Chapter 2
Combined Impact of Outsourcing and Hard Times on BPO Risk and Security

C. Warren Axelrod
Delta Risk, USA

Sukumar Haldar
Anshinsoft Inc., USA

ABSTRACT

The security of business processes, particularly those based on IT (information technology) systems, is at increased risk when the processes are outsourced, especially during difficult economic times. This chapter examines factors affecting the cyber security of BPO (business process outsourcing) and argues that the combination of effects of outsourcing and the economic environment leads to even greater levels of risk than do the individual components. Suggestions are made as to how the risks might be mitigated.

INTRODUCTION

IT-based BPO arrangements continue to proliferate in the current difficult economic conditions, as private companies, government agencies, and other organizations seek to reduce their costs. The potential for compromise from cyber security exploits also increases, however. Over the past decade, the expansion of BPO, particularly offshore, was during times of continued economic growth, save for the recession around 2001 when a number of major outsourcers failed, giving little or no notice, as described in (Berinato, 2001). Prosperous times tend hide nefarious activity. However, when the tide recedes, questionable activities are exposed, as for example with Satyam. Motivation for exploiting outsourced services generally rises.

Threats posed by insiders, in particular, are thought to increase considerably as employees are fired and remaining employees are both disgruntled and feel threatened economically. Insider threat is difficult to measure since insiders operate using authorized access and practices. Consequently, while one might expect computer crime generally to increase when individuals are

DOI: 10.4018/978-1-60960-123-2.ch002

suffering economic hardship, any measures of such increases will be called into question since many exploits by insiders are not detected, and many of those that are detected most often go unreported.

RISKS OF OUTSOURCING

As business processes are moved outside the organization domestically or offshore, they usually become more dependent than previously on communications networks in order to connect outsourcers and client organizations. The economics for long-distance and international communications greatly favor the use of the Internet public network over private networks. Even when the communications are between known and trusted entities and individuals, the use of public networks exposes systems to cyber attack by others.

Often, outsourced business processes rely on computer systems that were developed for internal use by trusted employees. When access to these systems is granted to a service provider's employees, different access rights may be appropriate. However, restrictions on access to sensitive data, and on the handling of such data, may not be feasible with the current systems nor may the client organization realize the need to restrict data access and the functional capabilities of computer applications.

Another important, if not the most important, risk of outsourcing is that which relates to humans. Third-party service providers' employees may not have the same commitment to the client company that internal employees do. They may not have the understanding of the business environment and processes of the client company, nor sufficient training in regard to security and privacy. When the service provider is located offshore, other factors must be considered relating to differences in culture, language, physical and cyber infrastructures, legal and regulatory requirements, time zones, travel distances, and so on.

While there are certainly variations among researchers with respect to specific risk categories and their scope, for the most part there is commonality, as the mapping in Table 1 illustrates.

RISKS OF ECONOMIC DISTRESS

There are a number of threats that, while always present, are exacerbated by significant changes and economic stress, as described in a series of blogs (Axelrod, 2008). That these concerns are now mainstream is illustrated by the summary of many of these threats and their potential impact in recent articles (Campbell, 2009) and (Zarrella, 2009).

They include the following:

- Propensity to engage in fraudulent activities (for financial gain)
- Propensity to engage in destructive activities as a result of feeling disgruntled, wronged, etc. (for revenge)
- Increased opportunity for crime due to less stringent controls and employee apathy
- Increased vulnerabilities due to change and confusion relating to bankruptcies, mergers, and acquisitions

As can be seen from the above, risks in hard times derive from increasing numbers of vulnerabilities, opportunities, and propensities. The propensity to engage in fraudulent and other criminal activities is significantly increased in hard times as the pressure to continue to maintain a particular lifestyle or to pay off debts lowers the resistance of law-abiding citizens to overtures by predatory criminals. At the same time, people are more distracted and therefore less likely to recognize social engineering exploits. These factors are addressed elsewhere (Axelrod, 2009)