Category: Business Information Systems

Information Technology Business Continuity

Vincenzo Morabito
Bocconi University, Italy

Gianluigi Viscusi
University of Milano, Italy

INTRODUCTION

Continuity could be and should be strategic for the business competitive advantage. Besides natural disaster, from blackout to tsunami, businesses face in daily activities critical challenges in IT management for assuring business continuity; for example, business continuity management results must be strategic, because of the infrastructural, organizational, and information systems changes that are required to assure compliance with regulatory norms (see, e.g., the impact of Basel II norms in financial sector), or must have and maintain a time-to-market advantage (disasters can facilitate competitors in a first mover perspective). Nevertheless, business continuity is at present often synonymous with risk management at the IT level, disaster recovery at the hardware level, or in the best case—at the data management level—with data quality management. These perspectives fail to unveil the strategic value of IT business continuity as a framework assuring alignment of strategy, organization, and systems, allowing a competitive advantage in a dynamic competitive environment. Moreover, even when business continuity, under these perspectives, has become one of the most important issues in IT management, there still appears to be some discrepancy as to the formal definitions of what precisely constitutes a disaster, and there are difficulties in assessing the size of claims in the crises and disaster areas. Taking these issues into account, we propose: (a) an analysis of the different facets of the concept of business continuity, and (b) an integrated framework for strategic management of IT business continuity. To these ends, we move from the finance sector—a sector in which the development of information technology (IT) and information systems (IS) have had a key impact upon competitiveness. Indeed, banking industry IT and IS are considered "production," not "support" technologies. The evolution of IT and IS has challenged the traditional ways of conducting business within the finance sector. These changes have largely represented improvements to business processes and efficiency but are not without their flaws, in as much as business disruption can occur due to IT and IS sources. The greater complexity of new IT and IS operating environments requires that organizations continually reassess how best they may face changes and exploit these later for organizational advantage. As such, IT and IS have supported massive changes in the ways in which business is conducted with consumers at the retail level. Innovations in direct banking would have been unthinkable without appropriate IS, and merger and acquisition (M&A) initiatives represent the ideal domain to show what value can lead strategic management of IT business continuity. Taking these issues into account, we point out the relevance of continuity for maintaining customers, and time-to-market in complex and evolutionary competitive environments. Due the relevance of IT to maintain a value-added continuity, our contribution aims to clarify the concept of IT business continuity, providing a framework, exploiting the different facets that it encompasses, and showing the strategic implications to the field of IS&T.

BACKGROUND

The evolution of IT and IS has challenged the traditional ways of conducting business within the finance sector, as a consequence of new business models emerging, for example, from e-business (Müller, Viering, Ahlemann, & Riempp, 2007; Pennings & Harianto, 1992; Ross, Vitale, & Weill, 2001). These changes have largely represented improvements to business processes and efficiency, introducing new challenges and critical issues as much as business interruptions can occur due to IT and IS sources. The greater complexity of new IT and IS operating environments requires that organizations continually reassess how challenges change and exploit those for organizational competitive advantage. In particular, this article seeks to investigate how companies in the financial sector understand and manage their business continuity problems. In fact, business continuity has become one of the most important issues in the banking industry (Lam, 2002), but its relationship with disaster recovery still causes some discrepancy in providing a formal definition on the one hand of what precisely constitutes a disaster, and on the other hand of what is business continuity beyond disaster recovery. Taking into account the different typologies of disaster that can occur in particular in the financial sector (Lam, 2002; Nemzow, 1997), we can define a disaster as an incident that leads to the formal invocation of contingency/continuity plans or any incident that leads to a loss of

revenue; indeed, we can consider a disaster any accidental, natural, or malicious event that threatens or interrupts normal operations or services, causing the failure of the enterprise. In the area of organizational crises and disasters, the degree to which a company has been affected by one or more of such interruptions is the defining factor.

