

Is your Corporate Risk Program the Corporation's Biggest Risk?

By *Peter B. Giblett*

For further information please go to www.giblett.info



*Corporate Risk – Statutory Compliance –
Improving Business Performance*

Is your Corporate Risk Program the Corporation's Biggest Risk?

Corporate Risk is the chance of something happening, in terms of probability and impact, that will affect achievement of business objectives. It has been identified many times in the past 10 years as one of the key challenges to business continuity. Yet many organizations still consider this somebody else's problem.

Risk taking is often seen as essential to business growth – it is true that many corporations would not be here today but-for the risks taken in the past. There is however a difference between the risks taken in order to grow a business and the risk of failure due to loss of key assets. We all know failure to innovate will cost companies more than just revenue. It has the potential of destroying market share and consumer confidence. One is a matter of expediency the other a matter of delinquency.

A properly designed risk management program should be designed to provide corporate 'peace of mind'. It should provide a structured and disciplined approach to assessing and managing the uncertainties and opportunities faced. It is necessary to formulate a clear and precise plan that will address the protection of specific assets and enable business continuity in the event of the unthinkable occurring. Corporate risk management is underpinned by the creation of a sound asset protection program.

Is your corporation up-to the challenge?

Some of the categories that need to be considered include:

- Loss of premises
 - Disaster Recovery
 - Business Continuity
 - Fail-over sites
- Loss of Employees
- Financial Risk
 - Corporate Reporting
 - Unionization
- Legal Exposure
 - SOX, and other similar regulatory requirements have made their mark on the corporate landscape in how we complete our corporate financial reporting.
 - The Legal impact for IT has been increasing exponentially since Y2K.
- Human Rights
 - Privacy
 - Discrimination
- HR Exposure
 - Disabilities
 - Sexual Harassment
- Mergers and Acquisitions
- Demergers & Divestitures
- Joint Ventures
- Corporate Policy
 - Theft
 - Fraud
 - Identity Theft

Loss of Premises

Loss of premises is perhaps the most dramatic way in which a corporation can be affected in the event of a disaster. Consider this. In the UK recently there was a fire at a petroleum depot that was located on the edge of an industrial complex.



We all know how disasters strike – it is always somebody else’s problem, well not on this occasion. The fire took place on Sunday morning at 7am close to where I lived at the time. Fortunately no-one was working in the vicinity, at the time the fire started, but it caused wide-spread devastation, including closing the UK’s major motorway. (Picture courtesy of the BBC).

The building next to the depot was the headquarters for a major electrical retailer, which was at least 700 or 800 yards away from the depot, that employed over 500 people. All of the windows were blown out of this building and power was cut as the neighboring depot went up in smoke.

Here are pictures of some of the businesses premises impacted by the explosion that I took a month or so later.



None of these buildings caught fire, but all were closed for a minimum of 6 months, some eventually had to be bulldozed and rebuilt. Many smaller business of-course failed to re-open from the disaster.



Our electronics chain had a full disaster recovery plan ready – they simply opened at their disaster recovery site – All key workers reported to the new site on Monday morning and all other workers were at new desks within a month. Neither the Customer Services Helpline, nor the IT facility was located at the HQ building. The systems were located at another site in the town, and there was no

necessity to activate the failover site. By normal opening time, 10am, all stores in the nationwide chain opened on time and suffered no defect as a result of this disaster.

On-going disaster planning - Many companies have a need for an in-house disaster plan but cannot justify the additional technical staffing and overhead costs. It is essential to engage the right facilities that will ensure a rapid response at a minimal cost.



Simple measures can often be taken to limit the scope of a disaster – e.g. locating the control station for a major North American electrical grid supplier under the flight path to a major airport is a disaster waiting to happen – especially if the company has adequate land available to build this facility elsewhere.

I have not here even considered terrorist attack – where many high-profile international businesses need to take additional precautions.

Loss of People

Loss of premises is perhaps the most dramatic way in which a corporation can be affected in the event of a disaster, yet it is the people that are perhaps the heart of the corporation. I recently took a short flight with most of the major officers of one company attending a strategic meeting. Thankfully nothing untoward happened – but the fact remains that no more than two key personnel should have been on that flight.

