Morad Benyoucef, 
Samer Forzley 
School of Management, University of Ottawa 
{Benyoucef, sforzley}@management.uottawa.ca

Business Continuity Planning and Supply Chain Management

Business Continuity Planning (BCP) has evolved significantly and gained acceptance since the events of September 11, 2001. It is defined in the literature as an integrated set of formalized procedures used by an organization to recover from events that disrupt business operations. These procedures call for vertical and horizontal integration of all functional groups within the organization as well as with all external groups that interact with it. Information technology (IT) plays a central role in that integration. This paper reviews and discusses the current state of business continuity planning as it applies to the supply chain and points to the efforts undertaken by business and government to mitigate the risks of supply chain disruptions. The organization’s supply chain continuity plan must extend to all supply chain participants, as illustrated by real-life examples. The most advanced business continuity planning requires equally advanced IT tools to increase visibility both inside and outside the organization and to automate supply chain planning and execution. The paper therefore extends a framework for supply chain continuity to include an IT component that runs supply operations and supports a plan for their continuity.

Introduction

Perhaps one of the oldest and most recognized continuity plans was the biblical building of the ark by Noah:

and he went aboard the boat to escape—he and his wife and his sons and their wives. With them were all the various kinds of animals—those approved for eating and sacrifice and those that were not, along with all the birds and other small animals. They came into the boat in pairs, male and female, just as God had commanded Noah. (Genesis 7:8)

The survivors of the ark were tasked to continue life on Earth and repopulate it. Thus Noah’s ark itself is an example of a plan used to mitigate the consequences of a disaster (the flood) and guarantee continuity.

Short of divine intervention, humans cannot predict disasters and misfortunes. There is no need to reach far into history for examples of natural and human-made catastrophes that caused significant disruption. The span of only the last few years has witnessed terrible floods, fires, tsunamis, and hurricanes; nearly all of which are relatively common. For several of the most recent disasters, the response was quick and contained. Thanks to business continuity planning, the damage caused by these tragic events was minimized, and in many cases further disasters were averted.

Business continuity planning (BCP) is “an integrated set of formalized procedures and resource information that companies can use to recover from a disruption of business operations” (Melynky, Zsidisin, & Ragatz, 2005). BCP is fairly new. It was not until World
War II that it started to take shape as a science, and not until the events of September 11, 2001, that it started gaining acceptance in corporate boardrooms. It was not until 2002 that the Sarbanes-Oxley Act (SOA) came into effect to force organizations to perform (among other tasks) recovery procedures for their data (Decker, 2005), activities that have always been vital in resuming normal operation after a disruption. Beyond recovery of data, BCP touches every function of the organization, making sure processes are available to continue the business operation, regardless of what happens. It involves all departments, beyond information technology (IT) into finance, marketing, shipping, receiving, and others. Most interesting, it is slowly expanding to cover entities that interact with the organization, such as customers and suppliers.

It is important to note that nowadays, governments are leading the way in BCP initiatives, in large part because they have the task of ensuring public safety and well-being. Indeed, governments worldwide have increased their spending on disaster recovery and relief programs. Nationwide disaster recovery can be expensive and usually requires public commitment and support. As observed by David Granniss of Harvard University's School of Government, “the current political, social, and security climate in the United States has provided the impetus for significantly larger domestic preparedness budgets at the federal, state, and local levels” (Granniss, 2003, p. 1). The U.S. government budgeted a staggering $38 billion for homeland security for the year 2003 alone. But this funding cannot be sustained forever. As stated by Granniss, “if no further terrorist attacks occur, this elevated level of spending will be difficult to maintain” (Granniss, 2003, p. 1).

Why does the U.S. government need to spend so much money on security? It would be a mistake to assume that the funding is strictly dedicated to counterterrorism measures such as tighter security at airports. The reality is that a significant portion of the money is being spent on securing the U.S. infrastructure and its supply chain. “Americans rely on these vast networks [supply chains] to provide everything from clean water and gasoline to electricity and telephone service. Most take their operability and reliability for granted until natural disasters, human error, or terrorists disrupt them” (Roberts, 2003, p. 1). A prime example is the power outage of 2003 (in parts of Canada and the United States) that caused leaders to realize the significant effort and funding necessary to ensure that electric systems run at optimal levels to avert disasters as much as possible. To ensure that the U.S. supply chain is protected, the Department of Homeland Security was instructed to address security in the supply chains of agriculture, food, water, public health, emergency services, government services, defense industrial base, information, and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, and postal and shipping services (Roberts, 2003).

