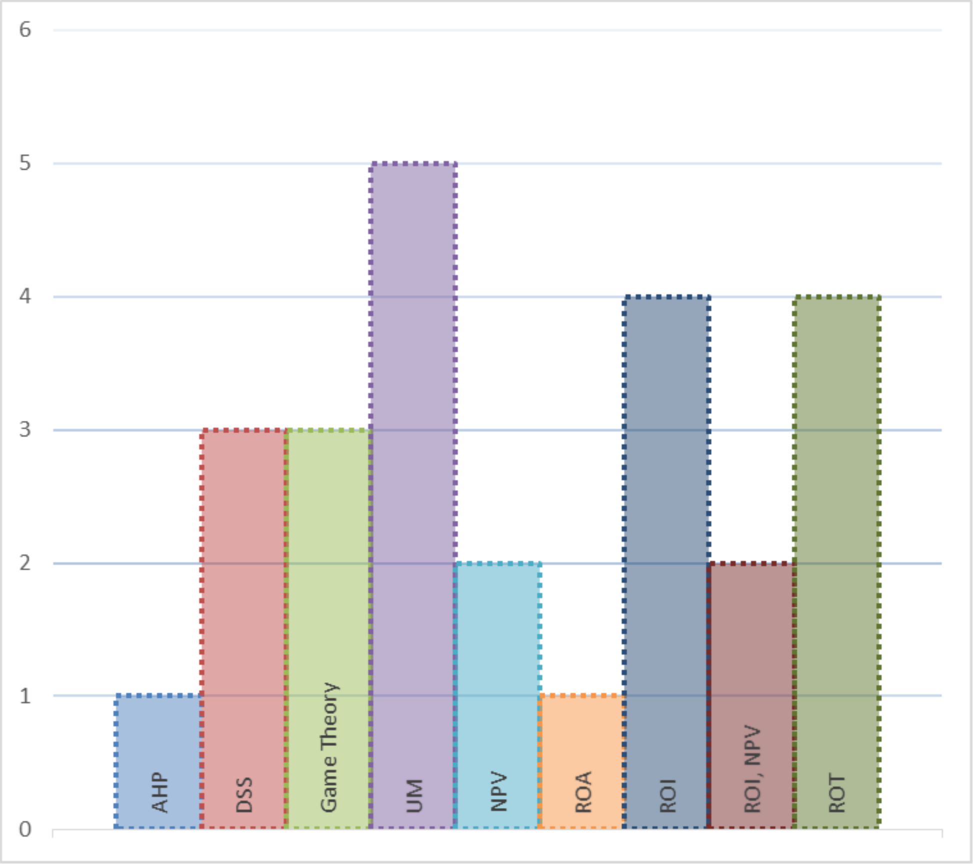


Figure 3 – Primary studies by category

Looking at the results we can conclude that the focus of unique approaches is on three main categories namely: Return on Investment (ROI); Real Options Theory (ROT); and Utility Maximization (UM). While solid representation of ROI and UM is no surprise the strong presence of ROT research was unexpected as we had considered this approach to be rather niche and more focused on financial market valuation rather than corporate investment decisions.

We also note that the majority of primary studies approached the problem from an academic perspective with focus on fundamental theories like utility maximisation, game theory or real option theory. This could be due to the selection criteria of SLRs which tend to exclude grey or non refereed literature (e.g. white papers, etc.). Yet, several papers discuss practical implementation and extensions of the primary approaches. Hausken (2006b) analyses different classes of information security breach functions in order to examine the robustness of the Gordon-Loeb model, which is recognised in this paper under the Utility Maximization approach. Gordon et al. (2015) extends the ROT approach by assessing the impact of information sharing at the example of a firm deciding on security investment timing. The authors find that sharing reduces a firm's uncertainty concerning a cybersecurity investment and decreases the value of the deferment option associated with the investment.

3.2 Result review question (2)

Overall, 90 key elements were extracted from the primary studies with several elements mentioned across multiple studies. To better understand which elements are considered key to this research topic we attempted to collate the individual elements into topical element categories. Table 10 provides a description for element alignment in each category.

Element category	**Description**
Benefit	Elements which have direct beneficial attributes like cost reduction, revenue or are explicitly described as benefit in the primary study
Cost	Elements which are a direct or indirect cost like operating cost, opportunity cost, switching cost, etc.
Function	Elements which are constructs like decision trees, mitigation quality parameters, fuzzy numbers, etc.
Impact	Elements that describe impact in context of the approach, like potential damage or list of end effects

Resource	Elements which are considered resources like fixed budgets, asset values or attacker resources
Threat	Elements which describe or measure threats in context of the approach, like threat probability, attackers efficiency or rate of occurrence
Volatility	Elements which are specifically described as volatility element in the primary study
Vulnerability	Elements which describe vulnerability in context of the approach, like exposure factor, vulnerability parameter estimates or bypass rate

Table 10 - Element category details

Table 11 goes into full detail on how the extracted elements for all papers are aligned with element categories.

Element category	**Elements**
Benefit	Cost saving (ROI), Expected benefits (ROT), Financial benefits (ROI), Interest rates (NPV, ROI), Reduction in expected damages (NPV), Reduction of opportunity cost (NPV), Revenue (DSS, ROI), Total expected benefits (ROT), Value of change in risk (ROI)
Cost	Cost and performance of remedies (DSS), Cost of attack (ROA), Cost of control (ROI, UM), Cost of incidents (ROI) , Damage cost estimate (GT), Direct cost (DSS), Inflation rate (ROI, NPV), Operating cost (NPV), Operating cost/revenue (NPV), Opportunity cost loss of C,I,A (DSS), Opportunity cost of capital (NPV), Potential loss of class (UM), residual risk (ROI), Switching cost (ROT), Total cost (DSS, ROT)

Function	AHP criteria tree (AHP), Baseline scenario (ROI), Binomial Options Pricing Model (ROT), Binominal lattice (ROT), Cross-over coefficient (UM), Defense trees (GT), Definition/Policy when to use ROSI (ROI), depreciation method (NPV), Discounted Return on Investment (ROI/NPV), Drift factor (ROT), Inefficiency factor (GT), Internal Rate of Return (ROI/NPV), Mitigation quality parameters (GT), Multi stage games (GT), Net Present Value (ROI/NPV), Protection level for each end-effect (DSS), Return On (Security) Investment (ROI/NPV), Return on Attack (GT), Risk metrics (ROI/NPV), Security threat probability function (UM), Sequential games (GT), Simultaneous games (GT), Strategy decisions (GT), Tax considerations (NPV), Triangular Fuzzy Numbers (ROI/NPV), Working capital considerations (NPV)
Impact	Attackers gain (ROA), Breach loss (UM), Impact factor (DSS), List of end-effects (DSS), Loss estimates (DSS), Potential damage (DSS), Profit at risk (DSS), Value at risk (DSS)
Resource	Asset value (GT, ROI), Attackers resources (GT), EoL value (NPV), Fixed budget (AHP), Initial investment (NPV)
Threat	Attackers efficiency (ROA), Average levels of attack (GT), Breach probability based on scale-free networks concept (UM), incident risk (ROI), Intensity of malicious attacks (ROT), Intensity threat (ROT), Rate of occurrence (ROI), Threat parameter estimates (GT), Threat probability (UM)

Volatility	Underlying volatility (ROT), Volatility estimate (ROT), Volatility parameter (ROT)
Vulnerability	Exposure factor (ROI), Net bypass rate for all security solutions (ROI), Secondary exposure factor (ROI), Underlying exposed assets (ROI), Vulnerability parameter estimates (GT), Vulnerability probability (UM)

Table 11 - Overview of elements and their use across approaches

Roughly a third of the elements are abstract constructs like decision trees, mitigation quality parameters, fuzzy numbers, etc. and have been included in the 'Function' element category representing the biggest section. Looking at the other categories, it shows that cost, benefit and threat are the main contributing factors as per our primary studies. This is not surprising as these are inherently linked to risk and value considerations in information security. Mapping these element categories to the reported approaches does reveal an even more interesting picture as Figure 4 shows.

