

Chapter 3.6

An Alternative Model of Information Security Investment

Peter O. Orondo

Acclaim Consulting Group, Inc., USA

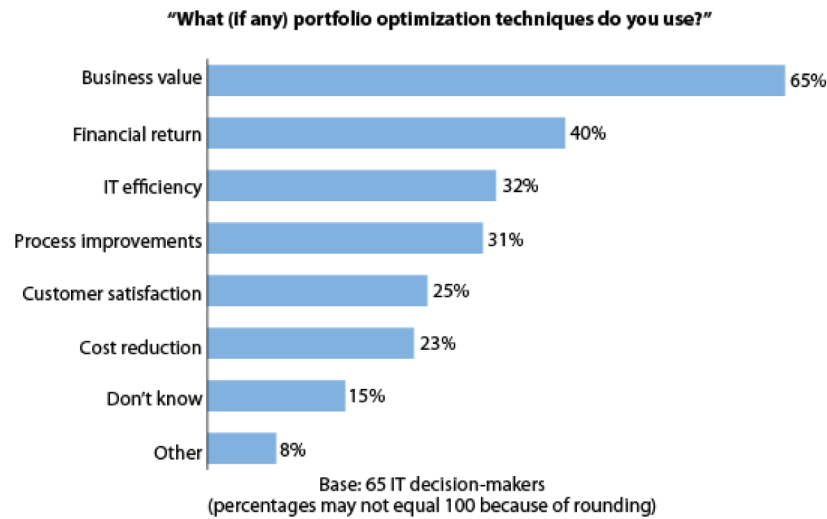
ABSTRACT

Most companies would agree that securing their information assets is worth some investment. It is thus plausible to assume that low levels of IT security investment indicate that only a small portion of the firm's business is IT asset value driven. It could also point to a misaligned corporate investment policy. Conversely, some firms may be investing more than is warranted given the value of their information asset holdings, thereby wasting shareholder resources. The question then becomes: What level of IT security investment is enough? Several models exist to help companies set their IT spending in general and Information Security spending in particular. The leading model out there is the Information Technology Portfolio Manage-

ment (ITPM) model. This is really nothing more than financial portfolio management theory applied to the information technology realm. Thus ITPM tries to optimize IT spending based on a number of factors like business value, efficiency and cost reduction among others. Despite current vigorous research at esteemed institutions like the Center for Information Systems Research (CISR) at MIT and at the Free University of Amsterdam, ITPM is still in its infancy and the field would benefit from alternative models. In this chapter, we propose an alternative model of IT security spending that firms may readily apply when setting their Information Security budgets. The model is analytical and starts by developing a model for the business value of information. It then develops a model for the cost of an information security breach. Finally, we find the relationship between the value model and the cost model from.

DOI: 10.4018/978-1-60566-132-2.ch008

Figure 1. IT portfolio optimization criteria (Symons, 2005)



INTRODUCTION

The global spending on IT may only be considered as leviathan – \$1.5 trillion in 2007 according to Forrester (Bartels, 2007), and is the driver for a very large segment of the global economy, especially in the western industrialized countries. At any individual firm, the \$1.5 trillion figure typically translates to between 1% and 8% of revenues. Since any firm’s spending is a balancing act amongst multiple competing priorities, it becomes critical for CIOs and IT managers to justify every penny spent on IT.

As we mentioned earlier, the most common model appears to be the ITPM model which views IT spending as an investment just like any other that the firm makes. ITPM then creates metrics, processes and monitoring tools that ultimately measure Return on Investment (ROI) for each IT dollar spent (Symons, 2005).

The Forrester Research cited (Symons, 2005) also reveals that firms are most likely to optimize their IT spending around Business Value. In other words, the firms surveyed decided that the business value of IT spending outweighed other considerations like financial return, cost reductions and even efficiency (see Figure 1).

This validates a key premise of our model, namely that IT Security Spending is integral to the firm’s value chain. We shall return to this notion of “Business Value” driven IT Security Spending later when we formulate our model.

ITPM however, is still in its infancy, and is fairly complicated to apply, monitor and measure in any given company. Additionally:

- ITPM is ultimately based on financial theory of portfolio optimization. While it is plausible that the basic concepts of Modern Portfolio Theory (MPT) – see for example (Markowitz, 1952) - should apply to IT spending, the two problems are sufficiently different that substantial conceptual modifications to MPT are in order before it can make sense to the IT Line Manager. At the very least, it is not clear that MPT is the best approach to model IT Investment Portfolios. For example, the IT Investment portfolio is not as liquid as a stock portfolio, if at all.
- ITPM is complicated and thus not easily accessible except to generally larger firms with a fair amount of resources devoted to IT process and operations modeling. This is

6 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/alternative-model-information-security-investment/54504

Related Content

Digital Game-Based Learning in Higher Education

Sauman Chu (2009). *Encyclopedia of Information Science and Technology, Second Edition* (pp. 1120-1124).

www.irma-international.org/chapter/digital-game-based-learning-higher/13716

A Knowledge Management Approach to the Loosely Coupled Systems

Jernej Agrezand Nadja Damij (2016). *Information Resources Management Journal* (pp. 75-90).

www.irma-international.org/article/a-knowledge-management-approach-to-the-loosely-coupled-systems/143169

Decision-making as a Facilitator of High-achievement in Non-hierarchical Technical Environments

Dwayne Rosenburgh (2009). *Open Information Management: Applications of Interconnectivity and Collaboration* (pp. 20-43).

www.irma-international.org/chapter/decision-making-facilitator-high-achievement/27790

Navigating the Legal Landscape of Information Governance

Hemendra Singh (2024). *Creating and Sustaining an Information Governance Program* (pp. 217-235).

www.irma-international.org/chapter/navigating-the-legal-landscape-of-information-governance/345427

Decision Framework for Engaging Cloud-Based Big Data Analytics Vendors

Emmanuel Wusuhon Yanibo Ayaburi, Michele Maasbergand Jaeung Lee (2020). *Journal of Cases on Information Technology* (pp. 60-74).

www.irma-international.org/article/decision-framework-for-engaging-cloud-based-big-data-analytics-vendors/263292