CITS:
The Cost of IT Security Framework

Marco Spruit, Department of Information and Computing Sciences, Utrecht University, Utrecht, The Netherlands

Wouter de Bruijn, Department of Information and Computing Sciences, Utrecht University, Utrecht, The Netherlands

ABSTRACT

Organizations know that investing in security measures is an important requirement for doing business. But how much should they invest and how should those investments be directed? Many organizations have turned to a risk management approach to identify the largest threats and the control measures that could help mitigate those threats. This research presents the Cost of IT Security (CITS) Framework to support analysis of the costs and benefits of those control measures. This analysis can be performed by using either quantification methods or by using a qualitative approach. Based on a study of five distinct security areas–Identity Management, Network Access Control, Intrusion Detection Systems, Business Continuity Management and Data Loss Prevention–nine cost factors are identified for IT security, and for only five of those nine a quantitative approach is feasible for the cost factor. This study finds that even though quantification methods are useful, organizations that wish to use those should do this together with more qualitative approaches in the decision-making process for security measures.

Keywords: *Business Continuity Management and Data Loss Prevention, Identity Management, Information Technology, Intrusion Detection Systems, Network Access Control, Security Framework*

INTRODUCTION

In August 2008 an identity theft scheme was unraveled when the United States justice department started prosecuting 11 people involved in the scheme (”US cracks biggest”, 2008). The criminals targeted nine major U.S. retailers and accessed their network by connecting to the wireless networks used by shops of those retailers. They were able to access the network as it had no encryption or hacked their way in despite the encryption. Once inside they tracked and collected credit card data. By going from city to city, a total of 40 million credit and debit card numbers were stolen. The suspects allegedly stored the information on compromised web servers and would encode credit card information on blank cards. Those cards where used to withdraw cash from ATM’s. The money was transferred to bank accounts in Eastern Europe, where some of the 11 suspects were located. It was unclear how much money exactly was made in the identity theft scheme.

DOI: 10.4018/jisp.2012100105

Had the involved retailers stronger encryption in place for their wireless networks, the hackers would have not been able to gather this amount of confidential data. The losses for the involved companies could run into well over ten million dollars.

The scheme is a clear example where investments in information security would have prevented a much larger loss. It is an important requirement for all organizations to keep their information assets secure.

In order to calculate the cost of future security measures they will have to make assumptions. If these are wrong, they will base their decisions on false data. Furthermore, for companies, it is not just about one implementation; if a company installs the best firewall out there but outsiders can easily access the wireless network from the parking lot of the building, security still is weak. Executive managers making the decisions will have to realize that making a measure in one area influences the validity of other security measures already taken. This all makes decision making in information security is a difficult task. In the complex environment with a multitude of factors troubling the view, making the right decisions is hard. Many companies resort to baseline measures as presented by standards and best practices. Many of those standards include an approach based on risk management. In this approach, organizations analyze risks before deciding on measures that can mitigate those risks. In some cases, the chance of an incident occurring is so small that so the organization can decide against any preventive measures. A risk management approach also allows them to prioritize the risks. After those risks are assessed the right mitigation strategy needs to be selected.

To help the decision making process, this research will present a framework which gives an overview of the cost factors that come into play. For some factors influencing the decision, it will be easy to calculate the exact costs. For some others, the time and resources it takes to even come to an imprecise estimate make it unfeasible for the quantitative approach. As the risk management approach to security seems to be the best way of informing executive managers about the risks and the effectiveness of a security measure, this will form the basis of the approach taken in this research.

There has been some attention to the topic of the economics of IT security, but the amount of papers, articles and books available on this topic are limited. Economic approaches to the problem have been tried, some coining the term 'Return on Security Investment', but they have not yet received widespread use. This is partially because most of the models focus on one implementation at a time. The consensus in the field at the moment seems to be that even though an economic approach can lead to better decision making, calculating the exact costs is almost impossible to do (Anderson, 2001; Gordon & Loeb, 2006b). This all leads to the following question which we will aim to answer in this research:

What aspects of IT security can be made quantifiable and how can the real costs of these aspects be measured?

The research question makes clear that some aspects are quantifiable, implying that others aren't, and shows the goal of creating a framework taking all costs into account. In order to create a complete framework, the qualitative aspects will also have to be added to the framework. The focus will be on the quantitative aspects.

RISK MANAGEMENT

Small organizations often will have an ad-hoc approach to IT Security, with the related tasks often being performed by the system administrator. As organizations grow larger a different approach is needed. Organizations use security standards and best practices. Even though this approach gives a good overview of what is needed in the security strategy, to best results are achieved if the strategy completely fits