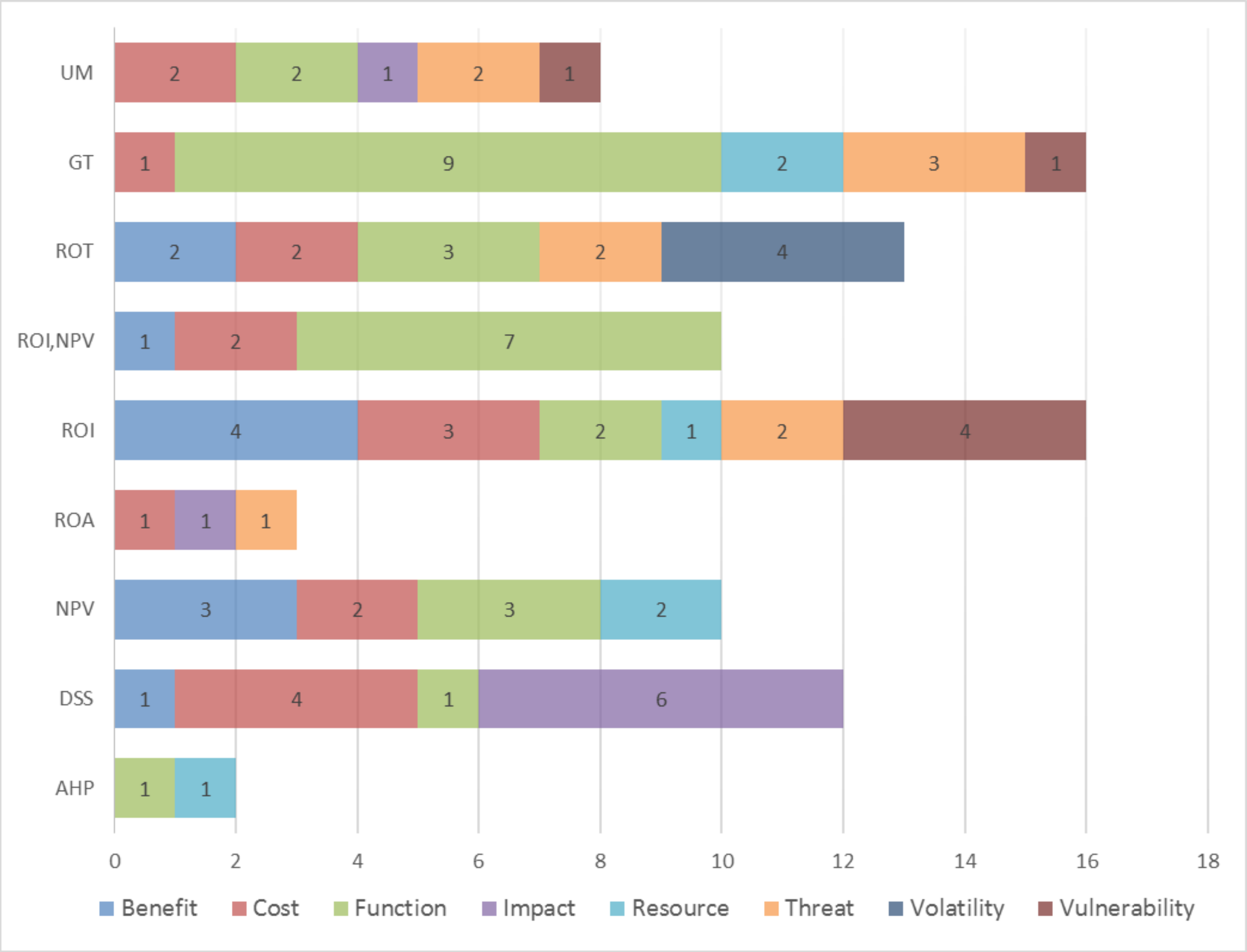


Figure 4 - Elements to approach category mapping

While any conclusion drawn here hinges on the chain of assumptions made up to this point (aligning primary studies with approach categories, extracting elements from the papers and aligning elements in element categories) the displayed breakdown intuitively makes sense. Both ROI and NPV show a strong reliance on benefit and cost factors whereas the 'ROI/NPV' and Game Theory have a high function element as they heavily focus on sub functions (ROI/NPV) and game strategies. Interestingly the Decision Support System (DSS) papers are driven by reasonably easily measurable factors cost and impact, which would appear to make a good candidate for real world implementation. We further note that 'Impact' has little mention as key element in primary studies other than in DSS and UM focused papers. The utility maximization

(UM) approach stands out due to its balanced distribution of elements which would speak for its usefulness to assess the true economic value of investments in this context but implicitly also carries all the complexities.

3.3 Result review question (3)

We noted 51 challenges reported by the authors in their papers. Similar to the key elements, challenges have been consolidated in (five) areas. Table 12 provides a description on how the reported challenges are mapped to challenge categories.

Challenge categories	**Description**
Accurate estimates	Challenges related to estimates of key parameters or inputs for the described method, like frequency of malicious events, loss magnitude or quality of estimates in general.
Complex to apply	Challenges related to the complexity of the method, like complex calculations, subjectivity, attacker function modelling, etc.
Constraint not considered	Challenges related to items specifically mentioned in the primary study as not being considered by the respective approach, like catastrophic loss or time factors.
Limited scenarios	Challenges related to limits in applicability as reported in the primary study, like limited to targeted attacks, unsuitable to compare more than two solutions, etc.
Real benefit	Challenges related to identification of real benefit of the approach

Table 12 - Challenge category details

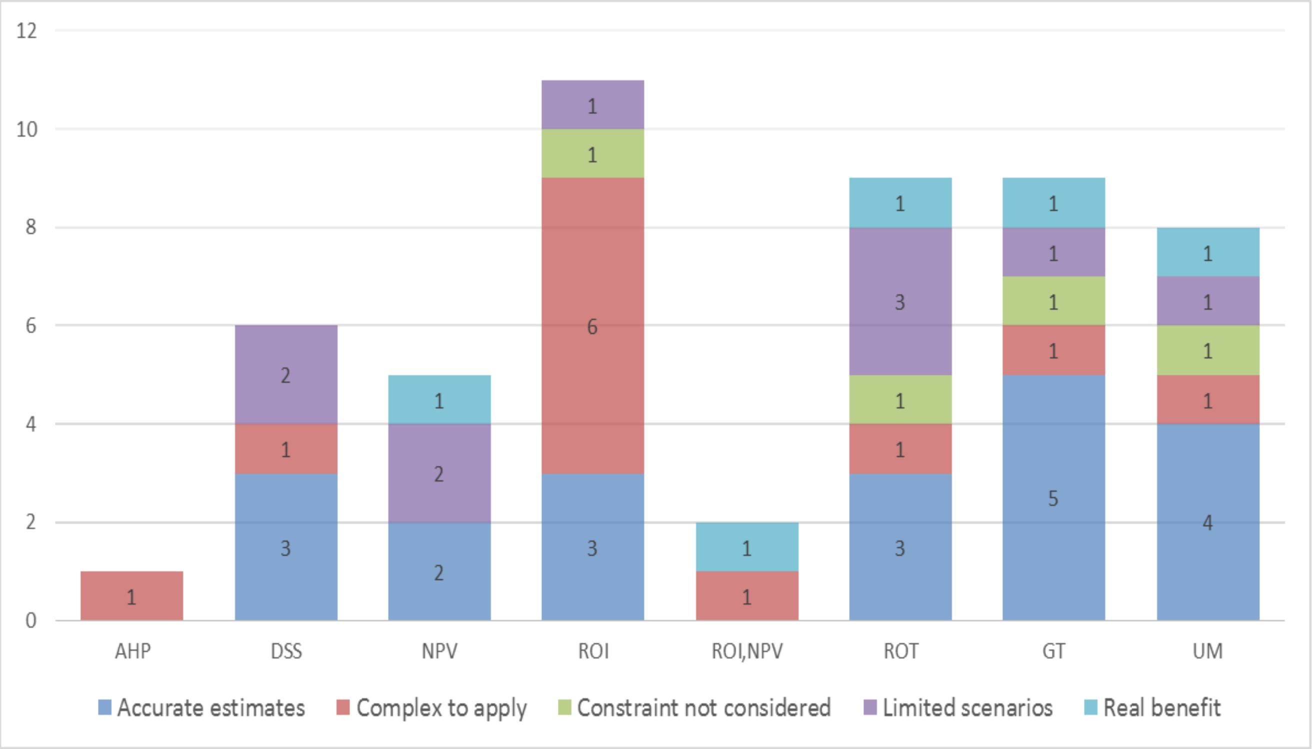


Figure 5- Challenges to categories mapping

While each approach category has its own challenges we see in Figure 5 that ‘Accurate estimates’ and ‘Complexity to apply’ are key challenges across most approaches. When interpreting this data it is important to note that a higher count of primary studies for a given approach is likely to produce an increased count of challenges for that approach. This is quite possible the reason why e.g. AHP shows a very low amount of challenges whereas GT or ROI show a wide range of challenges. It is interesting to observe that ROI lists complexity as key challenge which could be interpreted in a way that this approach may not scale well; alternatively, it could be argued that it is one of the most researched approaches and thus better understood in terms of challenges.