Supply chain disruptions can directly affect corporate stock prices by nearly 9%, and revenue losses by 20%

Just because governments are responsible for the safety and well-being of the public, they don’t have to deal with these responsibilities alone. BCP costs are high and sometimes unsustainable, which is why some governments have started engaging the private sector for help. Kayyem and Chang (2002) outlined the following motivations for a U.S. public-private partnership in business continuity planning: (a) the private sector owns more than 80% of U.S. systems, 90% of which are in critical infrastructure; (b) September 11 made it clear that the private sector has a crucial role to play in emergency planning and response; (c) people spend the majority of their time away from home, inside private institutions; (d) the partnership will stave off inefficiency; and (e) involving the private sector in government initiatives in general is an important goal in itself. One obstacle to a true partnership is scarce financial recourse, given that most businesses still regard BCP as a cost item rather than a cash-generating item. Surprisingly, even when they do find and allocate resources for continuity planning, most businesses fail to take full advantage of BCP capabilities. In the United States, for instance, only 10% to 15% of large businesses have up-to-date BCP (the percentage is even lower for small businesses). Two out of five companies that experience a catastrophe never resume operations, and of those that do, one third go out of business within 2 years (Ekdlund, 2001).

One area that is often overlooked in business continuity planning is the firm’s supply chain (Computer Business Review, 2004), despite the fact that, in many industries, supply chain disruptions are on the rise (Singhal, 2005). The risk of supply chain disruption is defined as “the probability of an incident associated with inbound supply from individual supplier failures or the supply market” (Zsidisin, 2003, p. 222), usually resulting in the inability of the purchasing firm to meet the demands of its customers. Such disruptions can lead to large and unplanned cost increases, revenue reduction, and lower market share (Zsidisin, Ragatz, & Melnyk, 2003). The September 11 attacks, for instance, led to claims for more than $11 billion for related business interruptions (Pabai, 2004). Fortunately, as more and more firms begin to rely on the supply chain and capabilities of their suppliers, business managers and researchers are coming to realize the scope of supply chain disruptions (Zsidisin et al., 2003).
One question that comes to mind when a supply chain disruption occurs is “Is my IT infrastructure to blame?” It is no secret that, nowadays, supply chain planning (SCP) and supply chain execution (SCE) rely heavily on high-performance networks, hardware, and software. Thus, an IT-related failure can seriously disrupt the supply chain and affect many of its participants. Another question that comes to mind is “Are my supply chain partners to blame?” The supply chain is defined as the set of material and informational interchanges in the logistical process, stretching from acquisition of raw materials to delivery of finished products to the end user (Council of Supply Chain Management Professionals [CSCMP], 2005). All partners, from suppliers and service providers to customers, are links in that chain, and efficient SCP and SCE suppose that all these links act in harmony to avoid supply chain disruptions and to respond to them in harmony when they happen.

The objective of this paper is to discuss the role of an organization’s IT infrastructure as well as its relationships with suppliers in planning business continuity for the supply chain. The authors believe that because SCP and SCE rely on the organization’s IT infrastructure, the IT department in general and the chief information officer (CIO) in particular should be involved in ensuring the continuity of the supply chain. “Involved,” however, should not mean “in charge.” The organization’s chief operations officer (COO) should be “in charge” of the supply chain’s BCP, and through him or her, all members of the organization will find themselves involved. The CIO should be in charge of the continuity of the IT infrastructure, which runs all the firm’s business processes, including the supply chain. To support this argument, we extend Zsidisin et al.’s (2003) supply chain business continuity framework to include an IT component.

The paper is organized as follows. Section 2 defines and discusses the concepts of business continuity, disaster recovery, and risk management as well as the relationship between the three concepts. Section 3 addresses the role of IT in business continuity and disaster recovery. Section 4 details business continuity in the supply chain and includes reports on cases of supply chain disruptions that could have been avoided if business continuity planning had been extended to all supply chain participants. This section also discusses and extends Zsidisin et al.’s supply chain business continuity framework to include an IT component. Concluding remarks are given in Section 5.

