Int. J. Production Economics 115 (2008) 104–112

Contents lists available at ScienceDirect

Int. J. Production Economics

journal homepage: www.elsevier.com/locate/ijpe

Can business process reengineering lead to security vulnerabilities: Analyzing the reengineered process

Sanjay Goel *, Vicki Chen

BA310b, School of Business, University at Albany, SUNY General Electric Energy, 1400 Washington Avenue, Albany, NY 12222, USA

ARTICLE INFO

Article history:
Received 1 June 2006
Accepted 20 May 2008
Available online 24 May 2008

Keywords:
Security
Risk analysis
Information assurance
Business process reengineering (BPR)
Six sigma
General electric

ABSTRACT

Digitization, while a boon for business productivity, carries inherent liability for information security. During the last few decades, companies have reengineered business processes on the back of digital data and computer networks. Recently, companies are beginning to realize that increased accessibility, and productivity, carries a hidden cost of making the data more vulnerable to security breaches. It makes intuitive sense to incorporate information security into strategic decision-making during business process reengineering. However, the intricate and complex nature of information security obscures the return on security investment, making companies reluctant to invest in security policies or technology. Consequentially, companies are often forced to suboptimally retrofit security into their business processes in response to security breaches. The case study presents an information security risk analysis proactively conducted at General Electric Energy's Wind Division after the business process reengineering of their product data storage and sharing process. The goal of the study was to identify the security risks in the redesigned process using a structured matrix-based risk analysis approach that links the assets of the organization at risk to security controls.

1. Introduction

Information technology has been the primary driver in business process reengineering (BPR) (Malhotra, 1998) efforts in firms. This has led to improved efficiencies in back office operations as well as improved availability of services (Hammer and Champy, 1993). However, digitization of data, while essential for reengineering, increases the data's vulnerability to information security[1] breaches. Early efforts at BPR failed to recognize the importance of integrating security into the design. Before the digital age, information security was not a major concern; consequentially, the hidden cost of digital security is not considered by corporations when computing return-on-investment (ROI) for their BPR projects. Business processes need to be scrapped and fundamentally rebuilt in order to incorporate security most efficiently (Hammer, 1990; Hall et al., 1993; Davenport and Stoddard, 1994). Fear of law suits and other financial losses caused by security breaches that could result in incidents such as leakage of personal confidential information, disclosure of export controlled information, or terrorist attacks are forcing many companies to re-evaluate their current security practices and standards. These companies are thus attempting to retroactively add security to their processes at a significant cost. Companies are also responding to the proliferation of government legislations such as SOX, FISMA, HIPAA, and FERPA that mandate security risk analysis in organizations to protect personal confidential information. However, security is still considered an impediment to productivity and a forced mandate rather than an intrinsic element of conducting business.

* Corresponding author. Tel.: +1 518 442 4925.
E-mail address: goel@albany.edu (S. Goel).

[1] Hereafter security in this context will mean information security.

0925-5273/$ - see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.ijpe.2008.05.002

Faced with ever changing threats and possible solutions, managers struggle to make security decisions. They analyze risks routinely in their activities; however, they may be unable to comprehend the security problem due to its complexity. Comprehensive security risk analysis involves assessing the dependencies between assets, vulnerabilities, threats, and controls (Goel and Chen, 2005). As the number of parameters grows in each of these categories, the combinatorial complexity increases rapidly. Given the limits of human cognitive ability (Miller, 1956), even smaller information security risk problems contain enough parameters that managers find these problems difficult to grasp. Consequently, it is imperative to use cognitive aids while analyzing security risks.