3.4 Result review question (4) and (5)

To understand whether research in this area is progressed by only a particular institution or region, or whether there is a wider research community, we looked at the authors of the primary studies. In addition, we obtained all authors and co-authors affiliations as well as their geographic location. As can be seen in Figure 6 there is a strong research base in the US (particularly out of Maryland and Texas) with notable contributions from Croatia, Italy, Norway, Japan, Germany and China. The strong presence of primary studies by US researchers is not a surprise as, according to the inclusion/exclusion requirements for this SLR, our results are biased by language. We cannot comment on whether there is a strong research community covering this topic publishing in languages other than English or German. It must also be noted that this data only answers the specific question set for our SLR, only considering primary studies fitting the strict criteria described in section 2.4. It does not consider supplemental or tangential papers published on this topic.

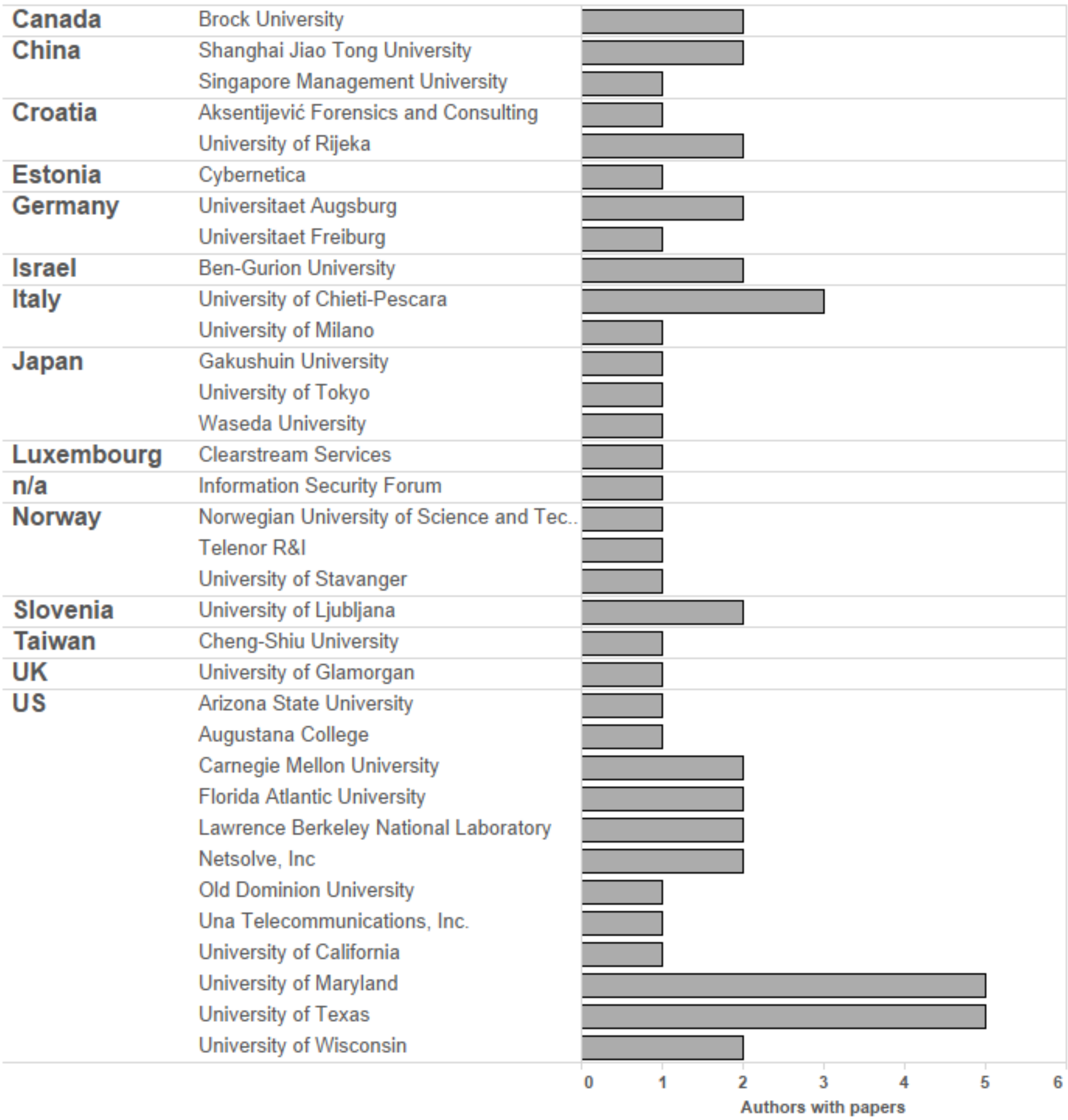


Figure 6 – Geographical distribution of primary studies

Lastly, to answer RQ5 on whether there is a trend towards a certain approach; based on our assessment of primary studies we were unable to identify a clear research trend. While utility maximization leads in publications on this topic, it certainly does not dominate the domain. The lack of novel ROI focused publications after 2005 is something of interest as it provides an indicator of the decline in original contributions to this research approach. Publications on ROT are mainly observed between 2007 and 2010 but we continue to see research activity in this area. Notably, Gordon et al. (2015) extend the ROT approach with the aspect of sharing cybersecurity related information among firms, thus addressing some of the reported challenges on this approach (such as difficulties predicting threat timing/occurrence and key parameters needing to be estimated or simulated based on historical data).