**Business Continuity, Disaster Recovery, and Risk Management**

As defined by the Security and Privacy Research Center, business continuity “determines how a company will keep functioning until its normal facilities are restored after a disruptive event” (Scalet, 2005). Variations of this definition exist, but they share the primary emphasis on business continuity’s concern with finding alternative methods to continue operation in the event of a disaster. Disaster recovery, on the other hand, is defined as “the restoration of computing and telecommunication services after an event has disrupted those services” (Scalet, 2005). Again, experts suggest variations of this definition, but they all agree that disaster recovery is a reaction to a disaster, in a situation in which an asset is no longer available and must be recovered, restored, or replaced. How do business continuity and disaster recovery interact? The terms are sometimes used interchangeably, perhaps because both designate practices to assist a company in recovering from unforeseen disruptive events. An effective contingency plan should incorporate the elements of both disaster recovery and business continuity. In essence, disaster recovery is concerned with the technical recovery processes, whereas business continuity is concerned with the logistical processes designed to temporarily bypass damaged technical elements.

Risk is inherent in every project. It is defined as “an uncertain event or condition that, if it occurs, has a positive or a negative effect on a project’s objectives” (Project Management Institute, 2000, p.17). Project managers spend significant time speculating on it, and they reserve funds to deal with it. They consider every possible issue that may affect a project, then quantify its cost and estimate the probability of the occurrence of the risk. For each risk, they multiply the cost by the probability of its occurrence. Then the project risk budget is computed as the sum of all the individual risk costs. The project risk is referred to as the “known unknowns,” so called because risks are known in nature but are known only probabilistically in terms of occurrence. Project managers often request additional funds, commonly called the “management reserve,” for risks that are “unknown unknowns,” so called because their nature may not be known, and/or the likelihood of their occurrence may be estimable. Most organizations allocate funds to mitigate against “known unknowns” such as server downtime and power outages. These funds constitute the organization’s contingency funds, which are allocated toward different elements of disaster mitigation such as insurance and currency hedging, as well as other parts of the business continuity or disaster recovery plan.

Unfortunately, there is a great disconnect between risk management theory and practice. Despite widespread recognition of risks and the potential hazards they present, organizations spend very little on business continuity planning, with one survey showing that 54% of enterprises devote less than 1% of their IT budget to BCP (Tanner, 2004). Also, because BCP is a fairly new practice, organizations are having a difficult time assessing their need, performing ROI (return on
investment) analysis, or simply knowing where to start. Surprisingly, the causes of most business interruptions are already known. According to The Disaster Recovery Journal, “the most prevalent sources of business interruption include human error (43%); power outages (39%); followed by natural disasters (8%); and terrorism (1%)” (Montella, 2005). Based on these numbers, one can easily conclude that an organization can achieve a great deal of readiness by addressing the top two sources of interruptions. If human errors can be reduced through proper training, and if power outages can be resolved by the purchase of power generators, one can argue that 82% of the business interruption risk can be easily and cost-effectively eliminated. Training is not a mandate of BCP but rather a part of everyday life in an organization, while purchasing and installing a power generator is a straightforward task. So what is the main barrier? Are organizations being bogged down with the other 18% of the problem? Is it worth investing so much money in trying to prevent terrorism attacks, knowing that they are a mere 1% of the problem? The answer probably lies in the fact that as soon as they start their BCP, organizations find themselves stuck trying to resolve every conceivable disaster scenario. Organizations instead should go after the low-hanging fruit first. They should, for instance, plan processes and institute training to eliminate as many human errors as possible. As an example, they should build processes to ensure that a database administrator cannot mistakenly delete key tables while performing basic administrative tasks. Disaster recovery will then build in replication and backups, so that data can be restored if it is deleted by mistake, and business continuity will prepare the organization to react to such an unanticipated event. The priority for the organization should be to prepare employees for the unexpected. Once employees are able to think and work through unexpected events, they can easily adapt to the 18% of complications associated with natural disasters and terrorism. Most important, the organization needs to proceed with discipline by adopting a clear and proven recipe for its BCP.

