

EXPERTISE IN BUSINESS  
MANAGEMENT + CONSULTING



Klay Management Ltd.

# Mitigating Operational Risk – Not Just for the Field Anymore

*How Business Continuity Planning  
Reduces Corporate Operational Risk*

A White Paper



## CONTENTS

<b>1. Introduction</b>	<b>3</b>
<b>2. Mitigating Corporate Operational Risk</b>	<b>3</b>
<b>2.1. Building Corporate Competency</b>	<b>4</b>
<b>3. Corporate Operations</b>	<b>4</b>
<b>4. Corporate Operational Risk</b>	<b>5</b>
<b>4.1. Corporate Governance</b>	<b>5</b>
<b>4.2. Human Knowledge Assets</b>	<b>6</b>
4.2.1. Effects of a Disaster from an HR Perspective	7
4.2.2. Mitigating Risks to Personnel	8
<b>4.3. Data Assets</b>	<b>9</b>
<b>4.4. Key Vendor Outage</b>	<b>11</b>
<b>5. Summary</b>	<b>12</b>
<b>6. Appendix</b>	<b>14</b>
<b>Bibliography</b>	<b>15</b>

## 1. Introduction

*What we anticipate seldom occurs: but what we least expect generally happens. (Benjamin Disraeli)*

Within the energy industry, risk awareness in field operations is a way of life. Every company has safety plans, crisis management plans, emergency response plans, and accompanying training and testing procedures. These plans and programs ensure that employees are constantly aware of the dangers around them -- dangers associated with the mechanics of what they do, the products they produce, and the regions in which they work.

In some respects, this high level of competency in the areas of safety and risk management has led to a certain complacency when it comes to the risks associated with *corporate* operations. After all, if anyone understands risk and how to manage it, an energy firm does. Surely if a business continuity plan was required, they would be the first to realize it.

This paper seeks to create a better understanding of the unique risks a corporate headquarters faces, and how – just as with traditional crisis management – advance planning can help mitigate those risks and ensure the continuity of a company’s most critical corporate functions.

## 2. Mitigating Corporate Operational Risk

*Court disaster long enough, and it will accept your proposal. (Mason Cooley)*

Recent high-profile incidents have served to raise the awareness of Business Continuity Planning (BCP)<sup>1</sup> among corporate executives, board members, shareholders, industry regulators, and governments. These same incidents have also raised the awareness of what could happen, from a “that would never happen” attitude to a “when it happens” attitude, at least at RBC Royal Bank and RBC Insurance. In a recent interview with Klay Management, Jeff Collins, Director of Investments for RBC Insurance<sup>2</sup>, noted that “pitching business continuity used to be a real struggle” for him. People tended to believe the probabilities were too low to worry about. Over the past four years

---

<sup>1</sup> A Business Continuity Plan (BCP) refers to the process of developing advance arrangements and procedures that enable an organization to continue its critical processes after a disruptive event. A Business Continuity Program is an ongoing program supported by the executive to ensure business requirements are assessed, resources are allocated, and strategies and plans are tested and maintained.



they have been hit by Y2K concerns, 9/11, SARS, and other threats. Now, the executives he works with believe that the next major event is right around the corner. Attitudes towards the importance of business continuity “have done a complete 180.” Collins went on to say,

In the insurance industry, the probability of events occurring are measured as once every 10 years, every 20 years, every 100 years, and so on. Recent experience has shown that these risks (*of incidents causing business disruption*) happen far more frequently than that. As a result, we have dramatically increased the probabilities of events happening.

## 2.1. **Building Corporate Competency**

To better understand how to mitigate operational risk in a corporate headquarters, a company must understand what is at risk, how it is at risk, and what to do about it. Fundamentally, business continuity planning develops corporate competency in the following areas:

- **Understanding what processes are most critical to the corporation, and why.** This includes knowing how the loss of each process might affect other processes, what the cost to the corporation would be if that process could not be completed, and what is needed to complete the most critical processes (i.e. what people, systems, data and facilities are required). This part of the Business Continuity Program is called a Business Impact Analysis (BIA).
- **Protecting the corporation’s most critical business assets, including human knowledge assets and data.** This includes recognizing threats and risks to these assets and implementing mitigation measures to protect them.
- **Ensuring the identified critical processes and assets are recoverable at the time of a business disruption.** This includes not just planning and training for recovery, but testing to ensure it can be done.