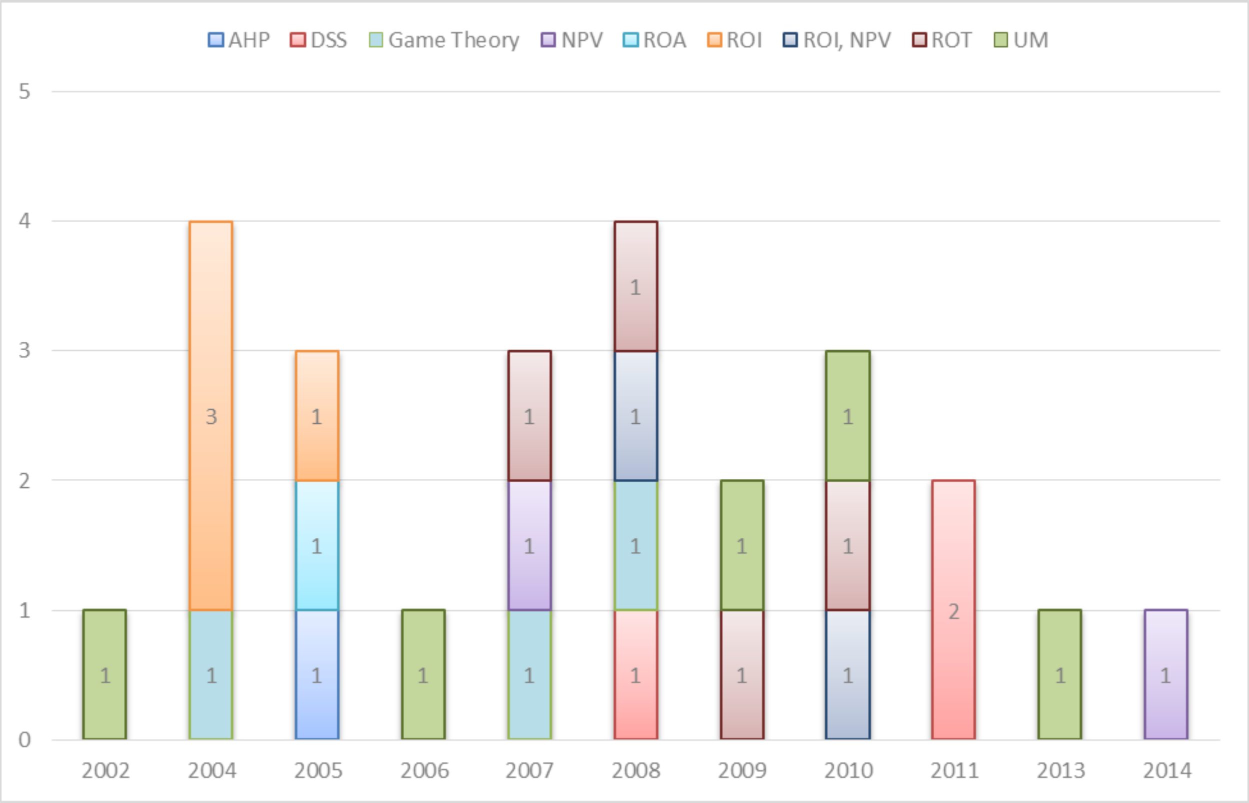


Figure 7 - Primary studies by year of publication

As the simple timeline of primary study by approach did not provide a very satisfactory answer to RQ5 we retrieved additional metadata in hope to arrive at a better indication of research trends. The intention was to understand the impact the primary studies and the approach they propose on other studies over time. We decided to look at citation count for each primary study based on data provided through Google Scholar due to its comprehensive citation coverage

(Meho and Yang, 2006). To support collection of citation data and calculation of metrics (cites_year) we utilized 'Publish or Perish' (Harzing, 2007).

Somewhat expected the citation count (absolute and average) is higher for papers published earlier on, particularly for the seminal paper by Gordon and Loeb (2002) [ID 80]. We generally observe that research on game theory and utility maximization provides a constant stream of cited papers over the years with a noticeable spike in 2008. Primary studies on other approaches appear to have a limited reach based on citation count which may indicate opportunities for further research; or simply point to a lack of interest in these areas. Again, no clear trend is observed but publication frequency and citation metrics point towards an ongoing interest in game theoretic approaches as well as general utility maximization research.

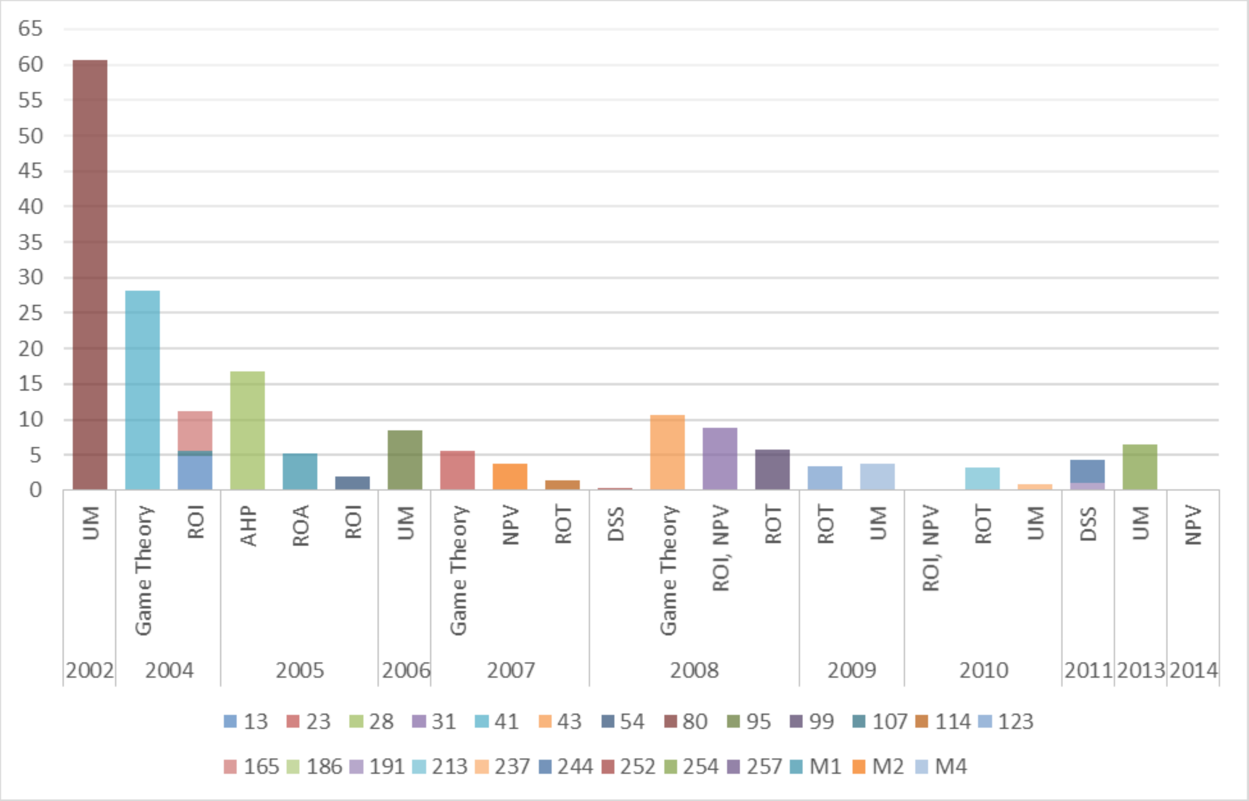


Figure 8 - Primary studies by publication year with average citations per year

4 The wider perspective

One of the advantages of the SLR process is that it helps focus the search process and ensures that relevant literature is captured in an unbiased way and using a repeatable process. However, it also means that some relevant wider literature is missed for not meeting the inclusion/exclusion criteria. In this section, we complement the SLR results by capturing the wider perspective to provide a more comprehensive view of the topic.

Gordon et al. (2015) emphasises the importance for firms to understand the process by which they can derive the most efficient allocation of their cybersecurity-related resources. This is now an widely accepted challenge and research on options to understand and address this gap is well underway (Gordon et al., 2003, Hausken, 2007, Dengpan et al., 2011). Recent efforts in knowledge and information sharing, as it pertains to cyber security, try to improve the defenders position by enhancing the collective knowledge on tools, techniques and procedures (TTP) of threat actors. Despite the collective benefits of moving towards a complete information game from a defender's perspective, firms are slow to adopt. Some antitrust concerns aside (Department of Justice, 2014), the main challenge to overcome is that of free-riding; quasi the tragedy of the cyber sharing commons. It is in the best interest of firms to consume, but not necessarily share, cyber intelligence to improve their security position. This potentially redirects attackers to other firms, and therefore, reduces the other firm's contest success (Hausken, 2007). With little market incentive to move away from such practices, governments are starting to encourage organisations to do 'the right thing' by applying a Thaler and Sunstein (2003) libertarian paternalism approach as evidenced in the US Cybersecurity Information Sharing Act of 2015 (The White House, 2015, Cybersecurity Information Sharing Act of 2015, 2015).

The question remains as to what the working approaches and strategies are for information security investments. In their empirical study, Rowe and Gallaher (2006) introduce a conceptual approach to consider the trade-offs between various investment and implementation strategies. Their conclusion provides a macroeconomic view stating that policy makers and organizations would benefit from a robust analysis of the difference between the social and the private costs of cyber security. Although not an empirical study, the model proposed by Bojanc and Jerman-Blazic (2012) provides an interesting approach for the evaluation of investments in security based on quantitative analysis of security risks. The authors evaluate the profitability of security measures based on ROI, NPV and IRR using the output to compare individual measures with each other. Gordon and Loeb (2006) describe their findings of an empirical study they conducted among S&P 500 firms. They conclude that there seems to be a movement towards using more economic analysis in evaluating information security activities. Based on the study, a particular interest in NPV can be seen, but they also note that budgeted expenditure level on information security is largely driven by such items as past year's budget, best practices in the industry, or a must do approach. Wei et al. (2007) conducted an empirical analysis of information-security investments surveying Japanese enterprises in context of vulnerability levels related to computer virus incidents. Taking the number of security measures as a proxy variable of security investment, they confirm that the effects of information security investment contribute to the reduction of relevant vulnerability levels.