The following five-step business continuity planning recipe was published in a joint study by the Universities of Vienna and South Australia (Quirchmayr, 2004). First, formulate a framework for robust project management. This framework should include a business continuity policy for the organization and should make use of standard project management processes. Second, assumptions and conditions for BCP must be identified. These assumptions should clearly identify disaster scenarios that will most likely affect the organization, identify the most critical areas of operations, and include recovery time objectives. By identifying the most critical business units and the recovery timeline, business continuity planners can define the recovery sequence so as to reduce the impact of a disaster. Third, an action plan should be instituted, including business continuity measures, data backup, and technical procedures for restoration. The process should outline how management will procure resources as needed, as well as a decision-making process, a communication plan, and arrangements with stakeholders and suppliers. The action plan might also include preparation of disaster recovery manuals, to be shared with members of the recovery team. Fourth, the plans should be tested and reviewed. Industry standards suggest that disaster simulation should take place once every 6 months, with quarterly tests preferred by some analysts. Deficiencies identified during the testing phase should be highlighted, and the plan should be adjusted to address these deficiencies. Fifth, “other issues” should be addressed, such as office relocation, risk mitigation, and interaction with external parties.

The Role of IT in Business Continuity and Disaster Recovery

There is no doubt that IT has a key role to play in an organization’s planning for business continuity and disaster recovery. The role of the CIO in such situations is to translate the business contingency needs so that the IT department can use its resources to bring business continuity and disaster recovery planning to life. This can be achieved in the following way (CIO.com, 2005): first, by maintaining redundancy in all vital components (i.e., network, server, power grid); second, by ensuring availability of adequate capacity to sustain rapid failover (i.e., migrate functionality to a backup system after failure) and recovery; and third, by testing capacity availability without disrupting current operations. These efforts are made easier by technologies such as high availability solutions (hardware and software) designed for continuous operation in the event of a failure of one or more components; distributed architectures in which applications are placed in various physical locations; load balancing across multiple physical sites using hot backups; data replication using techniques such as data mirroring, shadowing, and clustering; and storage management solutions that allow for easy replacement of damaged storage devises without interrupting operations. These solutions can be expensive, and one of the roles of the CIO is to ensure that money is spent wisely. For example, the IT department can provide two separate systems that back up each other’s functions, each system running a separate live application. In the event of a disaster, the two systems will failover, allowing users of both systems to continue to operate. Solutions such as this one reduce the cost of implementing business continuity and disaster recovery and allow IT to play a central role in preparing for disasters while keeping costs to a minimum.

One must wonder whether the problem is in the cost itself (which
is evidently high and sometimes out of small organizations’ reach) or in the risk assessment process. For various reasons, managers have not convinced themselves that disasters can affect their organizations, rather than simply being other people’s problems. They often limit themselves to the obvious steps of backing up data onto tapes. This rather surprising observation came from a survey of businesses whose primary disaster recovery plan was data backup. When asked if they have prepared a disaster recovery plan, 100% said yes (Tanner, 2004).

When it comes to planning continuity for the supply chain, it has an even more difficult time getting commitments from other parts and members of the organization, which are involved in running their own departments as efficiently as possible. Product managers, for instance, are involved in ensuring that interruptions do not affect the delivery of their products, and IT does not have visibility into this area. Moreover, business continuity for the supply chain is focused on mitigating enterprise risk, which is not the mandate or the expertise of the IT department. Good risk management requires an enterprise-wide perspective, and IT does not have that and can rarely influence it (Smith, 2004). For these reasons, plus the fact that operations (including the health of the supply chain) are the responsibility of the organization’s COO and also because the IT department is limited in its reach and resources; supply chain continuity must become the role of the COO. The IT department should focus on what it does best, and that is to build technical solutions that address the requirements of BCP for all operations, including the supply chain.

Business Continuity Planning for the Supply Chain

This section first discusses business continuity for the supply chain, then reports on cases of supply chain disruptions that could have been avoided with proper information sharing between supply chain partners. It then discusses a framework for supply chain business continuity and extends it with an information technology component.

As defined by the Council of Supply Chain Management Professionals (2005), supply chain management (SCM) “encompasses the planning and management of all activities involved in sourcing and procurement, conversion, and all logistics management activities” as well as the coordination and collaboration with suppliers, intermediaries, service providers, and customers. The council’s definition insists on the fact that SCM is an “integrating function” that links business processes within and across organizations. In addition to the logistics process, integration touches marketing, sales, product design, finance, and IT. SCM therefore is concerned with integrating supply chain participants in a seamless fashion to ensure that goods and information flow smoothly from one participant to another. Any disruption to the flow will lead to significant interruptions downstream that may have a devastating impact on the performance and competitive advantage of supply chain participants (Vinas & Jusko, 2004).