## 3. **Corporate Operations**

*If you can't describe what you are doing as a process, then you don't know what you are doing. (W. Edwards Deming)*

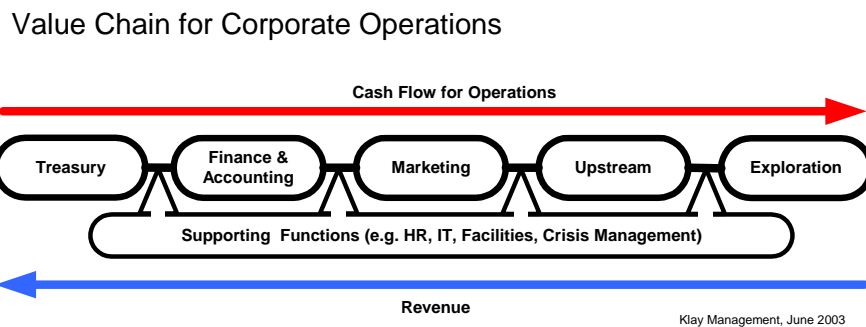
---

<sup>2</sup> Jeff Collins is Director of Investments for RBC Insurance and former Vice-President of Canadian operations for ABN Bank. He sits on contingency committees at the local, national, corporate, and U.S. operations level, and is also a member of RBC’s Business Continuity Emergency Task Force.

---

In most large corporations, business units rely on a steady cash flow from corporate headquarters to ensure the continuity of their operations, and the corporation relies on a steady revenue stream to ensure profits. The purpose of a corporate headquarters, therefore, is to ensure that this circular flow of cash is managed as efficiently as possible, and to provide required services, expertise, and leadership to the business units. In the context of this discussion, the management of cash – both revenue streams and cash flow for operations – includes being able to account for what happens to that money, and how it is invested.

Acknowledging the importance of corporate processes in not only facilitating the creation of revenue by the businesses, but in creating its own revenue through prudent financial management, is required in order to recognize the unique risks that head office operations face.



## 4. Corporate Operational Risk

*There cannot be a crisis next week. My schedule is already full.  
(U.S. Secretary of State Henry Kissinger, June 1969)*

Threats to business continuity come in many forms: natural disasters, human-caused events, and technological accidents. Regardless of cause, the *effect* of a major business disruption to a corporate headquarters can take many forms. The following describes just some of the areas – both functional and asset-based – that can be effected by a disaster and impact the Corporation’s financial position.

### 4.1. Corporate Governance

There is no shortage of examples of corporate governance gone wrong and how it can effect a company – Enron, Arthur Andersen, and WorldCom are some of the more noteworthy ones. Some might wonder how a business continuity program can help in a situation where corrupt practices cause a company to falter or fail. In large corporations particularly, keeping track of how different

units are conducting their business has always been a challenge to corporate governance. By understanding the processes that the businesses use and the control mechanisms in place, the Corporation can ensure compliance with its values and vision. And, through regular testing of the plan, opportunities for questionable practices can be uncovered and highlighted, resulting in constructive changes to processes and procedures.

A Corporation's Business Continuity Program provides opportunities for operational synergies to be harnessed with other programs and projects that rely on the same information. The documentation requirements of the Sarbanes-Oxley Act – which was enacted to help ensure good corporate governance – are quite similar to the requirements needed to maintain a Business Continuity Program (particularly the Business Impact Analysis, or BIA). Any function that is deemed material to the financial statements through the Sarbanes-Oxley initiative is also considered critical from a BCP perspective. Having said that, there are other functions, such as those required to actually recover the business after a major disruption (IT, HR, Facilities, and Crisis Management services), that are considered critical from a BCP perspective that Sarbanes-Oxley may not consider material.