An alternative approach to the issue would be to considering risk transfer options as provided by cyber insurance. Miaoui et al. (2015) propose to distribute investments between controls to protect against security attacks; insurance to transfer the residual risk of loss; and forensic readiness to maximise capability to collect digital evidence. The authors consider the interdependence of the investment strategies of their model when computing the optimal total investment. Mukhopadhyay et al. (2013) propose a way to assist firms to decide on the utility of cyber-insurance products and to what extent they can use them. The authors discuss using Copula based Bayesian Belief Networks to assess and quantify cyber-risk as decision support for using cyber insurance products as risk management tool. This is related to previous work by Herath and Herath (2011) who describe a copula-based simulation for determining the annual net premiums for cyber-insurance policies adopting an empirical approach using Archimedean copulas.

5 Study limitations and threats to validity

This section discusses the limitations of the study and threats to validity. This study suffers from limitations inherent to SLR as described by Kitchenham and Charters (2007). This includes limitations on search comprehensiveness and material selection. Due to the volume of papers returned and analysed, there is always the possibility that the study might have missed a relevant paper (due to an error or oversight) at any of the different stages of the search process. However, given the way the research questions were designed, and the way the analysis is based on a set of papers, the impact of any such potential omissions on the study findings and conclusions should be limited.

While the search terms were carefully crafted, search term definition is a potential limitation to the study as relevant papers might have been missed. This is particularly true for papers not published in English. To mitigate this weakness, forward and backward reference checking was conducted on key publications to identify any potentially missed studies. As is custom with SLRs, for papers to be considered as primary studies, they have to be published in a peer-reviewed outlet. This put further restrictions on the selection process as material published for example as white papers (which is common in industry) could not be selected.

6 Conclusion

This systematic literature review aimed to answer questions related to economic information security decision-making processes. Following standard SLR processes we identified 25 highly relevant papers describing approaches supporting decision processes for information security investments taking economic factors into consideration. We aligned the reported approaches into nine categories and identified research in utility maximization, game theory and real options theory to be areas where novel ideas are prevalent. We extracted key elements for each primary study as mentioned by the authors and collated the individual elements into element categories. Based on this we analysed which elements authors consider most relevant for their approaches and found both ROI and NPV to show a strong reliance on 'Benefit' and 'Cost' elements whereas Game Theory has a high reliance on' Function' elements due to its focus game strategies. We further noted that the Decision Support System (DSS) studies are driven by readily measurable elements 'Cost' and 'Impact'. Many of the primary studies discuss challenges pertaining to their approach which we also extracted and summarized; we noted 'Accurate estimates' and 'Complexity to apply' the approach as key challenges across most studies. Looking at the sources of research we observe that a considerable number of primary studies are accredited to researchers affiliated with US based institutions but also note considerable contributions from European regions. Representation of the APAC region is limited but this could be due to language restrictions applied (IC2) for this SLR.

Lastly, we analysed the publication timeline for the selected primary studies and found no clear trend towards one particular information security investment valuation approach. We did observed a decline in ROI and ROT publications whereas UM publications are notably present across the timeline. This is supported by our analysis of citation count where we see studies on UM and GT being visibly more influential than other approaches.

Taking the findings of this systematic literature review into consideration a reasonable assumption can be made that challenges originating from uncertainty on estimates for key variables is a problem which requires prior solution. A perceived increase in research activity into externalities of information security and impact of information sharing seems to support this but would require a more in depth review for confirmation.

7 References

Alavi, M. and Henderson, J. C. (1981) 'An Evolutionary Strategy for Implementing a Decision Support System', *Management Science,* 27(11), pp. 1309-1323.

Anderson, R. 'Why information security is hard - An economic perspective'. *17th Annual Computer Security Applications Conference, Proceedings*, Los Alamitos: IEEE Computer Society, 358-365.

Arora, A., Hall, D., Piato, C. A., Ramsey, D. and Telang, R. (2004) 'Measuring the risk-based value of IT security solutions', *IT Professional,* 6(6), pp. 35-42.

Badenhorst, K. P. and Eloff, J. H. P. (1990) 'Computer security methodology: Risk analysis and project definition', *Computers & Security,* 9(4), pp. 339-346.

Beecham, S., Baddoo, N., Hall, T., Robinson, H. and Sharp, H. (2006) 'Protocol for a systematic literature review of motivation in software engineering', *University of Hertfordshire*.

Biolchini, J., Mian, P., Ana and Travassos, G. (2005) *Systematic Review in Software Engineering*.

Bistarelli, S., Dall'Aglio, M. and Peretti, P. (2007) 'Strategic games on defense trees', in Dimitrakos, T., Martinelli, F., Ryan, P.Y.A. & Schneider, S. (eds.) *Formal Aspects in Security and Trust Lecture Notes in Computer Science*, pp. 1-15.

Blakley, B., McDermott, E. and Geer, D. 'Information security is information risk management', *Proceedings of the 2001 workshop on New security paradigms*, Cloudcroft, New Mexico. 508187: ACM, 97-104.

Bodin, L. D., Gordon, L. A. and Loeb, M. P. (2005) 'Evaluating Information Security Investments Using the ANALYTIC HIERARCHY PROCESS', *Communications of the ACM,* 48(2), pp. 79-83.

Bojanc, R. and Jerman-Blazic, B. (2012) 'Quantitative Model for Economic Analyses of Information Security Investment in an Enterprise Information System', *Organizacija,* 45(6), pp. 276-288.

Bojanc, R. and Jerman-Blažič, B. (2008) 'An economic modelling approach to information security risk management', *International Journal of Information Management,* 28(5), pp. 413-422.

Brereton, P., Kitchenham, B. A., Budgen, D., Turner, M. and Khalil, M. (2007) 'Lessons from applying the systematic literature review process within the software engineering domain', *Journal of Systems and Software,* 80(4), pp. 571-583.

Capko, Z., Aksentijevic, S. and Tijan, E. (2014) 'Economic and financial analysis of investments in information security', *2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, pp. 1550-6.

Cavusoglu, H., Mishra, B. and Raghunathan, S. (2004) 'A Model for Evaluating IT Security Investments', *Communications of the ACM,* 47(7), pp. 87-92.

Cavusoglu, H., Raghunathan, S. and Yue, W. T. (2008) 'Decision-Theoretic and Game-Theoretic Approaches to IT Security Investment', *Journal of Management Information Systems,* 25(2), pp. 281-304.

Cremonini, M. 2005. Evaluating information security investments from attackers perspective: the return-on-attack (ROA).

Cronin, P., Ryan, F. and Coughlan, M. (2008) 'Undertaking a literature review: a step-by-step approach', *British journal of nursing (Mark Allen Publishing),* 17(1), pp. 38-43.

Cybersecurity Information Sharing Act of 2015. 2015.

Davis, A. (2005) 'Return on security investment – proving it's worth it', *Network Security,* 2005(11), pp. 8-10.

Demetz, L. and Bachlechner, D. (2013) 'To Invest or Not to Invest? Assessing the Economic Viability of a Policy and Security Configuration Management Tool', in Böhme, R. (ed.) *The Economics of Information Security and Privacy*: Springer Berlin Heidelberg, pp. 25-47.

Dengpan, L., Yonghua, J. and Mookerjee, V. (2011) 'Knowledge sharing and investment decisions in information security', *Decision Support Systems,* 52(1), pp. 95-107.

Department of Justice 2014. Justice Department, Federal Trade Commission Issue Antitrust Policy Statement on Sharing Cybersecurity Information. Office of Public Affairs.

