DOI: 10.1145/1666420.1666452

BY FABIO ARDUINI AND VINCENZO MORABITO

Business Continuity and the Banking Industry

SINCE THE SEPTEMBER 11TH ATTACKS on the World Trade Center,[8] tsunami disaster, and hurricane Katrina, there has been renewed interest in emergency planning in both the private and public sectors. In particular, as managers realize the size of potential exposure to unmanaged risk, insuring "business continuity" (BC) is becoming a key task within all industrial and financial sectors (Figure 1).

Aside from terrorism and natural disasters, two main reasons for developing the BC approach in the finance sector have been identified as unique to it: regulations and business specificities.

Regulatory norms are key factors for all financial sectors in every country. Every organization is required to comply with federal/national law in addition to national and international governing bodies. Referring to business decisions, more and more organizations recognize that Business Continuity could be and should be strategic for the good of the business. The finance sector is, as a matter of fact, a sector in which the development of information technology (IT) and information systems (IS) have had a dramatic effect upon competitiveness. In this sector, organizations have become dependent upon technologies that they do not fully comprehend. In fact, banking industry IT and IS are considered production not support technologies. 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. As a consequence business continuity planning at banks is essential as the industry develops in order to safeguard consumers and to comply with international regulatory norms. Furthermore, in the banking industry, BC planning is important and at the same time different from other industries, for three other specific reasons as highlighted by the Bank of Japan in 2003:

- *Maintaining the economic activity of residents in disaster areas*[2] by enabling the continuation of financial services during and after disasters, thereby sustaining business activities in the damaged area;
- *Preventing widespread payment and settlement disorder*[2] or preventing systemic risks, by bounding the inability of financial institutions in a disaster area to execute payment transactions;
- *Reduce managerial risks*[2] for example, by limiting the difficulties for banks to take profit opportunities and lower their customer reputation.

Business specificities, rather than regulatory considerations, should be the primary drivers of all processes. Even if European (EU) and US markets differ, BC is closing the gap. Progressive EU market consolidation necessitates common rules and is forcing major institutions to share common knowledge both on organizational and technological issues.

The financial sector sees business continuity not only as a technical or risk management issue, but as a driver towards any discussion on mergers and acquisitions; the ability to manage BC should also be considered a strategic weapon to reduce the acquisition timeframe and shorten the data center

merge, often considered one of the top issues in quick wins and information and communication technology (ICT) budget savings.

Business Continuity Concepts

The evolution of IT and IS have 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 keep abreast of changes and exploit those for organizational advantage. In particular, this paper seeks to investigate how companies in the financial sector understand and manage their business continuity problems.

BC has become one of the most important issues in the banking industry. Furthermore, 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.

One definition of what constitutes a disaster is an incident that leads to the formal invocation of contingency/continuity plans or any incident which leads to a loss of revenue; in other words it is any accidental, natural or malicious event which threatens or disrupts normal operations or services, for as long a time as to significantly cause the failure of the enterprise. It follows then that when referring to the size of claims in the area of organizational crises and disasters, the degree to which a company has been affected by such interruptions is the defining factor.

The definition of these concepts is important because 80% of those organizations which face a significant crisis without either a contingency/recovery or a business continuity plan, fail to survive a further year (Business Continuity Institute estimate). Moreover, the BCI believes that only a small number of organizations have disaster and recovery plans and, of those, few have been renewed to reflect the changing nature of the organization.

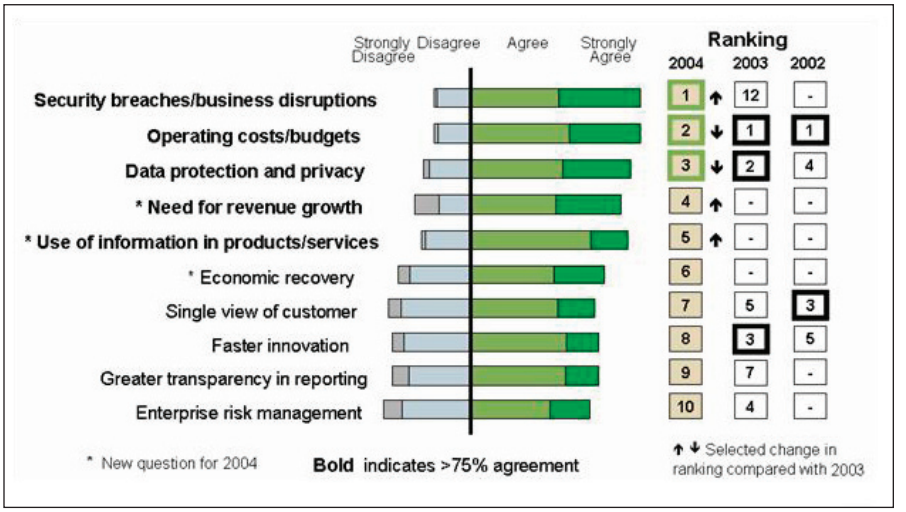
In observing Italian banking industry practices, there seems to be major differences in preparing and implementing strategies that enhance business process security. Two approaches seem to be prevalent. Firstly, there are those disaster recovery (DR) strategies that are internally and hardware-focused[9] and secondly, there are those 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 stand-alone operation. We have labeled this second type of business continuity approach (BCA).

