IRM PRESS
701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.irm-press.com
ITB15306

This chapter appears in the book, ***Computer Security, Privacy, and Politics: Current Issues, Challenges, and Solutions*** by **R. Subramanian** © 2008, IGI Global

Chapter VII

Business Cases for Privacy-Enhancing Technologies

Roger Clarke, Xamax Consultancy Pty Ltd, Australia;
University of New South Wales, Australia;
Australian National University, Australia;
and University of Hong Kong, Hong Kong

Abstract

Many categories of e-business continue to under-achieve. Their full value cannot be unlocked while key parties distrust the technology or other parties, particularly the scheme's sponsors. Meanwhile, the explosion in privacy-intrusive technologies has resulted in privacy threats looming ever larger as a key impediment to adoption. Technology can be applied in privacy-enhancing ways, variously to counter invasive technologies, to enable untraceable anonymity, and to offer strong, but more qualified pseudonymity. After their first decade, it is clear that privacy-enhancing technologies (PETs) are technically effective, but that their adoption lags far behind their potential. As a result, they have not delivered the antidote to distrust in e-business. If individuals are not spontaneously adopting PETs, then the opportunity exists for corporations and government agencies to harness PETs as a core element of their privacy strategies. The financial investment required is not all that large. On the other hand, it is challenging to attract the attention of executives to an initiative of this nature, and then to adapt corporate culture to ensure that the strategy is successfully carried through. This chapter examines PETs, their application to business needs, and the preparation of a business case for investment in PETs.

Introduction

A substantial technical literature exists that describes privacy-enhancing technologies (PETs). On the other hand, there is a very limited literature on why organisations should encourage the adoption of PETs, invest in their development, and provide channels for their dissemination. The purpose of this chapter is to present a framework within which organisations can develop a business case for PETs.

The chapter commences by considering contexts in which trust and distrust of organisations by individuals are important factors in the achievement of organisational objectives. An examination is then undertaken of how an organisation's privacy strategy can make significant contributions to overcoming distrust and achieving trust. The role of information technology is then considered, including both privacy-invasive technologies ("the PITs"), and those that protect and enhance privacy. A taxonomy of PETs is presented, which distinguishes among mere pseudo-PETs, PETs that are designed as countermeasures against specific PITs, tools for uncrackable anonymity ("savage PETs"), and "gentle PETs" that seek a balance between nymity and accountability. Opportunities for organisations to incorporate PET-related initiatives within their privacy strategies are examined, and the development of business cases is placed within a broader theory of cost-benefit-risk analysis.

Trust and Distrust

This chapter is concerned with how organisations construct business cases for the application of technology in order to preserve privacy. The need for this arises in circumstances in which firstly either trust is lacking or distrust inhibits adoption, and secondly effective privacy protections can be a significant factor in overcoming the trust gap.

Trust is confident reliance by one party about the behaviour of other parties (Clarke, 2002). It originates in social settings. Many of the elements evident in social settings are difficult for organisations to replicate in merely economic contexts. Hence a great deal of what organisations call trust is merely what a party has to depend on when no other form of risk amelioration strategy is available to them.

If trust can be achieved, then it may become a positive driver of behaviour. A more common pattern, however, is for distrust to exist. This represents an impediment to fulfilment of the organisation's objectives, because it undermines the positive impacts of other drivers such as cost reductions and convenience.