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

ITB15307

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

Chapter VIII

Privacy through Security: Policy and Practice in a Small-Medium Enterprise

Ian Allison, The Robert Gordon University, UK

Craig Strangwick, ABC Awards Ltd, UK

Abstract

The chapter discusses how one small business planned for, and implemented, the security of its data in a new enterprise-wide system. The company's data was perceived as sensitive, and any breach of privacy as commercially critical. From this perspective, the chapter outlines the organizational and technical facets of the policies and practices evidenced. Lessons for other businesses can be drawn from the case by recognizing the need for investments to be made that will address threats in business critical areas. By highlighting the need for organizations to understand the nature of the risk and the probability of an event occurring, the security approaches highlight the need to address both the threats and actions in the event of an incident to reduce the risk to privacy.

Introduction

Privacy often is discussed in the literature as an ethical issue, whereby members of society are perceived to have a right to privacy and that right is considered to be eroded through the application of information technology. The Internet and supporting architectures are considered to make privacy more vulnerable because behaviour can be monitored, personal data can be commodified and exchanged, and data can be combined from different sources to enable analysis of individuals' records (e.g. Spinello, 2006; Tavani, 2004). The invasion of privacy is seen to occur through the access to, and control of, personal information.

Consequently, debates in the literature focus on what we understand privacy to be, the degree to which privacy can be taken as a right, to what degree privacy should be protected and how computer technology affects privacy. In other words, the morality of individual, organizational, and societal actions is evaluated. What is ignored in these debates is the business implication of privacy and how this shapes information security activity within organizations.

Security research, on the other hand, focuses on the threat of attack by hackers or malware, and the tools and technical solutions available to address these threats. The need to develop secure architectures or build applications that avoid security pitfalls, whilst important, mostly does not address the way in which such decisions affect privacy.

This chapter, therefore, seeks to straddle these two fields to show how organizations need to take privacy into account as a business issue in order that this shapes information security policies and practice. To achieve this we draw on the experiences of one small-medium enterprise (SME). The formal definition of SMEs varies from country to country, but for the purposes of this chapter we have defined SMEs as employing less than 500 people. This definition does not mean that the lessons are not applicable to larger organizations but that the focus of the study, and data drawn from previous studies, matches this definition.

The remainder of this chapter begins by outlining why privacy is a business issue, recognising the financial and legal imperatives organizations face. Current security policies and practices in SMEs worldwide are then reviewed highlighting the weaknesses currently evident in the way that SMEs approach their information security.

The focus of the chapter is a case study based on ABC Awards Ltd, a small UK-based assessment body who offers vocational qualifications through a variety of learning centres. The study relates to their development of an enterprise-wide information system and underpinning infrastructure. Policy and practice were developed to