As a consequence, we define BCA as a framework of disciplines, processes, and techniques aiming to provide continuous operation for "essential business functions" under all circumstances.

More specifically, business continuity planning (BCP) 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."[6] BCP has been addressed by different contributions to the literature. Noteworthy studies include Julia Allen's contribution on Cert's Octave method[a1] the activities of the Business Continuity Institute (BCI) in defining certification standards and practice guidelines, the EDS white paper on Business Continuity Management[4] and finally, referring to banking, Business Continuity Planning at Financial Institutions by the Bank of Japan.[2] This last study illustrates the process and activities for successful business continuity planning in three steps:

1. Formulating a framework for robust project management, where banks should:
   a. develop basic policy and guidelines for BC planning (basic policy);
   b. Develop a study firm-wide aspects (firm-wide control section);
   c. Implement appropriate progress control (project management procedures)
2. Identifying assumptions and conditions for business continuity planning, where banks should:
   a. Recognize and identify the potential threats, analyze the frequency of potential threats and identify the specific scenarios with material risk (Disaster scenarios);
   b. Focus on continuing prioritized critical operations (Critical operations);
   c. Target times for the resumption of operations (Recovery time objectives);
3. Introducing action plans, where banks should:
   a. Study specific measures for business continuity planning (BC measures);
   b. acquire and maintain back-up data (Robust back-up data);
   c. Determine the managerial resources and infrastructure availability capacity required (Procurement of managerial resources);

Figure 1. 2004 top business priorities in industrial and financial sectors (source Gartner)



a The Operationally Critical Threat, Asset, and Vulnerability Evaluation Method of CERT. CERT is a center of Internet security expertise, located at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University.

d. Determine strong time constraints, a contact list and a means of communication on emergency decisions (Decision-making procedures and communication arrangements);
e. Realize practical operational procedures for each department and level (Practical manual)

4. Implement a test/training program on a regular basis (Testing and reviewing).

Business Continuity Aspects

The business continuity approach has three fundamental aspects that can be viewed in a systemic way: *technology, people and process*.

Firstly, *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 in a worst case scenario could lead to the unavailability of data centers. Its development ought to ensure IT emergency procedures intervene and protect the data in question at company facilities. In the past, this was, whenever it even existed, the only part of the BCP.

Secondly, *people refers* to the recovery of the employees and physical workspace. In particular, BCP teams should be drawn from a variety of company departments including those from personnel, marketing and internal consultants. Also the managers of these teams should possess general skill and they should be partially drawn from business areas other than IT departments. Nowadays this is perceived as essential to real survival with more emphasis on human assets and value rather than on those hardware and software resources that in most cases are probably protected by backup systems.

