ABSTRACT

Management may see information security as an inhibitor to daily operations if the investment is not well aligned with current business activities or is presented in financial terms not relevant to their agenda. While this chapter shows that information security improvements create bottom-line business benefits, there is still a need for security managers to focus on quantifying those benefits in relevant financial terms. The purpose is to demystify the principles of general investment processes and criteria for calculating the benefits and costs of investments while accentuating alignment to the imperatives of the organization that makes the investment. As information security investments are assessed alongside other investment projects, it helps to consider them on an equal footing, implying the use of similar, and ideally the same, methods of financial cost projection. It is equally important to position and present the proposed investment in a relevant business context.

INTRODUCTION

When top level management makes investment decisions it strives to find a balance between risk and reward for the company to meet the overall goals and ambitions. These goals could be defined as single year financial targets combined with annual budgets and rolling forecasts or they could be related to more long-term metrics used to drive a change.

Since 2008 we have witnessed unprecedented changes in the global economic environment that has presented new risks and challenges combined with new technologies, where some have helped improve information security and some have brought new risks and concerns.
Many security professionals struggle with the fact that costs associated with information security incidents can have large components which are difficult to quantify. Information security decisions still need not be taken with a complete lack of quantified value. Quite to the contrary, in the manner of any investment request, there are often numerous opportunities to collect data and trend information in order to measure the effectiveness of the investment.

If investments in information security are assessed alongside other investment projects it helps to consider them on an equal footing, implying the use of similar (and ideally the same) methods of financial cost projection. Benefits that cannot be measured with quantitative values may mean less to senior management. They may see information security as an inhibitor to their daily operations if the investment is not well aligned with current business activities or is presented in financial terms that seem not relevant to their agenda (Tsiakis and Pekos, 2008).

This chapter is aimed at providing information security professionals with a brief introduction to performing cost benefit analyses of information security investments and presenting them to management in order to bridge the gap between security professionals and business leaders.

It is based on recent reports and previous research on the topic, and should be considered as a summary only. For a deeper analysis and broader perspectives on obtaining support and funding from senior management, please refer to the full reports.

The Need for Alignment to Business Needs

Over the past several years, we have witnessed unprecedented changes in the global economic environment. Increased pressure to improve profitability, coupled with increased government and industry regulations and austerity measures have presented new risks and challenges — challenges that many organisations are now struggling to address. We also witnessed new technologies introduced and adopted, some that helped improve information security and some that brought new risks and concerns.

The professional services firm Ernst & Young (2012) has conducted research on the impact of the downturn in the market by conducting more than 50,000 direct meetings with senior executives since 2008 as well as performing annual benchmark studies, the latest published in December 2012, run by the Economist Intelligence Unit (EIU) surveying 1,500 C-suite, board directors and senior managers from around the world.

As with earlier studies, Ernst & Young have factored out the impact of sector and distinguished between the highest and the lowest quartile of performers, in both revenue and EBITDA growth, to identify specific patterns of action that might explain the difference in performance. Top level management could use this study, and others, to help define priorities for investments to meet the overall goals and ambitions of the company.

Four key areas have been identified where high performers are significantly ahead of their competitors: customer reach, operational agility, cost competitiveness and stakeholder confidence (see Table 1).

Companies researched share that information is a fundamental asset to them. Information security is therefore critically important to protect data against a wide variety of threats, such as unauthorized disclosure, data errors or loss of information.

The annual Global State of Information Security® run by the professional services firm PwC (2012) shows that from 2008 to 2009 there was a significant drop in respondents expecting increased information security budgets, reflecting the initial impact of the financial crisis. For the following years barely more than half of the respondents expected increases in budget spend, while 45 percent of the 9,300 respondents see a tightening of information security budgets for 2013.