This devastating impact was estimated in a joint study by the Georgia Institute of Technology and the University of Western Ontario. The study concluded that supply chain disruptions can directly affect corporate stock prices by nearly 9%, with losses mounting to 20% months after the disruption (Montella, 2005). The losses can be easily traced, with share prices being dependent on the net present value (NPV) of future cash flows. With an interruption in the supply chain, the company will be unable to produce goods for sale, and without sales, revenues will fall and cash flows will diminish. With inventory levels being always kept to a minimum (i.e., just-in-time [JIT] inventory management), businesses can afford to risk such interruptions only if they make sure “that they and their partner-suppliers develop and deploy strong business continuity plans” (Continuity Central, 2004). One can therefore argue that implementing BCP for the supply chain ensures that shareholder wealth is preserved. It should also be noted that the risk of a supply chain disruption is a function of the probability of its occurrence and the impact it might have, and that a low probability may be overwhelmed by a disastrous impact (Zsidisin et al., 2003).

A company’s effort at implementing BCP for its supply chain can be as successful as all its other efforts at managing the supply chain. Furthermore, implementing BCP does not always mean spending significant amounts of money on new technology. Indeed, companies such as Wal-Mart already have the know-how and financial resources to use RFID (radio frequency identification) technology (among many other technologies) to monitor components of their supply chain. For most companies, however, such technology isn’t necessary, and a simple dialogue and effective communication between supply chain members can go a long way in business continuity preparedness.

Surprisingly, many companies still cannot see the supply chain beyond their immediate suppliers. A 2004 survey revealed that less than 40% of companies reported sharing information with their suppliers on a regular basis, while almost 20% reported no sharing of information (Violino, 2004). What makes this survey more alarming is that companies are also reluctant to share information with their customers. Indeed, 25% of surveyed executives reported that their companies rarely share supply chain information with their customers (Violino, 2004). If information is not seamlessly flowing from supplier to customer, then a company positioned near the end of the supply chain has only a limited view of the issues affecting companies at the beginning of the chain. With such limited visibility, organizations
have less time to react and thus face a greater risk of disruption. The problem can be solved through tight system integration of all supply chain participants, and IT has a significant role to play in that integration. IT has been quite successful in developing business-to-business (B2B) solutions that help organizations implement effective supply management strategies. RFID technology, for instance, allows systems to track the flow of goods and alert management if any interruptions in the supply chain are detected.

A key element of supply chain management design should be resilience. According to a Harvard University Study (Coutu, 2002) adopted by James Rice (2003) resilience is achieved through flexibility and redundancy. Flexibility is realized through such supply chain elements as the ability to shift supply to a second source, flexible contracts for upside (and downside) demand, a multi-skilled taskforce that can adapt easily to new jobs when a disruption occurs, facilities designed for multiple products and rapid changeovers, and contracts for additional transportation. Redundancy is achieved through redundant inventory storage, multiple suppliers, supply contracts that include penalties for non-delivery, multiple production sites, and dedicated transportation. Although some of these items do not apply to all organizations, consideration of the list makes it clear that BCP must be built into the supply chain in a way that makes it resilient to disruptions.

When Continuity Planning Is Done in Isolation

No matter how much effort and resources a company dedicates to its BCP process, its ability to recover after a supply chain disruption is “only as good as its supplier’s ability to recover” (Computer Business Review, 2004). This subsection reports on real-life cases of supply chain disruptions that could have been avoided if the organization’s BCP had been extended to its suppliers. The first case involves a high-tech company based in Ottawa (Ontario, Canada) and concerns the blackout of August 14, 2003. The blackout was due to a massive power outage that occurred throughout parts of the Northeastern and Midwestern United States and Ontario, Canada. The company in question prides itself on its extensive business continuity readiness, and its customers have become dependant on it. The company has built redundancy into all its components: It has multiple data centers and redundant servers, it constantly replicates data; and it owns power generators at each location. The company has engrained business continuity planning into its corporate culture, all staff members are trained every quarter on BCP, and disasters are simulated at least once every 6 months.