#### **4.2. Human Knowledge Assets**

Every company acknowledges the importance of its people, but few have plans in place to retain that knowledge or to acquire it through alternate means should a disaster occur. Loss of human assets can be the *cause* of a disaster (a threat), the *result* of a disaster (an effect), or both. For instance, the sudden loss of key personnel, or the loss of significant numbers in a short period, can actually *cause* a disruption in critical business processes. The upcoming exodus of baby-boomers from the workforce is a prime example: “By 2010, “as many as 60% of today’s experienced management personnel will retire from the (oil and gas) industry even if various ‘golden handcuff’ incentives are initiated to retain perhaps 20% of them.”<sup>3</sup> Faced with such a situation, advance-planning is required to capture as much of the individualized knowledge that experienced personnel have, in order to reduce the negative impact to the corporation.

On the other hand, losing key personnel due to loss of life may be the result of a disaster. But, without advanced planning on how this will be handled, the situation can actually degrade into yet

---

<sup>3</sup> Beazley, Boenisch and Harden, p. 5

another disaster – the unexpected loss of large numbers of staff over a relatively short period of time.

#### 4.2.1. Effects of a Disaster from an HR Perspective

Of the hundreds, if not thousands, of articles that have been written about the effects of September 11<sup>th</sup>, certain key elements are consistent throughout. Understandably, the most important lesson is the value of people to an organization, and the inherent frailty of that asset. Although most of the companies impacted by September 11<sup>th</sup> had some kind of disaster recovery plan in place (they had already learned the importance of business continuity planning after the first World Trade Centre bombing in 1993), they had significantly underestimated the effect of a disaster on their workforce. As long-term impacts of the disaster were analyzed, it was found that those companies who struggled the most did so because of overwhelming staff losses.<sup>4</sup> Aside from the losses caused by the event itself, some people never did return to work due to the trauma they were facing, others continued to leave long after the event. Jeffrey W. Greenberg, CEO of Marsh & McLennan Companies remarked in a Harvard Business Review article, “I agreed to an interview with the Wall Street Journal and said that we had lost 313 people. As it turned out, I was wrong. A number of our employees had been so shocked by their ordeal that they’d left the city or hadn’t answered their phones.”<sup>5</sup> The longer it takes to restore normalcy for people, the more stress they are placed under. Some people simply give up and go home.

One company that was very successful in addressing this issue was Morgan Stanley. In the aftermath of the tragedy, Morgan Stanley was missing seven employees and six on-site contract workers. Thirty-five hundred employees were displaced, and yet Morgan Stanley was back in business when the opening bells sounded once again in the stock markets the following Monday. Contingency plans for their people included the ability to work from home, the provision of grief counselors, aggressive planning to get people back to work earlier, enhanced communications with employees, senior management and the media (including an initiative called “rumour control”), and strategies to deal with temporary housing, transportation and communication.<sup>6</sup> All of Morgan Stanley’s contingency plans – data and application recovery, HR plans, and work area recovery –

---

<sup>4</sup> Ferris, Gregory J. [www.rmmag.com/](http://www.rmmag.com/)

<sup>5</sup> Greenberg, Jeffrey W.

<sup>6</sup> Ferris, Gregory J. [www.rmmag.com/](http://www.rmmag.com/)

were tested on a regular basis, so that when the crisis hit their people knew what to do, despite the trauma and chaos around them.

Another common theme in stories of September 11<sup>th</sup> is the importance of planning for communication needs. Communication choke points occurred due to congestion on public networks, requiring alternate methods of communicating.<sup>7</sup> Equally important to *how* you plan to communicate, is *what* you plan to communicate, and *who* is responsible for doing so. Confusion among employees as to what was going on and what was expected of them only added to an already stressful situation.

The one thing that all of the stories emanating from September 11<sup>th</sup> have in common is that traditional Disaster Recovery Planning<sup>8</sup> (DRP) is simply inadequate. It underestimates the dynamics of people in a crisis situation. Unlike computer hardware, people become traumatized in a disaster and it is unrealistic to expect them to operate normally in a changed situation or alternate work site.<sup>9</sup> An understanding of these potential dynamics is required to ensure planning is realistic.