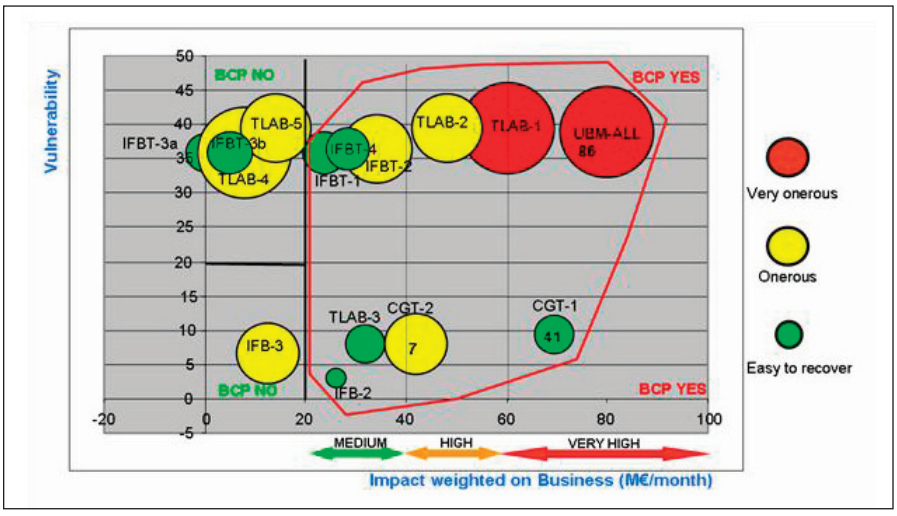
Finally, the term *process* here refers to the development of a strategy for the deployment, testing and maintenance of the plan. All BCP should be regularly updated and modified in order to take into consideration the latest kinds of threats, both physical as well as technological.

Whereas a simple DR approach aims at salvaging those facilities that are salvageable, a BCP approach should have different foci. One of these ought to be treating IT and IS security with a wider internal-external, hardware-software framework where all processes are neither in-house nor subcontracted-out but are a mix of the two so as to be an integrating business function rather than a stand alone operation. From this point of view the BCP constitutes a dual approach where management and technology function together.

In addition, the BCP as a global approach must also consider all existing relationships, thus giving value to clients and suppliers considering the total value chain for business and to protect business both in-house and out.

The BCP proper incorporates the disaster recovery (DR) approach but rejects its exclusive focus upon facilities. It defines the process as essentially business-wide and one which enables competitive and/or organizational advantages.

Figure 2. Vulnerability & business impact matrix



IT Focus Versus Business Focus as a Starting Point

The starting point for planning processes that an organization will use as its BCP must include an assessment of the likely impact different types of 'incidents' will/would make on the business. As far as financial companies are concerned, IT focus is critical since, as mentioned, new technologies continue to become more and more integral to on going financial activities. In addition to assessing the likely impact upon the entire organization, banks must consider the likely effects upon their different business areas. The "vulnerability & business impact matrix" (Figure 2) is a tool that can be used to summarize the inter-linkages between the various information system services, their vulnerability and the impact on business activities. It is useful in different ways.

To start, the BC approach doesn't focus solely upon IT problems but rather uses a business-wide approach. Given the strategic focus of BCP, an understanding of the relationships between value-creating activities is a key determinant of the effectiveness of any such process. In this way we can define correct BC perimeter (Figure 2) by trying to extract the maximum value from BCP within a context of bounded rationality and limited resources. What the BCP teams in these organizations have done is focus upon how resources were utilized and how they were added to value-creation rather than merely being "support activity" which consumes financial resources unproductively. In addition, the convergence of customer with client technologies also demands that those managing the BCP process are aware of the need to "... expand the contingency role to not merely looking inward but actually looking out." Such a dual focus uncovers the linkages between customer and client which create competitive advantage. Indeed, in cases where clients' business fundamentally depends upon information exchange, for instance many banks today provide online equity brokerage services, it might be argued that there is a 'virtual value chain' which the BCP team protects thereby providing the 'market-space' for value creation to take place. Finally, another benefit is that vulnerability and business impact can aid the prioritization of particular key areas.

New and Obsolete Technologies

Today's approach to BCP is focused on well-structured process management and business-driven paradigms. Even if some technology systems seem to be "business as usual," some considerations must be made to avoid any misleading conjecture from an analytical side.

When considering large institutions with systemic impact- not only on their own but on clients businesses as well- two key objectives need to be considered when facing an event. These have been named RPO (Recovery Point Objective) and RTO (Recovery Time Objective) as shown in Figure 3. RPO deals with how far in the past you have to go to resume a consistent situation; RTO considers how long it takes to resume a standard or regular situation. The definitions of RPO and RTO can change according to data center organization and how high a level a company wants to its own security and continuity to be.

For instance a dual site recovery system organization must consider and evaluate three points of view (Figure 3). These are: application's availability, BC process and data perspective.