These preliminary definitions are relevant because as estimated by the Business Continuity Institute (2007), most organizations facing a significant crisis, without either a contingency/recovery or a business continuity plan, fail to maintain market position competitively or even to survive a year further. Moreover, state-of-the-art analyses (Bank of Japan, 2003; Barnes, 2001; Elliott & Swartz, 1999; Lam, 2002; Nemzow, 1997; Zambon, Bolzoni, Etalle, & Salvato, 2007) point out that only a small number of organizations have disaster and recovery plans, and among those, few have been renewed to reflect the changing nature of the organization.

In this article we consider in particular our experience in studying practices of the Italian banking industry, where major differences emerge in preparing and implementing strategies that enhance business process security. Comparing them with state-of-the-art literature, we notice two prevalent approaches. On the one hand, there are disaster recovery (DR) strategies that are internally and hardware focused (Lewis, Watson, & Pickren, 2003); on the other hand, there are strategies that treat the issues of IT and IS security within a wider internal-external, hardware-software framework. The latter deals with IS as an integrating business function rather than as a standalone operation. We consider this second type of strategy as part of what in literature (Barnes, 2001; British Standard Institute, 2006; Cerullo & Cerullo, 2004; Nemzow, 1997) is defined as business continuity planning (BCP). Taking these issues into account, we point out the need for a comprehensive IT business continuity approach because of the relevance of the IT for the business continuity of the organizations in the finance sector, encompassing technological, organizational, and strategic facets of the whole system carrying out the business activities. We define the IT business continuity approach (IT-BCA) as a framework of disciplines, processes, and techniques aiming to provide continuous operation for essential business functions under all circumstances. IT-BCA considers business continuity planning as a core element of business continuity initiatives.

More specifically, business continuity planning can be defined as "a collection of procedures and information [that have been] developed, compiled and maintained [and are] ready to use—in the event of an emergency or disaster"(Elliott & Swartz, 1999). BCP has been addressed by different contributions to the literature, such as Allen's (2001) studies on Cert's Octave method, the activities of the Business Continuity Institute (2007) and of the British Standard Institute (2006) in defining certification standards and practice guidelines, the EDS white paper on Business Continuity Management (Decker, 2004), and the activity of financial institutions such as the study carried out by the Bank of Japan (2003). This last study illustrates the process and activities for successful business continuity planning in three steps:

1. formulating a framework for robust project management,
2. identifying assumptions and conditions for business continuity planning, and
3. introducing action plans.

Considering the first step above, banks should (i) develop basic policy and guidelines for business continuity planning (*basic policy*); (ii) develop a study of firm-wide aspects (*firm-wide control section*); and (iii) implement appropriate progress control (*project management procedures*). In the second step, banks should (i) recognize and identify the potential threats, analyze the frequency of potential threats, and identify the specific risk scenarios (*disaster scenarios*); (ii) focus on continuing prioritized critical operations (*critical operations*); and (iii) target times for the resumption of operations (*recovery time objectives*).

Finally, in the third step where actions plans must be introduced, the banks should (i) study specific measures for business continuity planning (*business continuity measures*); (ii) acquire and maintain backup data (*robust backup data*); (iii) determine the managerial resources and infrastructure availability capacity required (*procurement of managerial resources*); (iv) determine strong time constraints, a contact list, and a means of communication on emergency decisions (*decision-making procedures and communication arrangements*); (v) realize practical operational procedures for each department and level (*practical manual*); and (vi) implement a test/training program (*testing and reviewing*).

IT business continuity, indeed, is not only an IT/IS issue, but involves organizational facets, having a strategic impact on banks' competitive advantage and value.

IT BUSINESS CONTINUITY AS A STRATEGIC PATH TO VALUE

In this section we discuss the IT business continuity approach as a path to value for banks, encompassing three fundamental facets that can be viewed in a systemic way: *technology, people,* and *process.*

Technology refers to the recovery of mission-critical data and applications contained in the Disaster Recovery Plan (DRP). It establishes technical and organizational measures in order to face events or incidents with potentially huge impact that could even lead to the unavailability of data centers. The DRP development defines and ensures IT emergency procedures that intervene and protect the data relevant for