#### 4.2.2. Mitigating Risks to Personnel

The SARS outbreak in Toronto provided companies with lessons in mitigating risks to personnel and in the importance of understanding what is most critical to a corporation. RBC's Jeff Collins noted that all five of the big banks in Toronto instituted a portion of their business continuity plans in response to SARS by creating 'clean teams' to ensure that 'one-hour critical' bank activities continued (in this case, the trading floor). A skeleton staff was moved to the disaster recovery site where they worked in isolation from other employees for the full two weeks of each outbreak. Team members were not allowed to socialize with other people, and were forbidden from physically interacting with other employees.

Both the disaster recovery site and the primary site were still in operation and had to be fully synchronized in order for the plan to work (unlike most situations where the primary site is deactivated due to the disaster, and only the recovery site is in operation). Staff also had to become comfortable with using web-based software to conduct business meetings. With the synchronization and communication issues dealt with, they now know that having staff in separate

---

<sup>7</sup> Bell, Judy

<sup>8</sup> Disaster Recovery Planning generally refers to technology plans only.

<sup>9</sup> Cruickshank, Doug, pp. 20,21

locations does not affect productivity. Utilizing this approach as a permanent risk mitigation strategy has now become an option for the company.

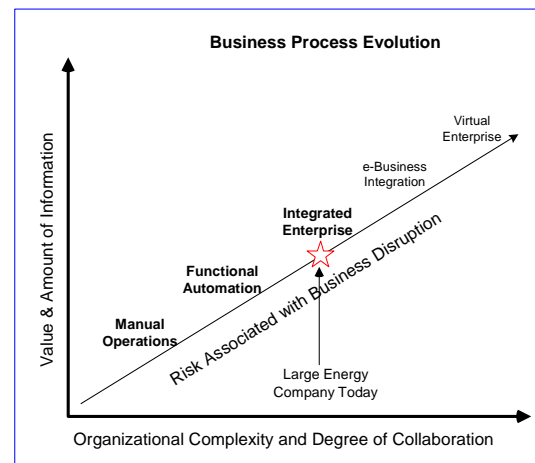
To understand a bit more about how other Canadian corporations are responding to threats to human assets, we can take a look at the results of surveys conducted by Mercer Human Resource Consulting in response to the SARS epidemic. The Mercer report noted that,

While many organizations have disaster recovery plans, they tend to deal with issues relating to the loss of or damage to the physical work site. We are now faced with a situation that leaves the work site intact, but may limit the availability of employees to attend.<sup>10</sup>

When the first survey was completed at the end of April 2003, 11% of Canadian respondents stated they had policies in place to deal with health-related emergencies. By May 2<sup>nd</sup>, that percentage had jumped to 25%. Most companies cancelled social events (88%), while many implemented more rigorous measures, including voluntary quarantine, restricted travel, contingency plans, and working from home (from 46% to 38%). Clearly, the importance of taking planning beyond the simple DRP and developing a more balanced approach to business continuity is taking hold in corporate Canada – with SARS being the wake-up call.

### 4.3. Data Assets

An ever-increasing degree of collaboration and integration is required to ensure the consolidation of information and the rationalization of processes in a large corporation. Similarly, the value of corporate data is rising as we rely more heavily on the information generated. It makes sense then, that as organizational complexity and the value of corporate information continues to increase, so too does the risk associated with a business disruption. Both data and the complex systems that allow it to be utilized must be protected.



Several significant technology trends are making it increasingly urgent to protect data assets and manage them appropriately. The exponential growth in data volumes is the most alarming.

<sup>10</sup> <http://mercerhr.com/knowledgecenter/reportsummary.jhtml/dynamic/idContent/1090705>

“According to a University of California, Berkeley study, more information will be created over just the next two years than all that has been created throughout history up to now. The study also predicts that 93 percent of that information will be digitally stored.”<sup>11</sup>

Four basic things must be accomplished to protect a company’s data assets:

1. Consolidate and rationalize how data assets are managed (including hard data),
2. Duplicate data to ensure there is always at least one additional copy somewhere,
3. Keep duplicate data assets far enough away from the originals so as to protect them from regional disaster,
4. Ensure that recovery can actually be accomplished through advanced planning, regular testing, and preferably, automation of recovery efforts.<sup>12</sup>

Charles King, Senior Industry Analyst with The Sageza Group Inc. provided his insights into the last point in a recent white paper, based upon his experiences in helping companies restore after September 11th:

