Categories of Approaches for IT Security Investment Decisions: A systematic literature review

Laura Niedzela
Martin-Luther-Universität Halle-Wittenberg, Germany, laura-maria.niedzela@wiwi.uni-halle.de

Leonard Nake
Martin-Luther-Universität Halle-Wittenberg, Germany, leonard.nake@wiwi.uni-halle.de

Tizian Matschak
University of Goettingen, Germany, tizian.matschak@uni-goettingen.de

Follow this and additional works at: https://aisel.aisnet.org/wi2022

Recommended Citation

This material is brought to you by the Wirtschaftsinformatik at AIS Electronic Library (AISeL). It has been accepted for inclusion in Wirtschaftsinformatik 2022 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.
Categories of Approaches for IT Security Investment Decisions: A systematic literature review

Laura Niedzela¹, Leonard Nake¹ and Tizian Matschak²

¹ Martin Luther University Halle-Wittenberg, Chair of Information Management, Halle (Saale), Germany
{laura-maria.niedzela,leonard.nake}@wiwi.uni-halle.de
² Universität Goettingen, Chair of Information Security and Compliance, Goettingen, Germany
tizian.matschak@uni-goettingen.de

Abstract. With an increasing amount of potential IT security breaches, ensuring the resilience of IT infrastructures and information assets is becoming a crucial task for companies today and in the future. When considering an investment, there are several decision-making approaches supporting companies to invest in adequate IT security measures. Providing an overview of these approaches mainly motivates the topic of this paper. Building on a systematic literature review we identify three main categories of these approaches for IT security investment decisions: the risk and return category, game theory category, and behavioral category. The analysis points out that the categories and approaches require a more detailed examination regarding their influencing factors.

Keywords: IT Security, Investment, Decision-Making, Categorization.

1 Introduction

Ensuring the resilience of a company's IT infrastructure is becoming increasingly important given the damage that can be caused by security breaches [1]. Therefore, a company’s decision about the portfolio of appropriate IT security measures and the associated investments is crucial and holds an extensive strategic influence.

There are several approaches from different research fields designed to support companies in making decisions about potential investments in IT security measures. We consider three research fields following Shao et al. (2019) [1]. Approaches from Game Theory mostly focus on the interplay between firms and attackers [2], [3], behavioral approaches focus on the behavior and attitude of decision-makers [4], [5] and Risk and Return approaches calculate returns of IT security investments given a specific IT security risk [6-9]. While approaches from the same research field vary considerably in their focus and methodology, approaches from different research fields vary even in the factors assumed to influence the investment decision. For instance, many Game Theory approaches emphasize the importance of cooperation with competitors in IT security investments [10], [11], however, this influencing factor is rarely mentioned in approaches designed to estimate the risk of security breaches and
the respective return of IT security investments [6-9]. Therefore, when applying an approach from one research field to make decisions about IT security investments, the insights of other research fields are not taken into consideration. Hence, applying a single approach might lead to suboptimal results since factors relevant to the respective investment might not be considered.

To generate profound insights of approaches for IT security investments decisions and to build a solid basis for future research, the goal of this paper is to categorize existing approaches depending on their methods and factors considered. Hence, we raise the following research question: Which categories of decision-making approaches can be identified that support companies in investing in IT security measures?

This paper is structured as follows: In section 2, we present the applied research method in detail. Specifically, we conducted a systematic literature review following the work of vom Brocke (2009) [12]. Section 3 introduces the results of the conducted analysis and describes the identified categories. Finally, section 4 summarizes our findings, their limitations and discusses the research agenda of our ongoing research.

2 Research Method

To answer our research question, we conduct a systematic literature review with high scientific rigor. Therefore, we apply vom Brocke’s (2009) “Framework for literature reviewing” [12] consisting of five review steps. In step 1 we define the scope of the review. In the second step, the topic of the paper is put into context. This step was integrated into our introduction. In step 3 we describe our literature search, followed by the analysis of our literature in step 4 and the conclusion and research agenda in step 5.

**Figure 1. Literature search process**
We start with classifying our literature review as step 1 of vom Brocke’s (2009) framework. For this, we use the six characteristics of Cooper’s (1988) “Taxonomy of Literature Reviews” [13]: We focus on research outcomes and theories. Our goal is to analyze central categories of IT security decision-making. The perspective of the review is neutral and the coverage is exhaustive with selective criticism. We conceptually organize the results of our literature analysis and address specialized scholars as the audience of this paper.

With Cooper’s (1988) taxonomy as the basis for our literature review, we continue with step 3, the literature search. In this step, we were looking for central contributions to categories for decision-making in IT security investments. We conducted our search in scientific databases (Figure 1). In these, the previously defined search term was applied as a title search in all five databases. To achieve results that fit the topic of our paper best and to ensure replicability of the literature search, three exclusion criteria were formulated. We excluded hits with contributions (1) that do not address decision factors of investments in IT security measures. We also excluded hits with contributions (2) that focus on specific industries or business sectors, as we wanted to generate universally applicable decision factors. Also, we wanted to address an international scientific audience, which is why we also excluded hits (3) that are not in English and have not been peer-reviewed.

In the end, the literature search consisted of five steps: duplicate removal, title selection, abstract selection, full-text selection, backward selection and resulted in a total number of 58 hits. The whole literature search process is illustrated in figure 1.

3 Analysis of the Results

The result of our analysis (Table 1) reveals that the majority of the approaches can be categorized according to Shao et al. (2019) [1] and other contributions into the three categories: Risk and Return (59%), Behavioral (12%), and Game Theory (12%) with an unfitting rest (17%). A list of the identified papers with their corresponding categories can be found at the following URL: https://bit.ly/3pXezI5.