When the power went out, the company’s business continuity team sprang into action. All went well and according to plan. Staff knew the processes that they needed to follow, and the company’s customers did not experience any service interruption. Trouble, however, was on the horizon. Before the incident, the company had setup alterations that were triggered when the diesel supply reached a certain level. Having consumed a significant amount of diesel and having reached the midway point in its reserves, the company had 24 hours remaining in power generation capacity. The company followed procedure and called its diesel fuel supplier, asking for a replenishment of supply. To the shock of the recovery team, the supplier informed the company that because the blackout was widespread and because it had no power generation capacity of its own, it was not able to pump diesel fuel out of its tanks. The company struggled to call other local suppliers of diesel fuel. Some were in the same situation as the original supplier, and others that had power generation had made commitments to their existing customers and forecasted that they would be able to supply diesel fuel to the company within 24 hours at best. To guarantee enough generation lead time, the company’s staff had to get diesel fuel from various locations using 20 liter containers. After the disaster state was lifted, the company realized that its failure to extend its BCP to its suppliers was a significant mistake. The company therefore adopted a policy of reviewing the BCP status of its suppliers and has since entered into more than one supply agreement with various vendors where that was applicable. The company has also built closer ties with its suppliers and has entered into preferred customer status with
A far more publicized case occurred in March, 2000. During that time, a Philips semiconductor plant in Albuquerque, New Mexico, that supplied Nokia and its competitor Ericsson with specialized microchips for mobile phones was damaged by fire. The chips were critical components of mobile devices and could not be supplied by other vendors.

Philips contacted Nokia and Ericsson (as well as other major customers) and told them to anticipate a one week delay in shipments (Schmitt, 2007). Both companies had enough safety stock to cover the one week delay so there was no reason for panic. However, Nokia (but not Ericsson) maintained constant communication with Philips throughout their recovery procedure and found out that the Albuquerque plant would take months to recover from the fire incident. Nokia actually had put in place a strong BCP with its suppliers and actively monitored its supply chain. Ericsson, on the other hand, did not enter into this kind of arrangement and was not even aware of the extent of the fire damage (and the fact that it would take months rather than weeks to resume production) for several days. Nokia’s BCP paid off. Shortly after learning of the extent of the fire “Nokia made rapid changes to its designs, substituted other similar components and increased its market share of the rapidly growing mobile phone market. Ericsson reported both short and long range production shortfalls, and posted a $1.7 billion loss in that year’s handset division” (Virtual Corporation, 2007).

Several big companies, such as Sony, Boeing, Hershey, Nike, and Cisco, have been hurt by disruptions in recent years (Singhal, 2005), but there is not enough space in this paper to report on all of them. The lesson to be learned from these and other cases is that business continuity planning can hedge only so much risk if undertaken in isolation. Extending BCP to suppliers and customers improves the response of the organization to disasters and gives it a clear competitive advantage.

Framework for Supply Chain Business Continuity

Zsidisin et al. (2003) propose a framework for supply chain business continuity that, compared to BCP recipes such as the one introduced in Section 2, represents a more focused, yet comprehensive, approach to the problem at hand. A brief description of the framework is given below; for the complete study, the reader should refer to the original publication. The framework identifies the following four stages for supply chain continuity planning:

Creating awareness: The organization must recognize the risk of supply chain disruptions and understand their potential consequences. This awareness must be developed internally and externally (i.e., with clients, suppliers, and other partners) so that everyone participates in managing the risk.

Prevention: To reduce the chances of supply chain disruptions and reduce their impact, the following processes must be implemented: (a) risk identification enumerates the sources of potential supply chain disruptions, (b) risk assessment evaluates the likelihood of each identified risk source and its impact on the organization, (c) risk treatment develops strategies for reducing the likelihood and impact of these risk sources, and (d) risk monitoring continuously watches developments in the supply chain that may increase or decrease these risks.

Remediation: The organization needs a recovery plan for after a disruption occurs. The plan should address ways to shorten the duration of the disruption, minimize its impact and identify the resources needed to carry out the recovery plan.

Knowledge management: When supply chain disruptions occur, the organization must review the important lessons learned (things gone right, things gone wrong, and the results of the remediation effort), with feedback to the earlier stages in the continuity planning process. Based on this review, the existing BCP must be revised, with the aim of addressing its deficiencies.