Dedicated and talented customers and vendors worked under extreme conditions. They had little or no time to sleep, and in some cases no reasonable way to get home and back. After working thirty-six or more hours, under the weight of everything that happened, the judgement and abilities of even the best people suffered... The lesson is to automate the replication and recovery processes. When employees are stressed and optimal (*primary*) decision-makers are not available, the chances of human error and elongation of the recovery process grow exponentially. Clients should demand that their vendors provide solutions that automate these critical processes.<sup>13</sup>

The important thing to remember here is that, protecting data by itself is simply not enough. It is the *process* that provides value to the corporation – the interaction between data and people, and the systems to support that interaction. Any one of these by itself is inadequate to ensuring that the process can be performed and the flow along the value-chain continues uninterrupted.

Even if a corporation has planned appropriately for all of the process needs mentioned above, they still require a place for all of this to happen. On September 11, many plans did not anticipate a regional disaster. Trying to find an alternative facility at the time of disaster was an almost impossible task, not to mention an expensive one.

---

<sup>11</sup> EMC<sup>2</sup>, p.5

<sup>12</sup> EMC<sup>2</sup>, p.7

<sup>13</sup> King, Charles, p. 1

Office space, more than telecom or hardware, was the biggest problem for many of the companies displaced from the WTC. “We lost 480,000 square feet of space in the World Trade Center,” says David Snow, COO at Empire Blue Cross Blue Shield (\$2.2 B in assets, New York). “The real bottleneck was not telecommunications or IT, it was finding space for everyone. It wasn’t until the end of November that we got everyone into an office.”<sup>14</sup>

Jim Simmons, CEO of SunGard Availability Services, summed up his experiences in a recent speech:

When the twin towers of the World Trade Center went down, many workers from those towers had nowhere to go. Many had no emergency gathering place. They had no system for regrouping, most of them escaped into a void – no office, no desk, no phones, no information. They had been separated from the things that made it possible for them to pick up the processes they’d been involved in at work, and the next morning they were supposed to report for work at a recovery facility in a different state.

The information was there, but the company first had to communicate with its people and then had to get the people to the recovery (*site*).<sup>15</sup>

#### **4.4. Key Vendor Outage**

Companies have increasingly come to rely on committed relationships with vendors in order to assure the availability and quality of the products they need. Building committed vendor relationships has not only been a boon to productivity, it has also been used to reduce corporate risk by downloading riskier operations to other companies (e.g. outsourcing of marketing services). In some ways, however, the reliance on one key vendor to provide critical products or services can actually *create* risk.

In March 2000, a lightning bolt caused a blaze at a Phillips Electronics factory in Albuquerque, NM. Ten minutes after the strike the fire was out of control, and far away in Scandinavia this small event sparked a corporate crisis that shifted the balance of power between two of Europe’s largest electronics companies.<sup>16</sup>

The companies were Ericsson and Nokia; the product, computer chips required for the mobile phone market. Both companies relied on a steady supply of computer chips from this one factory to continue production. Nokia noticed “a glitch in its supply of computer chips” and immediately launched its business continuity plan. By the time Ericsson noticed what was happening, Nokia had

---

<sup>14</sup> MacSweeney, Greg

<sup>15</sup> Simmons, Jim, p. 16

<sup>16</sup> [www.contingencyplanning.com/article\\_index.cfm?article=523](http://www.contingencyplanning.com/article_index.cfm?article=523)

initiated contracts with most of the alternate suppliers. The result was a \$600M revenue loss for Ericsson, along with a 50% reduction in market share.<sup>4</sup>

The answer to mitigating this risk is twofold: 1) ensure key vendors have their own business continuity plans in place and that they are regularly tested and updated; 2) ensure the corporation's own plan contains an alternate strategy in case a key vendor is lost.

## 5. Summary

*To achieve great things, two things are needed; a plan, and not quite enough time (Leonard Bernstein)*

The business of an energy firm's corporate head office has more to do with financial management and service provision than the actual production of energy products, yet the risks to the corporation should corporate functions be jeopardized are very real. Debt financing arrangements, regulatory filings, billing processes – all these functions create significant risk to the Corporation if they cannot be accessed or completed within certain timeframes.

