Analyzing the Economic Impacts of Security Breaches Due to Outsourcing

Dimitrios Koumaridis, Emmanouil Stiakakis, and Christos K. Georgiadis

University of Macedonia, Department of Applied Informatics,
Egnatia 156, 54006 Thessaloniki, Greece
{koumaridis,stiakakis,geor}@uom.gr

Abstract. In our study, we present four different approaches on the subject that are connected more or less to each other, giving more attention on outsourcing security issues. A case study for the use of outsourced services is also presented using empirical data from an insurance company. This work concludes with an overview of our research, its limitations and by giving some research questions for future work.

Keywords: security economics, outsourcing, security breach.

1 Introduction

The aim of this work is to identify and examine some of the major approaches in the area of security economics. More specifically, four different approaches are examined. We start by presenting them in the section of theoretical background and then we mostly emphasize on the one dealing with the outsourcing policy of companies. These four approaches are connected to each other since they deal with the same subject but from a different point of view.

The first approach is a research by Wang [1] about the effects that disclosures have in business economics, regarding security policies and cases of security breakdowns. The second approach by Ioannidis et al. [2] presents the “conflict” between system administrators and system users about confidentiality and availability. The authors also present the endless effort of the administrators to exploit their budgets properly in order to raise their effectiveness. The third approach on the subject of security economics comes from Anderson [3] and is more behavioral rather than technical, as security is a combination of technology and policy over the proper usage of it. It deals mainly with differences in sentiments upon information security. The fourth approach deals with the rising development of the third partner services in many businesses and the problems occurring from the adoption of this outsourcing policy. It is of great importance that a company gives the opportunity to another company to process crucial and sometimes top secret data. The last approach is the main topic of our work. We conclude with a case study concerning a Greek insurance company about the usage of outsourced services and their impacts.
2 Theoretical Background – Literature Review

For a non-experienced observer, the aforementioned approaches are not connected to each other; however, there are certain similarities among them. These similarities will be understood once the following presentation of the approaches has been completed.

2.1 The Effects of Information Disclosures in Business Economics

Business nowadays relies heavily on information technology to perform daily operations. Because of this increasing reliance on information technology, information security related incidents could result in a tremendous impact on a firm’s operation and significant financial losses [1]. In order to address the issues and better manage information security risks, researchers and managers have strived to better understand and assess information security risks.

Some firms announce risks related to information security publicly. There are two competing motivations from the literature why firms disclose risk factors. On the one hand, the disclosure of risk factors may contribute to the reduction of the uncertainty that investors have regarding the firm’s performance [4]. On the other hand, a firm may disclose risk factors in order to reduce its future litigation costs associated with adverse events [5]. In the information security context, any motivation may be valid. Some firms are inclined to disclose to indicate preparedness, which corresponds to the first motivation, whereas other firms disclose in order to head off lawsuits, which is the second motivation.

Wang [1], through his research, tries to further examine investors’ reactions to security breaches. Investors’ reactions provide explanations to managers and researchers about what leads to the price and volume reactions to security incidents. When there is no disclosure cost, full disclosure exists because investors believe that non-disclosing companies have the worst possible information. However, if disclosure costs or uncertainty exist, companies will disclose only when the benefits exceed the costs. Disclosure may also be used to reduce ex post legal and reputation costs from bad news or when the firm faces earnings disappointments. General market participants can actually adjust their investment decisions regarding breach announcements given the sophisticated investors’ reactions. A trading strategy is performed to demonstrate profitable short-term investment opportunities given the information asymmetry among investors. There is a strong association between the textual contents of the news articles about security breach reports, and both the stock price and trading volume reactions to breach announcements. The results suggest that general breach announcements lead to different assessments of the impact of security incidents. However, specific news articles and those about confidential information result in a more consistent negative belief of the impact of security incidents on a firm’s future performance. By taking advantage of the different perceptions among investors, it is shown that, on average, one can make about 300% annual profit around the breach announcement date.