There is no question that implementing the four stages of the framework will help an organization mitigate the risks of supply chain disruptions. The supply chain is so complex, however, that it cannot be managed without information technology (Betts, 2001), and the most advanced framework for its continuity requires “equally advanced information and knowledge-management tools” (Kearney, 2005). Vinod Singhal (2005), for instance, recommends (among other actions) that executives invest in available technologies that can provide early warning of supply chain problems. Information technology provides more visibility inside and outside the organization and automates supply chain planning and execution (Betts, 2001; Zsidisin et al., 2003). In light of these observations, we extended Zsidisin et al.’s framework to include an IT component (see Figure 1).

Information technology supports the implementation of awareness by integrating the organization internally through the adoption of tools ranging from simple and affordable Intranets to complex and costly Enterprise Resource Planning (ERP) solutions. IT also integrates the organization externally through extranets and SCM software. This enables the sharing of information and knowledge, in a transparent, quick, and cost-effective manner, between the employees of the organization as well as between the various participants in the supply chain. The visibility brought by SCP tools enables risk identification and assessment. SCE tools enable automated risk monitoring. Business intelligence (BI) tools,
such as systems for mining supply chain partners’ reputation information (online and offline), watch for changes in the economic and political environment, monitor changes in supply markets, and examine the status of individual suppliers. Knowledge management systems (KMS) can be a valuable tool for the team in charge of drafting, carrying out, and reviewing the organization’s supply chain BCP. These systems provide easy and rapid access to best practices and lessons learned from previous disruption incidents. Finally, as discussed in Section 3, the IT infrastructure, which is used by the organization to plan and automate the supply chain as well as to provide support for its continuity planning, definitely should have its own BCP.

Conclusion

This paper discussed the role of an organization’s IT infrastructure and its relationship with suppliers in planning business continuity for the supply chain. Supply chain management relies on high-performance networks, hardware, and software. Thus, an IT-related failure can seriously disrupt the supply chain and affect many of its participants. All suppliers, service providers, and customers are links in the supply chain, and efficient SCM supposes that all these links respond in harmony to any disruption. The paper reported on cases of supply chain disruptions that could have been avoided if business continuity planning had been extended to all supply chain participants.

We believe that the organization’s IT department has an enormous responsibility in bridging the gap between what is perceived as its own responsibility and what is perceived as management’s responsibility toward BCP. In addition to translating business needs into practical and technical implementations, the IT department must make management aware of the limited role that information technology can play, and IT must engage management in a discussion on implementing proper BCP. The COO (and through him or her, all members) of the organization should be “in charge” of the supply chain’s BCP. The CIO, however (and through him or her, the IT department) should be “involved” in ensuring continuity for the supply chain, as well as “in charge” of ensuring continuity for the IT infrastructure that runs all business processes, including the supply chain. To support this argument, we extended Zsidisin et al.’s supply chain business continuity framework to include an IT component.

There is no doubt that BCP for the supply chain can be expensive and can require significant integration from a logistical and technical point of view. It is also difficult to achieve, as supply chain participants must be willing to cooperate openly, regardless of how protective they are about their information. As long as one participant can champion the cause of bringing BCP to the supply chain, however, the task in not impossible.

References


Smith, M. (2004, August 1). Why CIOs should take this job and shove it [Electronic version]. Retrieved November 25, 2007 from http://www.itworldcanada.com/a/CIO/3f3 e9 c3 4 - 6 9 0 f - 4 b 7 5 - b e f 0 - 8 9 6 e 5 ed 8 e 9 . html


About the Authors

Morad Benyoucef is Associate Professor of MIS at the University of Ottawa. His research interests include online marketplaces, IT support for trade mechanisms, online trust, modeling processes within service oriented environments, and Supply Chain Management. He has published papers in international journals including E-Commerce Research, Group Decision and Negotiation, and Services and Operations Management. His research is funded by the Canadian Foundation for Innovation and the National Sciences and Engineering Council of Canada. He holds a PhD in Computer Science from Université de Montréal.

Samer Forzley is Vice President Marketing at eBillme. He develops and manages marketing strategies and programs dedicated to customer and merchant acquisition. Prior to joining eBillme, Samer held senior eBusiness development and strategy positions with Alcatel, Primus, and Allstream. Samer holds a Bachelor of Arts in Economics and a Bachelor of Math in Computer Mathematics from Carleton University, he also holds a Master’s of Business Administration Degree from the University of Ottawa.