Companies around the world are realizing the importance of having a plan in place to mitigate these risks in case of disaster. They also understand that this plan must take a balanced approach to the needs of the corporation, encompassing not just IT, but human resource and facilities requirements as well. This realization has come, in large part, from the lessons learned by others – those who planned for and tested their business continuity capability, and those who did not.

Companies are also coming to realize that their plans must be driven by business needs, not IT requirements - acknowledging what is most critical to keeping the corporation alive and healthy, regardless of what occurs. But most companies are still struggling with the justification of preparing and maintaining a Business Continuity Program when there are so many other issues to be dealt with. In a business environment where change is occurring almost daily, and where expectations of shareholders and customers are constantly increasing, who has the time to devote to planning for something that may never occur?

The problem is, major business disruptions *do* occur. And far more frequently than we would like to imagine, as Jeff Collins of RBC Insurance noted. Furthermore, the expectations of shareholders, customers and the public at large are changing when it comes to delivery of service and profits. We are an instant society that expects instant results, and there is little sympathy for companies who are caught off guard. If a disaster such as 9/11 were to strike a company there would likely be

---



some sympathy and a relaxation of expectations, but the vast majority of major business disruptions are not of this cataclysmic nature. In fact, most computer downtime lasting more than 12 hours is due to power outages and surges<sup>17</sup>. Something as mundane and common as this would certainly not cripple a large corporation, but the cost in terms of money and reputation could be significant if it happened at year-end.

Does an energy company need a gold-plated Business Continuity Plan with multiple hot-sites that will guarantee continuation of business regardless of what happens? Probably not. But, it does need to understand what business functions are critical to its corporate well-being, how long it can function without them, where the risks to its corporate assets are and how to mitigate those risks, and how it can resume critical operations if a crisis were to occur. It also needs to have built competency in these areas through regular testing, to ensure that employees have the explicit knowledge required to recover highly complex systems and processes. Building corporate competency in these areas not only helps protect the corporation from unforeseen events, it helps to reduce the likelihood of certain events occurring, through prudent business practices.

---

<sup>17</sup> <http://www.contingencyplanningresearch.com/costofdowntime.htm>



## 6. Appendix

### Statistics of Interest

- “Two out of five companies facing a disaster go out of business within five years.” (Gartner Group of Stanford, Connecticut)
- “A study of leading Canadian businesses by Ernst & Young LLP found that 36% of respondents say the time required to restore critical systems and web-based business processes after an event is longer than their business can function without them.” (Cruickshank, Doug, CP Magazine).
- “Human error accounts for 32 per cent of data loss.” (O’Brien, Jennifer, Computing World Magazine).
- “In a new survey, 57 percent of US-based chief financial officers (CFOs) said that their companies currently have a business continuity plan in place to recover from a disaster. But more than one-third (36 percent) of respondents said their firms are not prepared for a catastrophic event or other major disruption.
- “According to the U.S. Bureau of Labor, 93 percent of companies that suffer a significant data loss are out of business within five years.” (Information Management Journal, May/June 2003).
- “Downtime costs vary from industry to industry, based on dependency upon technology and typical labor costs. Companies that are the most dependent upon automated systems, such as energy and telecommunications enterprises, accrue an average of nearly \$3 million in losses for every hour of downtime, based on lost revenue and employee idling, according to an October 2000 Meta Group study. IT-dependent manufacturing companies and financial institutions suffer per-hour revenue losses of \$1.5 million to \$1.6 million. Health care, media and hospitality/travel companies, less dependent upon IT infrastructure, lose between \$330,000 and \$636,000 of revenue per hour.” (Toigo, John William, Network Computing)

**THE COST OF DOWNTIME**

INDUSTRY SECTOR	REVENUE/HOUR	REVENUE/EMPLOYEE-HOUR
Energy	\$2,817,846	\$569.20
Telecommunications	2,066,245	186.98
Manufacturing	1,610,654	134.24
Financial institutions	1,495,134	1,079.89
Information technology	1,344,461	184.03
Insurance	1,202,444	370.92
Retail	1,107,274	244.37
Pharmaceuticals	1,082,252	167.53
Banking	996,802	130.52
Food/beverage processing	804,192	153.10
Consumer products	785,719	127.98
Chemicals	704,101	194.53
Transportation	668,586	107.78
Utilities	643,250	380.94
Health care	636,030	142.58
Metals/natural resources	580,588	153.11
Professional services	532,510	99.59
Electronics	477,366	74.48
Construction and engineering	389,601	216.18
Media	340,432	119.74
Hospitality and travel	330,654	38.62
Average	\$1,010,536	\$205.55