Critical Personnel include:

- Key employees
- Corporate executives (the CEO, CFO, CMO, etc.)
- External Stakeholders

Necessary to identify all employees who are key to business continuity and create policies to ensure continuity. Do not make the mistake of assuming that all key employees are senior in nature even the most junior of personnel can hold critical roles – for example the junior IT operator who monitors all of the overnight jobs, lack of adequate coverage could at the very worst mean loss of revenue.

Many organizations are starting to limit their risk in each area by succession planning. The key in succession management is to create a match between the future needs and the

aspirations of individual employees. One intent is increase the retention of employees because they recognize that time, attention and development that is being invested in them for the purpose of career and corporate development. All this assumes there is a meeting of the minds, without which plans mean very little.

Fraud & Theft

We have heard it said before that corporate theft is a victimless crime. According to one firm of Corporate Investigators "Internal theft and fraud is estimated to cost Canadian business in excess of \$4.3 Billion annually. It is estimated 80% of small business bankruptcies result from the misappropriation of corporate assets."

As a result today the corporate executive faces a very real challenge to protect corporate assets. Identity theft also has a place in the corporate realm, but here we are not talking about stealing the corporate credit rating, but the company assets – at the head of the list being the client list.

Protecting the client list is no less of a concern today than it was 100 years ago. However using the CRM system the tech-savvy salesperson is more easily equipped to walk out the door with a copy of the client list than ever before – and furthermore the victim does not even know it has happened until they start losing customers – the worst case scenario could be business closure and job losses. Now tell me there are no victims!

Mergers, Acquisitions, Demergers and Divestitures, Joint Ventures

It not the intent here to comment on the risks inherent with pre-merger negotiations of any deal. I assume pre-acquisition due diligence has been carried out. For most organizations it is the post-acquisition surprises that can have the greatest impact start as soon as the deal is finalized.

The impact can be across all areas in particular: integration issues; personnel issues; obsolete equipment requiring replacement; plant & office closures; warranty exposures; major contracts. Satisfying the enhanced customer base is a risk of its own.

From a business perspective in an M & A situation the organization will have new staff, new cultures, new reporting methods, duplicate systems that all have to be brought into a single coherent unit. The quicker the new business structure is identified the less the potential fallout.

It is rare that a merger ends in no job-losses and everyone knows this – so it is important to identify the new corporate structure as part of the deal. Previously happy staff suddenly find the smallest excuse to leave.

The IT impact may in itself be a reason to put up the STOP! sign before the merger is negotiated. We have all seen it – Corporation A uses System X while Corporation B uses System Y – incompatibilities can become a major concern. Additionally failure to deal effectively with the volume of data, the complexity of systems integration can have disastrous consequences for the companies and executives involved. There are some rare examples where the total IT costs related to the merger outweighed the benefits sought.

Demergers or divestitures also lead to cross system issues. Who owns what piece of data and who can access it, particularly for the business intelligence system.

Your corporate risk plan will need to be revised or even completely re-written as a result of the changing business structure.

Insurance

If you speak with an insurance broker or provider then they will assure you they are capable of providing 'a solution', yet is this really another solution? Insurance is only really capable of minimizing the fallout after the fact. It is good to know that the buildings or the people are insured but this alone does not keep the business running.

To paint a picture an event results in a branch office being destroyed with the loss of 50 lives. Insurance will allow compensation to be paid to the grieving families, and it will allow the building to be re-built. However the coverage is nothing more than the normal standard of insurance that is expected in the workplace.

Whilst it can alleviate some of the financial risks the money that the insurance settlements will bring is not in itself protection against the risks involved, this requires an active risk management program.

Building a Comprehensive Risk Management Program

The first step in corporate protection is to develop and maintain programs to identify and assess and categorize risks, then to ensure active plans are in place to monitor mitigation activities and track the status.

There is a need for a high-level corporate group to monitor all of these risks. This requires C-Level sponsorship across all categories and regular reviews to ensure that

- Risk Planning
 - Per Business unit
Each business unit is expected to assess prospective risks faced.
 - Per Location
Locations must each have a separate working plan .
 - IT plan
Each system requires some form of fail-over capability and certain at-risk businesses should locate their Data Centre off-site
- Impact of non-implementation

Ultimately all corporate risk relates to financial risk management. We all tend to define risks in terms of their effects on a firm's accounting results—such as earnings, net interest income, and return on assets, etc. They also have an insurance impact. Professional management of the risk is the key to success.