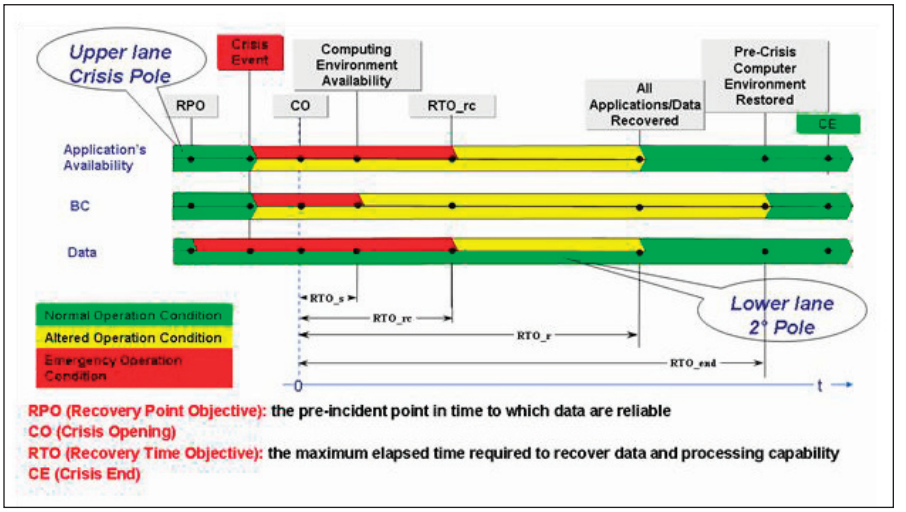
Data are first impacted (RTO) before the crisis event (CE) due to the closest "consistent point" from which to restart. The crisis opening (CO) or declaration occurs after the crisis event (CE).

"RTO_s," or computing environment restored point, considers the length of time the computing environment needs in order to be restored (for example, when servers, network etc. are once again available); "RTO_rc," or mission critical application restarted point, indicates the "critical or vital applications" (in rank order) are working once again; "RTO_r," or applications and data restored point, is the point from which all applications and data are restored, but (and it is a big but) "RTO_end," or previous environment restored point, is the true end point when the previous environment is fully restored (all BC solutions are properly working). Of the utmost importance is that during the period between "RTO_r" and "RTO_end" a second disaster event could be fatal!

Natural risks are also increasing in scope and frequency, both in terms of floods (central Europe 2002) and hurricanes (U.S. 2005), thus the coining of an actual geographical recovery distance, today considered more than 500 miles. Such distance is forcing businesses and institutions alike to consider a new technological approach and to undertake critical discussion on synchronous-asynchronous data replication: their intervals and quality. Therefore, more complex analysis about RPO and RTO is required.

However the most important issue, from a business point of view when faced with an imminent and unforeseen disaster, is how to reduce restore or restart time, trying to shrink this window to mere seconds or less. New pushing technologies (SATA – Serial ATA and MAID – Massive Arrays Inexpensive Disk) are beginning to make some progress in reducing the time problem.

Figure 3. RPO & RTO



Business Focus Versus Value Chain Focus

The business area selected by the "vulnerability and business impact analysis matrix" should be treated in accordance with the value chain and value system. In addition to assessing the likely disaster impact upon IT departments, organizations should consider disaster impacts over all company departments and their likely effects upon customers. Organizations should avoid the so-called Soccer Star Syndrome.6 In drawing an analogy with the football industry, one recognizes that greater management attention is often focused on the playing field rather than the unglamorous, but very necessary, locker room and stadium management support activities. Defenders and goalkeepers, let alone the stadium manager, do not get paid at the same level as the star player, yet their functions are just as vital to achieving the overall objectives of the football team. The value chain provides an opportunity to examine the connection between the exciting and the hum drum links that deliver customer value. The evolution of crisis preparations from the IT focused disaster recovery (DR) solutions towards the BC approach reflects a growing understanding that business continuity depends upon the maintenance of all elements which provide organizational efficiency-effectiveness and customer value, whether directly or indirectly.

Prevention Focus of Business Continuity

A final key characteristic of the BC approach concerns its primary role in prevention. A number of authors have identified that the potential for crises is normal for organizations.[7,11] Crisis avoidance requires a strategic approach and requires a good understanding of both the organization's operating processes, systems and the environment in which it operates.