Source: META Group, Inc., "Quantifying Performance Loss: IT Performance Engineering and Measurement Strategies", November 22, 2000

## Bibliography

- Author Unknown, *A pattern of business response to SARS emerges*, Mercer Human Resource Consulting LLC., April 27, 2003, <http://mercerhr.com/knowledgecenter>, (June 27, 2003).
- Author Unknown, *Becoming an Unbreakable Organization, Maintaining Focus on Business Continuity (white paper)*, EMC<sup>2</sup>, September 2002.
- Author Unknown, Goal QPC website, <http://www.goalqpc.com>, (June 27, 2003).
- Author Unknown, *Learning the lessons from SARS*, Business Continuity Institute website, U.K., <http://www.thebci.org>, (July 3, 2003).
- Author Unknown, *Majority of medium and large US companies now have business continuity plans*, The Business Continuity Institute website, [www.thebci.org](http://www.thebci.org), (June 27, 2003).
- Author Unknown, *Ten Tough Questions You Should be Asking About Your Information Availability*, Sungard Planning Solutions, Pennsylvania (2002).
- Beazley, Hamilton, Boenisch, Jeremiah, Harden, David, *Continuity Management, Preserving Corporate Knowledge and Productivity When Employees Leave*, John Wiley & Sons, Inc., Hoboken, N.J., 2002.
- Bell, Judy, *Updating Your Business Continuity Plan for a Post 9-11 World*, Disaster-Resource.com, [www.disaster-resource.com/articles/03p\\_042.shtml](http://www.disaster-resource.com/articles/03p_042.shtml) (July 3, 2003).
- Cruikshank, Doug, *The road to recovery: September 11 stripped us of our innocence, forcing corporations to recognize that disaster planning is a business necessity*, CA Magazine, v. 135(7) S'02 pp 20-23.
- Ferris, Gregory J., *Response and Recovery at Morgan Stanley*, Risk Management Magazine, New York, v. 49(12), Dec. 2002, <http://www.rmmag.com/> (July 4, 2003).
- Greenberg, Jeffrey W., *September 11 – A CEO's Story*, Harvard Business Review, October 2002, pp 58-64.
- Hiles, Andrew and Barnes, Peter, *The Definitive Handbook of Business Continuity Management*, John Wiley & Sons, Ltd., Chichester U.K., 2001.
- King, Charles, *After September 11: Lessons on Planning and Implementing Business Continuity, A White Paper*, The Sageza Group, Inc., Mountain View, CA, March 2002.
- Laye, John, *Avoiding Disaster, How to Keep Your Business Going When Catastrophe Strikes*, John Wiley & Sons, Inc., Hoboken, New Jersey, 2002.
- MacSweeney, Greg, *Disaster recovery planning: Sadder but wiser*, Insurance & Technology Magazine, v. 27(4), March 2002, pp 20-27.
- O'Brien, Jennifer, *Life-saving business strategies get low priority*, Computing Canada, v.25(12) Mr 26'99 pp 11,13.
- Power, Peter G., *Manage a Crisis, Don't Recover from Disaster*, Contingency Planning Magazine website, January 2003, pp22-26, [www.contingencyplanning.com](http://www.contingencyplanning.com), (June 27, 2003).



Ream, Scott, *How Mature is your Business Continuity Program?*, Contingency Planning Magazine, January 2002, pp 26-30.

Simmons, Jim, *Information Availability: The Next Frontier*, speech given at the Disaster Recovery Journal Conference, Orlando, Florida, September 10, 2002, SunGard Availability Services, <http://recovery.sungard.com>, (July 3, 2003).

Toigo, John William, *Storage Disaster, Will you Recover?*, Network Computing website, March 5, 2001, <http://www.networkcomputing.com/1205/1205f1.html>, (July 7, 2003).