Eisenga, A., Jones, T. L. and Rodriguez, W. (2012) 'Investing in IT Security: How to Determine the Maximum Threshold', *International Journal of information Security and Privacy,* 6(3), pp. 75-87.

Ekenberg, L., Oberoi, S. and Orci, I. (1995) 'A cost model for managing information security hazards', *Computers & Security,* 14(8), pp. 707-717.

European Network and Information Security Agency (2012) 'Introduction to Return on Security Investment', pp. 18. Available at: https://www.enisa.europa.eu/activities/cert/other-work/introduction-to-return-on-security-investment.

Faisst, U., Prokein, O. and Wegmann, N. (2007) 'Ein Modell zur dynamischen Investitionsrechnung von IT-Sicherheitsmaßnahmen', *Zeitschrift für Betriebswirtschaft,* 77(5), pp. 511-538.

Gordon, L. A. and Loeb, M. P. (2002) 'The economics of information security investment', *ACM Trans. Inf. Syst. Secur.,* 5(4), pp. 438-457.

Gordon, L. A. and Loeb, M. P. (2006) 'Budgeting Process for INFORMATION SECURITY EXPENDITURES', *Communications of the ACM,* 49(1), pp. 121-125.

Gordon, L. A., Loeb, M. P. and Lucyshyn, W. (2003) 'Sharing information on computer systems security: An economic analysis', *Journal of Accounting and Public Policy,* 22(6), pp. 461-485.

Gordon, L. A., Loeb, M. P., Lucyshyn, W. and Zhou, L. (2015) 'The impact of information sharing on cybersecurity underinvestment: A real options perspective', *Journal of Accounting and Public Policy,* 34(5), pp. 509-519.

Gordon, L. A., Loeb, M. P., Sohail, T., Tseng, C.-Y. and Zhou, L. (2008) 'Cybersecurity, Capital Allocations and Management Control Systems', *European Accounting Review,* 17(2), pp. 215-241.

Author (2007) *Publish or Perish*. Available at: http://www.harzing.com/pop.htm.

Hausken, K. (2006a) 'Income, interdependence, and substitution effects affecting incentives for security investment', *Journal of Accounting and Public Policy,* 25(6), pp. 629-665.

Hausken, K. (2006b) '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), pp. 338-349.

Hausken, K. (2007) 'Information sharing among firms and cyber attacks', *Journal of Accounting and Public Policy,* 26(6), pp. 639-688.

Herath, H. and Herath, T. (2011) 'Copula-based actuarial model for pricing cyber-insurance policies', *Insurance Markets and Companies: Analyses and Actuarial Computations,* 2(1), pp. 7-20.

Herath, H. S. B. and Herath, T. C. (2008) 'Investments in Information Security: A Real Options Perspective with Bayesian Postaudit', *Journal of Management Information Systems,* 25(3), pp. 337-375.

Herath, H. S. B. and Herath, T. C. (2014) 'IT security auditing: A performance evaluation decision model', *Decision Support Systems,* 57, pp. 54-63.

Hertz, D. B. (1979) 'Risk analysis in capital investment', *Harvard Business Review,* 57(5), pp. 169-181.

Hoo, K. J. S. (2000) 'How Much Is Enough? A Risk-Management Approach to Computer Security'.

Huang, C. D. and Behara, R. S. (2013) 'Economics of information security investment in the case of concurrent heterogeneous attacks with budget constraints', *International Journal of Production Economics,* 141(1), pp. 255-268.

Iheagwara, C., Blyth, A., Kevin, T. and Kinn, D. (2004) 'Cost effective management frameworks: the impact of IDS deployment technique on threat mitigation', *Information and Software Technology,* 46(10), pp. 651-664.

Jingyue, L. and Xiaomeng, S. (2007) 'Making cost effective security decision with real option thinking', *2007 International Conference on Software Engineering Advances*, pp. 1-9.

Keen, P. G. W. (1980) 'Adaptive design for decision support systems', *ACM SIGOA Newsletter,* 1(4-5), pp. 15-25.

Kesswani, N. and Kumar, S. 'Maintaining Cyber Security: Implications, Cost and Returns', *Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research*, Newport Beach, California, USA. 2751976: ACM, 161-164.

Khansa, L. and Liginlal, D. (2009) 'Valuing the flexibility of investing in security process innovations', *European Journal of Operational Research,* 192(1), pp. 216-235.

Kitchenham, B. and Charters, S. (2007) *Guidelines for performing Systematic Literature Reviews in Software Engineering*. Available at: http://www.dur.ac.uk/ebse/resources/Systematic-reviews-5-8.pdf.

Loch, K. D., Carr, H. H. and Warkentin, M. E. (1992) 'THREATS TO INFORMATION-SYSTEMS - TODAYS REALITY, YESTERDAYS UNDERSTANDING', *Mis Quarterly,* 16(2), pp. 173-186.

Matsuura, K. (2009) 'Productivity Space of Information Security in an Extension of the Gordon-Loeb's InvestmentModel', *Managing Information Risk and the Economics of Security*: Springer US, pp. 99-119.

Meho, L. I. and Yang, K. (2006) 'A new era in citation and bibliometric analyses: Web of Science, Scopus, and Google Scholar', *arXiv preprint cs/0612132*.

Miaoui, Y., Boudriga, N. and Abaoub, E. 'Insurance versus investigation driven approach for the computation of optimal security investment'. *Pacific Asia Conference on Information Systems* Singapore.

Miller, L. T. and Park, C. S. (2002) 'Decision Making Under Uncertainty—Real Options to the Rescue?', *The Engineering Economist,* 47(2), pp. 105-150.

Moore, T., Dynes, S. and Chang, F. R. (2015) 'Identifying How Firms Manage Cybersecurity Investment', pp. 32, Available: Southern Methodist University. Available at: http://blog.smu.edu/research/files/2015/10/SMU-IBM.pdf (Accessed 2015-12-14).

Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A. and Sadhukhan, S. K. (2013) 'Cyber-risk decision models: To insure IT or not?', *Decision Support Systems,* 56, pp. 11-26.

Neubauer, T. and Hartl, C. 'On the Singularity of Valuating IT Security Investments'. *Computer and Information Science, 2009. ICIS 2009. Eighth IEEE/ACIS International Conference on*, 1-3 June 2009, 549-556.

Neumann, J. v. and Morgenstern, O. (1964) 'Theory of games and economic behaviour', *Theory of games and economic behaviour.,* (3rd edition), pp. 641 pp.

Phillips, P. P. and Phillips, J. J. (2010) 'Return on Investment', *Handbook of Improving Performance in the Workplace: Volumes 1-3*: John Wiley & Sons, Inc., pp. 823-846.

Purser, S. A. (2004) 'Improving the ROI of the security management process', *Computers & Security,* 23(7), pp. 542-546.

Ross, S. A. (1995) 'Uses, Abuses, and Alternatives to the Net-Present-Value Rule', *Financial Management,* 24(3), pp. 96-102.

Rowe, B. R. and Gallaher, M. P. 'Private sector cyber security investment strategies: An empirical analysis'. *The fifth workshop on the economics of information security (WEIS06)*.

Saaty, T. L. (1994) 'How to Make a Decision: The Analytic Hierarchy Process', *Interfaces,* 24(6), pp. 19-43.

Sheen, J. N. (2010) 'Fuzzy Economic Decision-models for Information Security Investment', *Proceedings of the 9th WSEAS International Conference on Instrumentation Measurement Circuits and Systems (IMCAS 2010). Instrumentation, Measurement, Circuits and Systems*, pp. 141-7.

Shirtz, D. and Elovici, Y. (2011) 'Optimizing investment decisions in selecting information security remedies', *Information Management & Computer Security,* 19(2), pp. 95-112.

Siponen, M. T. and Oinas-Kukkonen, H. (2007) 'A review of information security issues and respective research contributions', *SIGMIS Database,* 38(1), pp. 60-80.

Srinidhi, B., Yan, J. and Tayi, G. K. (2015) 'Allocation of resources to cyber-security: The effect of misalignment of interest between managers and investors', *Decision Support Systems,* 75, pp. 49-62.

