Chapter XVII
Aligning IT Teams' Risk Management to Business Requirements

Corey Hirsch
LeCroy Corporation, USA

Jean-Noel Ezingeard
Kingston University, UK

ABSTRACT

Achieving alignment of risk perception, assessment, and tolerance among and between management teams within an organisation is an important foundation upon which an effective enterprise information security management strategy can be built .We argue the importance of such alignment based on information security and risk assessment literature. Too often lack of alignment dampens clean execution of strategy, eroding support during development and implementation of information security programs . We argue that alignment can be achieved by developing an understanding of enterprise risk management plans and actions, risk perceptions and risk culture. This is done by examining context, context and process. We illustrate this through the case of LeCroy Corp., illustrating how LeCroy managers perceive risk in practice, and how LeCroy fosters alignment in risk perception and execution of risk management strategy as part of an overall information security program. We show that in some circumstances diversity of risk tolerance profiles aide a management teams' function. In other circumstances, variances lead to dysfunction. We have uncovered and quantified nonlinearities and special cases in LeCroy executive management's risk tolerance profiles.

INTRODUCTION

A sociological understanding of risk perception as an input to information security development is becoming a necessity. We know this from two strands of literature: the first is the literature in risk assessment in fields other than information security. The second is the information security literature. In particular, understanding how management and functional teams perceive risk, and decide and act in managing risk, is one cornerstone of an effective enterprise information security management strategy. If managers do not understand the reasons behind an information security policy, or do not fully support the rationale behind it, they are unlikely to engage in its development or adhere to it later. Furthermore, divergent information security decisions and actions may have the effect of canceling out each other, and render the enterprise risk management strategy less effective. In addition, events such as mergers, security breaches, or regulatory changes may cause managers' perceptions of risk to evolve.

How, then, do managers perceive risk in practice? And how might an enterprise foster an aligned approach to risk management? This chapter presents such a methodology. We will use a medium sized manufacturer of test and measurement equipment, LeCroy Corp., to illustrate.

We will show that whilst there are areas where perceptions toward and tolerance of risk are shared within a department or work team, there can be substantial variations between different groups of managers. Groups which routinely work together on information security and risk management related tasks, however, have lower standard deviations in their risk judgments than teams which do not share this working experience. Yet this second group may have responsibilities that are critical to enterprise risk management.

Individuals in a population display variation in their tolerance for risk. A retired widower for example, might choose an investment known to offer lower returns than other investments available, because it also presented a lower likelihood of variations in return. A young entrepreneur on the other hand, might be willing to accept a high probability of surprises, as long as she felt the upside was commensurate with the downside. Willingness to accept a reduction in return, in order to reduce expected variation in return, is *intolerance to risk*. Willingness to accept high expected variation in return, in order to maximize expected return is *tolerance for risk*. This chapter will illustrate how top executives are mathematical in their risk appetite at low and medium stakes, yet highly risk-averse when the stakes are higher, such as when complete business success or failure are potential outcomes. The chapter will also demonstrate how to quantify an organization's level of risk tolerance, which will in turn enable a reader to align IT risk management strategy to an organization's risk culture.

BACKGROUND

A good understanding of both intolerance and tolerance to risk is at the core of any successful information security policy, usually developed in three stages. The first stage typically entails risk identification and assessment. This is usually followed by stages looking at how risks can be monitored and controlled, with a third and final stage concerned with risk avoidance and mitigation. For instance, COBIT 4.0 (ITGI, 2005) proposes that the "assess and manage IT risks" high level control objective should be met through a series of 10 activities culminating in the maintenance and monitoring of a risk action plan. Similarly, in ISO 17799:2005 (ISO, 2005a), the first section describing best practice is one on "risk assessment and treatment."

Sources of information security risk are usually documented in taxonomies of risks. They tend to list broad categories of risk sources (Backhouse & Dhillon, 1996) that can be used to ensure that