The goal of security risk management is to institute controls that mitigate risks to acceptable levels. Several techniques for analyzing security risks have been proposed. These techniques assist in prioritizing the deployment of controls based on the value of assets at risk. Most of the classical risk analysis techniques however are quantitative (Ozier, 1989; Vose, 2000; Littlewood et al., 1992), firmly rooted in reliability theory (Aven, 1992; Andrews and Moss, 1993) or probability theory (Mosleh et al., 1985; Schneier, 1999; Sahinoglu, 2005). They typically require probabilities of events and values of assets at risk to compute the exposure of the organization. They also need values for effectiveness of controls. Given changing assets, evolving threats, and rapidly emerging vulnerabilities, it is infeasible to accurately estimate these values, making quantitative methods an impractical approach for large-scale security risk analysis. On the other hand, very few qualitative techniques (Baskerville, 1993) are available. These techniques rely on relative comparisons and expert judgment in making security decisions. In some of the earliest work on security risk analysis, analysts have relied on checklists developed from industry standards or government mandates to estimate risk. Auditors (Krauss, 1972, 1980) commonly apply such checklists even today to ensure compliance with accepted industry practice. Fuzzy sets and possibility theory have also been considered for computing risks (Baskerville and Portougal, 2003; Zadeh, 1965, 1978; Dubois and Prade, 2001). Though such techniques provide more latitude in collecting data, it is still hard to obtain suitable data for risk modeling.

Contrary to general perception, security is not a purely technical decision; rather, it is a financial assessment where security investments should be commensurate with the value of assets at risk. Computing precise valuations of controls and security risk exposure involves detailed quantitative analysis, requiring probabilities of threats, valuation of assets, and effectiveness coefficients for controls. Such information is sparse and typically unreliable in practice. Several security management tools have been developed including OCTAVE (Alberts and Dorofee, 2003), CCTA/CRAMM (Barber and Davey, 1992; CCTA, 1991, 1993), CORAS (Stølen et al., 2002; Dimitrakos et al., 2002), and Stride (Casteele, 2004). These tools integrate multiple techniques that are woven together into a monolithic user interface. However, they are quite cumbersome to use and are typically black boxes to risk analysts which makes it difficult for them to incorporate intuitive judgment during analysis. Given the uncertainty in risk analysis, it is important to couple human judgment with analytic methods. An alternate matrix-based approach for risk analysis is suggested by Goel and Chen (2005) in which relative rankings of asset valuation, level of vulnerability, chances of manifestation of threat, and effectiveness of controls are aggregated to determine the appropriate set of controls. In this approach information is compactly organized into a cascading series of matrices that makes comprehension easier. In addition, the approach ensures transparency of data, thereby allowing analysts to isolate the importance of each asset, vulnerability, threat, and control by navigating through the matrices. The valuations and decisions on selecting controls are then made by experts who use their qualitatively judgment.

This paper briefly discusses the methodology and its application in a case study conducted at General Electric (GE) Energy Wind Division case study. The rest of this paper is organized as follows: Section 2 summarizes the matrix-based risk analysis methodology; Section 3 presents the case study; Section 4 discusses observations, and Section 5 contains concluding remarks.

2. Information security risk analysis

Security risk analysis involves a multi-step process of determining exposure to security threats that an organization faces. First, organizational assets, vulnerabilities, and threats are identified. Next, potential for exploitation of vulnerabilities by threats and the consequent damage to assets is estimated. Finally, a control strategy is developed that reduces the risks to manageable levels.

Assets are the organization's valuables impacted by security breaches in information systems. These include both tangible assets such as software, hardware, and data; and intangible assets such as reputation, trust, and morale. Vulnerability is a weakness in the organization that opens the door for threats to enter. There are several sources of vulnerabilities, including external adversaries (such as hackers, terrorists, and rogue government agents), information systems themselves (such as access control, software, databases, backup devices, and physical system access), human factors (such as malicious insiders, and human errors), environmental factors (such as storms, fire, and flood), and organizational factors (such as poor security policies, activities that encourage activism, etc.).

Risk analysis requires determining dependencies between assets, threats, and vulnerabilities either qualitatively via expert opinions or quantitatively using collected data. Risk analysis can be an endless process; it is therefore necessary to carefully define the scope of the analysis and focus on specific problems. This paper analyzes security risks in the context of the redesigned fulfillment process for general electric wind turbines, using the framework developed by Goel and Chen (2005). It evaluates the potential exposure in the redesigned process and suggests further refinements based on risk analysis. It also examines the controls required to manage exposure based on a cost–benefit analysis of the controls.