Strotz, R. H. (1955) 'Myopia and Inconsistency in Dynamic Utility Maximization', *The Review of Economic Studies,* 23(3), pp. 165-180.

Tatsumi, K.-i. and Goto, M. (2010) *Optimal Timing of Information Security Investment: A Real Options Approach. Economics of Information Security and Privacy*.

Thaler, R. H. and Sunstein, C. R. (2003) 'Libertarian Paternalism', *The American Economic Review,* 93(2), pp. 175-179.

The White House 2015. Executive Order -- Promoting Private Sector Cybersecurity Information Sharing. Office of the Press Secretary.

Wei, L., Tanaka, H. and Matsuura, K. (2007) 'Empirical-analysis methodology for information-security investment and its application to reliable survey of Japanese firms', *Transactions of the Information Processing Society of Japan,* 48(9), pp. 3204-18.

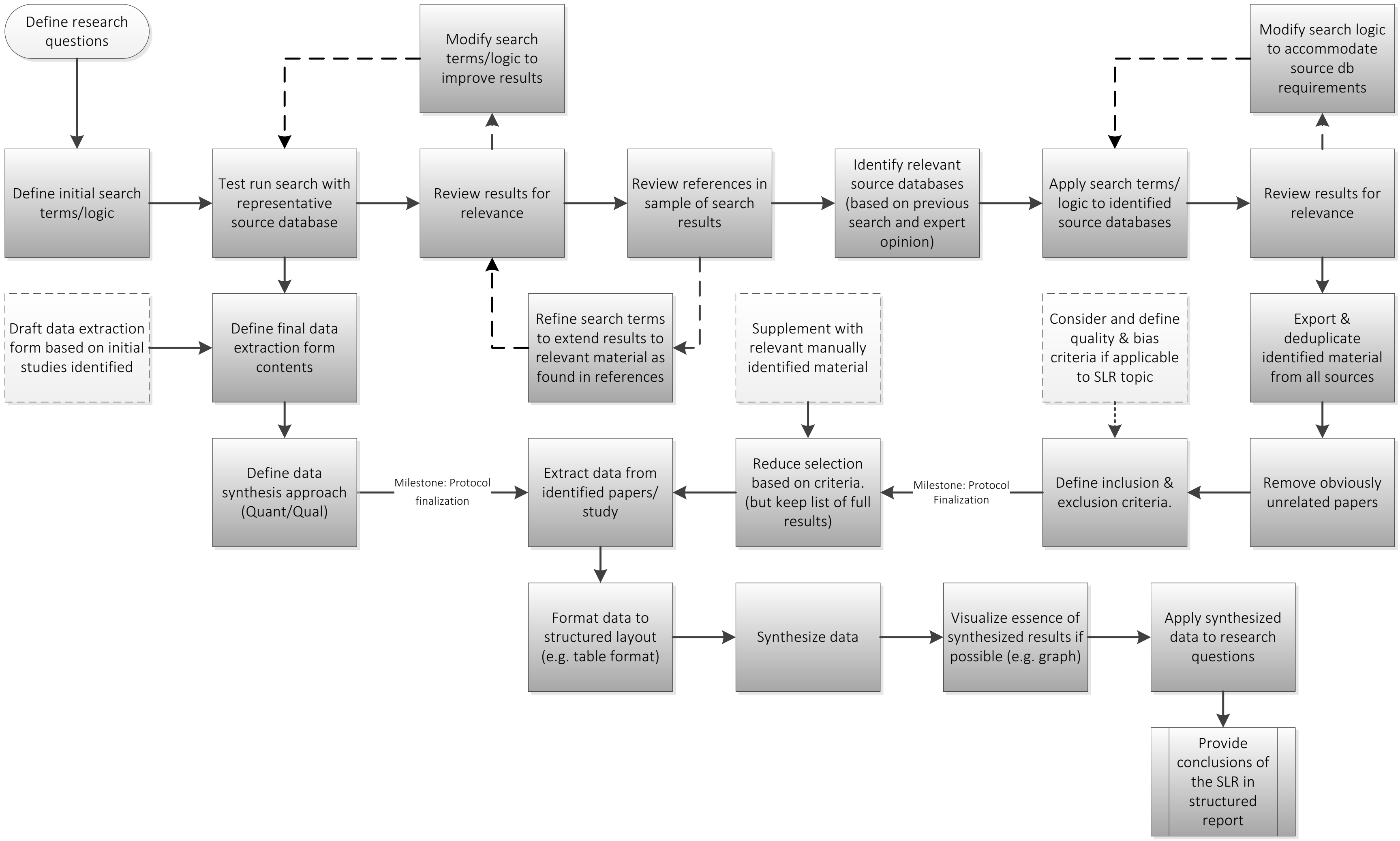
Willemson, J. (2010) 'Extending the Gordon&Loeb Model for Information Security Investment', *Proceedings of the Fifth International Conference on Availability, Reliability, and Security (ARES 2010)*, pp. 258-61.

Wood, C. C. and Parker, D. B. (2004) 'Why ROI and similar financial tools are not advisable for evaluating the merits of security projects', *Computer Fraud & Security,* 2004(5), pp. 8-10.

Yong Jick, L., Kauffman, R. J. and Sougstad, R. (2011) 'Profit-maximizing firm investments in customer information security', *Decision Support Systems,* 51(4), pp. 904-20.

Zikai, W. and Haitao, S. (2008) 'Towards an optimal information security investment strategy', *2008 IEEE International Conference on Networking, Sensing and Control (ICNSC '08)*, pp. 756-61.

8 Appendix – Systematic Literature Review workflow


Define research questions
Modify search terms/logic to improve results
Modify search logic to accommodate source db requirements
Define initial search terms/logic
Test run search with representative source database
Review results for relevance
Review references in sample of search results
Identify relevant source databases (based on previous search and expert opinion)
Apply search terms/ logic to identified source databases
Review results for relevance
Draft data extraction form based on initial studies identified
Define final data extraction form contents
Refine search terms to extend results to relevant material as found in references
Supplement with relevant manually identified material
Consider and define quality & bias criteria if applicable to SLR topic
Export & deduplicate identified material from all sources
Define data synthesis approach (Quant/Qual)
Milestone: Protocol finalization
Extract data from identified papers/ study
Reduce selection based on criteria. (but keep list of full results)
Milestone: Protocol Finalization
Define inclusion & exclusion criteria.
Remove obviously unrelated papers
Format data to structured layout (e.g. table format)
Synthesize data
Visualize essence of synthesized results if possible (e.g. graph)
Apply synthesized data to research questions
Provide conclusions of the SLR in structured report

9 Appendix – Key elements distribution

	AH	DS	G	NP	RO	RO	ROI,NP	RO	U	Tot
Elements	P	S	T	V	A	I	V	T	M	al
Benefit		**1**		**3**		**4**	**1**	**2**		**11**
Cost saving						1				1
Expected benefits								1		1
Financial benefits						1				1
Interest rates				1			1			2
Reduction in expected damages				1						1
Reduction of opportunity cost				1						1
Revenue		1				1				2
Total expected benefits								1		1
Value of change in risk						1				1
Cost		**4**	**1**	**2**	**1**	**3**	**2**	**2**	**2**	**17**
Cost and performance of remedies		1								1
Cost of attack					1					1
Cost of control									1	1
Cost of controls						1				1
Cost of incidents						1				1
Damage cost estimate			1							1
Direct cost		1								1
Inflation rate							1			1
Operating cost				1						1
Operating cost/revenue							1			1
Opportunity cost loss of C,I,A		1								1
Opportunity cost of capital				1						1
Potential loss of class									1	1
residual risk						1				1
Switching cost								1		1
Total cost		1						1		2
Function	**1**	**1**	**9**	**3**		**2**	**7**	**3**	**2**	**28**
AHP criteria tree	1									1
Baseline scenario						1				1
Binomial Options Pricing Model								1		1
Binominal lattice								1		1
Cross-over coefficient									1	1
Defense trees			1							1
Definition/Policy when to use ROSI						1				1
depreciation method				1						1
Discounted Return on Investment							1			1