In the BC approach, a practice organization should develop a BCP culture to eliminate the barriers to the development of crisis prevention strategies. In particular, these organizations should recognize that incidents, such as the New York terrorist attach or the City of London bombings are merely triggered by external technical causes and that their effects are largely determined by internal factors that were within the control of their organizations. In these cases a cluster of crises should be iden-

tified. Such clusters should be categorized along the axis of internal-external and human/social-technical/economic causes and effects. By adopting a strategic approach, decisions could be made about the extent of exposure in particular product markets or geographical sites. An ongoing change management program could contribute to real commitment from middle managers who, from our first investigation, emerged as key determinants of the success of the BC approach.

Management Support and Sponsorship

BCP success requires the commitment of middle managers. Hence managers need to avoid considering BCP as a costly, administrative inconvenience that diverts time away from money-making activities. All organizational levels should be aware of the fact that BCP was developed in partnership between the BCP team and front line operatives. As a result, strategic business units should own BCP plans. In addition, CEO involvement is key in rallying support for the BCP process.

Two other key elements support the BC approach. Firstly, there is the recognition that responsibility for the process rests with business managers and this is reinforced through a formal appraisal and other reward systems. Secondly, peer pressure is deemed important in getting laggards to assume responsibility and so affect a more receptive culture.

Finally, BCP teams need to regard BCP as a process rather than as a specific end-point.

Conclusion

Although the risk of terrorism and regulations are identified as two key factors for developing a business continuity perspective, we see that organizations need to adopt the BC approach for strategic reasons. The trend to adopt a BC approach is also a proxy for organizational change in terms of culture, structure and communications. The BC approach is increasingly viewed as a driver to generate competitive advantage in the form of resilient information systems and as an important marketing characteristic to attract and maintain customers.

Referring to organizational change and culture, the BC approach should be a business-wide approach and not an IT-focused one. It needs supportive measures to be introduced to encourage managers to adhere to the BC idea. Management as a whole should also be confident that the BC approach is an ongoing process and not only an end point that remains static upon completion. It requires changes of key assumptions and values within the organizational structure and culture that lead to a real cultural and organizational shift. This has implications for the role that the BC approach has to play within the strategic management processes of the organization as well as within the levels of strategic risk that an organization may wish to undertake in its efforts to secure a sustainable competitive or so called first mover advantage. C

References

1. Allen J.H. *CERT® Guide to System and Network Security Practices.* Addison Wesley Professional, 2001.
2. Bank of Japan, Business Continuity Planning at Financial Institutions, July 2003. http://www.boj.or.jp/en/type/release/zuiji/kako03/fsk0307a.htm
3. Cerullo V. and Cerullo, J. Business continuity planning: A comprehensive approach. *Informtion System Management Journal*, Summer 2004.
4. Decker A. Business continuity management: A model for survival. *EDS White Paper*, 2004.
5. Dhillon, G. The challenge of managing information security. In *International Journal of Information Management 1*, 1(2004), 243–244.
6. Elliott D. and Swartz E. Just waiting for the next big bang: Business continuity planning in the uk finance sector. *Journal of Applied Management Studies 8*, 1 (1999), 45-60.
7. Greiner, L. Evolution and revolution as organisations grow. In *Harvard Business Review* (July/August) reprinted in Asch, D. & Bowman, C. (Eds) (1989) Readings in Strategic Management (London, Macmillan), 373-387.
8. Lam, W. Ensuring business continuity. *IT Professional 4*, 3 (2002), 19 - 25
9. Lewis, W. and Watson, R.T. Pickren A. An empirical assessment of IT disaster risk. *Comm. ACM 46*, 9 (2003), 201-206.
10. McAdams, A.C. Security and risk management: A fundamental business issue. *Information Management Journal 38*, 4 (2004), 36–44.
11. Pauchant, T.C. and Mitroff, I. Crisis prone versus crisis avoiding organisations: is your company's culture its own worst enemy in creating crises?. *Industrial Crisis Quarterly 2*, 4 (1998), 53-63.
12. Quirchmayr, G. Survivability and business continuity management. In *Proceedings of the 2nd Workshop on Australasian Information Security, Data Mining and Web Intelligence, and Software Internationalisation.* ACSW Frontiers (2004).

Vincenzo Morabito (vincenzo.morabito@unibocconi.it) is assistant professor of Organization and Information System at the Bocconi University in Milan where he teaches management information system, information management and organization. He is also Director of the Master of Management Information System System at the Bocconi University.

Fabio Arduini (fabio.arduini@unicreditgroup.eu) is responsible for IT architecture and Business Continuity for defining the technological and business continuity statements for the Group according to the ICT department.