<table>
<thead>
<tr>
<th>Year of Publication</th>
<th>Risk and Return</th>
<th>Behavioral</th>
<th>Game Theory</th>
<th>Rest</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>1992</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>2002</td>
<td>1</td>
<td></td>
<td>2</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>2003</td>
<td></td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>2005</td>
<td></td>
<td></td>
<td>1</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>2006</td>
<td></td>
<td></td>
<td>1</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>2007</td>
<td></td>
<td></td>
<td>1</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>2008</td>
<td></td>
<td></td>
<td>1</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>2009</td>
<td></td>
<td></td>
<td>1</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>2010</td>
<td></td>
<td></td>
<td>1</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>2011</td>
<td></td>
<td></td>
<td>1</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>2012</td>
<td></td>
<td></td>
<td>1</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>2013</td>
<td></td>
<td></td>
<td>1</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>2014</td>
<td></td>
<td></td>
<td>1</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>2015</td>
<td></td>
<td></td>
<td>1</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>2016</td>
<td></td>
<td></td>
<td>1</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>2017</td>
<td></td>
<td></td>
<td>1</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>2018</td>
<td></td>
<td></td>
<td>1</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>2019</td>
<td></td>
<td></td>
<td>1</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>2020</td>
<td></td>
<td></td>
<td>1</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>2021</td>
<td></td>
<td></td>
<td>1</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Total</td>
<td>34</td>
<td>7</td>
<td>7</td>
<td>34</td>
<td>58</td>
</tr>
</tbody>
</table>

Table 1. Results of the Literature Search

3.1 The Risk and Return Category

The risk and return category contains approaches that use a combination of the risk and the potential damage of an IT security breach as well as the expected damage reduction
3.2 The Behavioral Category

The behavioral category is significant for the decision-making process in IT security investments. The awareness and behavior of decision-makers regarding an organization’s IT security can have a crucial impact on the resulting security measures. In this context, the reputational herding theory is often mentioned [14], which states that if decision-makers do not possess valid information and are therefore not able to make an appropriate investment decision, they tend to focus on the choices of other experts. The ability of decision-makers thereby depends on the information at hand, but also on their experience and savviness [1], [4], [5]. Reputational herding results from uncertainty in decision-making while aiming for maintaining a good reputation. Therefore, low reputation can lead to a discounting of one’s information, though on the other side good decisions can result in reputation improvements [1], [4]. It becomes apparent that investment decisions highly depend on the behavior of the decision-maker, e.g. the information security officer. This leads to some challenges, as the subjectivity of officers may limit their ability to objectively list the exact needs in information security. The result is an individual decision that can differ depending on the person making it [15], [16]. Regarding the behavioral category, organizational behavior such as industry norms, budget constraints, or other restrictions, also influences the investments in information security. As an example, decision-makers will take higher security risks, if the organization’s budget requests it [15-17].

3.3 The Game Theory Category

Game theory presents another category of decision-making approaches in security investments. Most articles describe the challenge of deciding between independent or centralized security investments of two companies with substitutional information assets. In this case, it is assumed that after an unsuccessful attack at one of the companies, the attacker might change the strategy and attack the other company. To ensure the failure of the attack and a change of strategy of the attacker, independent security decisions carry the risk of an over-investment in relation to the potential loss that the respective company is facing. In contrast to the independent IT security investment, an alliance between the companies and thereupon a centralized investment
decision could lead the companies to invest less and optimize their total cost [2], [10], [11]. Game Theory can also be applied to the context of information sharing between linked companies of a supply chain. This exchange of information leads to increased security risks since one’s own security risks also depend on the security investments of the linked companies [18], [19]. In addition to the use of game theory for investment decisions between two companies, there are also those decisions resulting from the interaction of a company and its attacker. In this case, the focus is rather on optimal use of the available security budget in control systems. Since only one vulnerability needs to be overseen for an attacker to succeed, a company needs to apply at least essential control systems that protect a majority of their assets [3].

3.4 The Rest

The last group contains all approaches that cannot be categorized into one of the three former categories. While this rest of the approaches is heterogeneous and can, therefore, not be seen as a coherent category, the individual approaches still provide meaningful insights into the decision process regarding IT security measures. For instance, one approach conducts a Delphi study to determine relevant information security investment drivers [20]. The results indicate that, in practice, decision-makers prioritize different factors in their decision, e.g. guaranteeing compliance with regulations, than approaches from other categories suggest.

4 Conclusion and Next Steps of Research

The protection of information assets and IT infrastructure has become increasingly crucial in recent years. The examination and selection of approaches for IT security investment decisions are therefore all the more important [1], [21]. Considering the wide range of research, an overview of categories on decision-making approaches supporting IT security investments becomes relevant. In this paper, we have used a structured literature search to identify and analyze the current state of research. We answered our research question by analyzing the central categories: the risk and return category, game theory category, and behavioral category, and by referring to those approaches that cannot clearly be assigned to one of the categories. By doing so, we built a profound basis for further investigations on decision-making approaches for investments in IT security.

Nevertheless, our analysis remains with some limitations. Although we have already conducted a comprehensive examination of the research field regarding the approaches on IT security investment decisions, our ongoing research focuses on the individual factors influencing the decision-making process. The goal is to further analyze these factors by creating a taxonomy. This will help to create a deeper understanding and to further identify research gaps. Also, this could solve the problem that not all approaches can be assigned to a particular category. A focus on decision-making factors would therefore lead to a holistic analysis, create a more consistent picture of the problem, and could be of high interest for practitioners and scientists.
References