Drift factor								1		1
Inefficiency factor			1							1
Internal Rate of Return							1			1
Mitigation quality parameters			1							1
Multi stage games			1							1
Net Present Value							2			2
Protection level for each end-effect		1								1
Return On (Security) Investment							1			1
Return on Attack (ROA)			1							1
Return on Security Investment (ROSI)			1							1
Risk metrics							1			1
Security threat probability function									1	1
Sequential games			1							1
Simultaneous games			1							1
Strategy decisions			1							1
Tax considerations				1						1
Triangular Fuzzy Numbers							1			1
Working capital considerations				1						1
Impact		**6**			**1**				**1**	**8**
Attackers gain					1					1
Breach loss									1	1
Impact factor		1								1
List of end-effects		1								1
Loss estimates		1								1
Potential damage		1								1
Profit at risk		1								1
Value at risk		1								1
Resource	**1**		**2**	**2**		**1**				**6**
Asset value			1			1				2
Attackers resources			1							1
EoL value				1						1
Fixed budget	1									1
Initial investment				1						1
Threat			**3**		**1**	**2**		**2**	**2**	**10**
Attackers efficiency (or EFF)					1					1
Average levels of attack			1							1
Breach probability based on scale-free networks concept									1	1
incident risk						1				1
Intensity of malicious attacks								1		1
Intensity threat								1		1
Rate of occurrence						1				1

Threat parameter estimates			2							2
Threat probability									1	1
Volatility								**4**		**4**
Underlying volatility								1		1
Volatility estimate								2		2
Volatility parameter								1		1
Vulnerability			**1**			**4**			**1**	**6**
Exposure factor						1				1
Net bypass rate for all security solutions						1				1
Secondary exposure factor						1				1
Underlying exposed assets						1				1
Vulnerability parameter estimates			1							1
Vulnerability probability									1	1
Grand Total	**2**	**12**	**16**	**10**	**3**	**16**	**10**	**13**	**8**	**90**
Elements	**AHP**	**DSS**	**GT**	**NPV**	**ROA**	**ROI**	**ROI,NPV**	**ROT**	**UM**	**Total**

Table 13 - Distribution of key elements across approaches

10 Appendix –Primary studies by ID

IID	***Paper/Study***
13	Arora, A., Hall, D., Piato, C. A., Ramsey, D., & Telang, R. (2004). Measuring the risk-based value of IT security solutions. *IT Professional, 6*(6), 35-42. doi: 10.1109/mitp.2004.89
23	Bistarelli, S., Dall'Aglio, M., & Peretti, P. (2007). Strategic games on defense trees. In T. Dimitrakos, F. Martinelli, P. Y. A. Ryan & S. Schneider (Eds.), *Formal Aspects in Security and Trust* (Vol. 4691, pp. 1-15).
28	Bodin, L. D., Gordon, L. A., & Loeb, M. P. (2005). Evaluating Information Security Investments Using the ANALYTIC HIERARCHY PROCESS. *Communications of the ACM, 48*(2), 79-83.
31	Bojanc, R., & Jerman-Blažič, B. (2008). An economic modelling approach to information security risk management. *International Journal of Information Management, 28*(5), 413-422. doi: 10.1016/j.ijinfomgt.2008.02.002
41	Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). A model for evaluating IT security investments. *Communications of the ACM, 47*(7), 87-92. doi: 10.1145/1005817.1005828
43	Cavusoglu, H., Raghunathan, S., & Yue, W. T. (2008). Decision-Theoretic and Game-Theoretic Approaches to IT Security Investment. *Journal of Management Information Systems, 25*(2), 281-304.
53	Davis, A. (2005). Return on security investment – proving it's worth it. *Network Security, 2005*(11), 8-10. doi: 10.1016/S1353-4858(05)70301-9

_80_ Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and Systems Security, 5*(4), 438-457. doi: 10.1145/581271.581274

_95_ Hausken, K. (2006). Income, interdependence, and substitution effects affecting incentives for security investment. *Journal of Accounting and Public Policy, 25*(6), 629-665. doi: 10.1016/j.jaccpubpol.2006.09.001

_99_ Herath, H. S. B., & Herath, T. C. (2008). Investments in Information Security: A Real Options Perspective with Bayesian Postaudit. *Journal of Management Information Systems, 25*(3), 337-375.

_107_ Iheagwara, C., Blyth, A., Kevin, T., & Kinn, D. (2004). Cost effective management frameworks: the impact of IDS deployment technique on threat mitigation. *Information and Software Technology, 46*(10), 651-664. doi: 10.1016/j.infsof.2003.11.004

_114_ Jingyue, L., & Xiaomeng, S. (2007). Making cost effective security decision with real option thinking. *2007 International Conference on Software Engineering Advances*, 1-9. doi: 10.1109/test.2007.4437622

_123_ Khansa, L., & Liginlal, D. (2009). Valuing the flexibility of investing in security process innovations. *European Journal of Operational Research, 192*(1), 216-235. doi: 10.1016/j.ejor.2007.08.039

_165_ Purser, S. A. (2004). Improving the ROI of the security management process. *Computers & Security, 23*(7), 542-546. doi: 10.1016/j.cose.2004.09.004

_186_ Sheen, J. N. (2010). Fuzzy Economic Decision-models for Information Security Investment. *Proceedings of the 9th WSEAS International Conference on*

Instrumentation Measurement Circuits and Systems (IMCAS 2010). Instrumentation, Measurement, Circuits and Systems, 141-147.

191 Shirtz, D., & Elovici, Y. (2011). Optimizing investment decisions in selecting information security remedies. *Information Management & Computer Security, 19*(2), 95-112. doi: 10.1108/09685221111143042

213 Tatsumi, K.-i., & Goto, M. (2010). *Optimal Timing of Information Security Investment: A Real Options Approach*.

237 Willemson, J. (2010). Extending the Gordon&Loeb Model for Information Security Investment. *Proceedings of the Fifth International Conference on Availability, Reliability, and Security (ARES 2010)*, 258-261. doi: 10.1109/ares.2010.37

244 Yong Jick, L., Kauffman, R. J., & Sougstad, R. (2011). Profit-maximizing firm investments in customer information security. *Decision Support Systems, 51*(4), 904-920. doi: 10.1016/j.dss.2011.02.009

252 Zikai, W., & Haitao, S. (2008). Towards an optimal information security investment strategy. *2008 IEEE International Conference on Networking, Sensing and Control (ICNSC '08)*, 756-761.

254 Capko, Z., Aksentijevic, S. and Tijan, E. (2014) 'Economic and financial analysis of investments in information security', 2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), pp. 1550-6.

257 Huang, C. D. and Behara, R. S. (2013) 'Economics of information security investment in the case of concurrent heterogeneous attacks with budget constraints', International Journal of Production Economics, 141(1), pp. 255-268.

M1 Cremonini, M. (2005). Evaluating information security investments from attackers perspective: the return-on-attack (ROA).

M2 Faisst, U., Prokein, O., & Wegmann, N. (2007). Ein Modell zur dynamischen Investitionsrechnung von IT-Sicherheitsmaßnahmen. *Zeitschrift für Betriebswirtschaft, 77*(5), 511-538. doi: 10.1007/s11573-007-0039-y

M4 Matsuura, K. (2009). Productivity Space of Information Security in an Extension of the Gordon-Loeb's InvestmentModel *Managing Information Risk and the Economics of Security* (pp. 99-119): Springer US.

Author Biogrphay

Daniel Schatz is the Director of Threat & Vulnerability Management for Thomson Reuters working in London/UK. He is a Chartered Security Professional (CSyP), member of the International Systems Security Association (ISSA-UK) and holds several qualifications including CISSP, CISM, ISO27001 LA/LI and MSc Information Security & Computer Forensics. He is currently pursuing his graduate studies in Information Security.

Rabih Bashroush is a Reader in Computer Science at the University of East London where he also leads the Enterprise Computing research group. Before joining UEL in 2010, Rabih was with the Queen's University Belfast for nearly 10 years, where he also received his PhD in Systems Engineering. He held visiting scientist posts at a number of organisations including: Software Engineering Institute, Carnegie Mellon University, USA; Philips Research Labs, Netherlands; and Danfoss Power Electronics, Denmark.