“It Will Never Happen To Me”

When disaster strikes, it arrives unexpectedly. And the consequences could be dire enough to put you right out of business. How can you ensure that your business is well-prepared for the next crisis?

Today, with new innovations arriving into the scenes at breakneck pace, most businesses are held ransom in a competitive “ball-and-chain” scenario – by complex business processes further entwined in a deep, perilous reliance on Information Technology (IT). In particular, for Small- and Medium- Businesses (SMBs), most do not have a contingency plan or any response mechanisms to fall back on when a crisis strikes, and this can be attributed to certain some popular beliefs which include:

**Myth 1** Business Continuity (BC) or Disaster Recovery (DR) planning are luxury suites reserved for the bigger boys;

**Myth 2** My organization is too small to require a crisis management plan; or

**Myth 3** Crises are one in a million – it will never happen to me.

What, then – if a crisis really does strike?

**CAN YOU AFFORD A CRISIS?**

Firstly, a crisis is defined as any situation that is threatening or could threaten to harm people or property, interrupt business, damage reputation and/or negatively impact share value.¹ Often, many SMBs are less disaster-resilient than larger, geographically dispersed multi-national corporations (MNCs). However, when a crisis strikes, the consequences suffered by a smaller company are usually dire enough to put it right out of business. During the famous September 11 1993 attacks in the United States of America, 18,000 businesses based in the New York regions were affected, with a vast majority being small businesses.² The smaller businesses were particularly vulnerable to the disaster impact and losses

---

¹ Respond to crisis before they arise, Johnathan Bernstein, Crisis Management Blog http://bernsteincrisismanagement.com/docs/respond_to_crisis_before_they_arise.html
because they had relatively smaller cash reserves. Those that were forced to close down operations temporarily encountered immediate cash flow problems. 150 out of 350 businesses affected during the World Trade Center bombing failed to survive the event. On the contrary, those that had tested and well-developed BC plans in place had their businesses back up and running within days.

**IT COULD HAPPEN TO YOU**

On a smaller scale, a lack of maintenance and negligence on the part of Development Bank of Singapore (DBS) witnessed a seven-hour system outage and disruption to its services. Any of the following: fires, security breaches, power and system outages, equipment failures, etc – can all potentially lead to loss of valuable data, costly and lengthy downtime, etc. The worst scenario that can befall during a crisis would be to suffer heavy losses in revenue, or like in the case of DBS, inflict irreparable damage to that business reputation you have painstakingly built over the years. However, there are steps you can take to prevent any of these from happening. And the good news is – your business does not have to wait for a crisis to happen.

**EXPECT THE UNEXPECTED**

“The way you manage a crisis is through the work you did before the crisis.”

*Mike Hatcliffe, head of corporate practice, Ogilvy Public Relations*

**Plan B: Business Continuity (BC) Planning**

BC planning and DR planning are often used interchangeably for business survival in the event of a crisis. Most contingency planners have currently included DR planning as a subset of BC planning, which itself is a subset of risk management. BC planning is defined as a concept used to create and validate a practiced logistical plan for how a business or organization will recover and/or restore partially or completely interrupted critical functions within a pre-determined time after a disaster or extended disruption. This is usually deployed by businesses to cushion the effects or impact of a business disruption, and is usually developed based on three core elements: business analysis, risk assessment, and crisis management.

Business Analysis Identify the nature of your business and which are processes are most critical and vulnerable to impact during an event of crisis. You should also identify the related dependencies for these processes, i.e. employees, infrastructure, equipment, etc.

Risk Assessment Evaluate the threats and vulnerabilities of your business. Learn from others’ mistakes and research on your industry’s past occurrences. Identify and formulate a crisis management plan by prioritizing the various crisis scenarios which may happen to your business. Plan for a crisis before it actually strikes and train your employees on the steps to take during the event of a crisis.

---

3 DBS CEO acknowledges censure by MAS, apologises for outage, [Channel News Asia, 4 August 2010](http://www.channelnewsasia.com/stories/singaporebusinessnews/views/1073318/1.html)

4 Business continuity and disaster recovery planning from an IT perspective, [David Bird](http://www.contractpackaging.org/files/public/BusinessContinuityBirdQuatro.pdf)

5 SMB business continuity basics, [CIO Blog](http://searchcio-midmarket.techtarget.com/tp/0,289483,sid183_gcI1180131,00.html)
On the IT fronts, you can avoid certain technological risks by taking up a clearly delineated technology adoption blueprint. Apart from fulfilling regulatory requirements for certain industries (such as Sarbanes-Oxley Act), the following measures can help remove potential risks and significant costs from operations and maintenance in your business IT:

- Plan your technologies according to your business needs. Don’t jump in innovations without first understanding your various options and alternatives available.
- Evaluate the budget required to acquire that technology. Many businesses adopt technology to the point of crisis which leads to overspending, yet acquiring less than satisfactory outcomes.
- Maintain and update your hardware, software, databases and networks regularly.
- Don’t save on security. Spending on security to protect your business from viruses, spam, DDoS attacks, etc can prevent the occurrence of a crisis, leading to much more exponential savings.
- Use only licensed software. Pirated or illegal software usage will not only flout regulations, but places your business at a higher risk of security breaches and service outages.

Crisis Management

What if crisis has already struck? Which are the steps you should take?

Communications & Execution
Firstly, you have to understand and differentiate between the marketing functions in non-crisis situations and a crisis scenario. The routine marketing function is to build and establish the value of your business, but a crisis communication function is to preserve that value. Identify your key audiences, authorized spokesperson/s and communication channels, and inform your crisis management team of your communication messages and the necessary steps to take. Here are some tips to follow in crisis communication:

- **Be honest** Formulate a communications message and stick to it.
- **Do not evade, avoid or argue** By doing any of these, you will only be putting your business in a worse situation than it already is. If you do not know the answer, do not lie but instead, communicate clearly that your team is working on it.
- **Emphasize on positives**, but not to the extent of exaggeration.
- **Explain the steps and solutions** you are taking in order to correct the situation.
- **Leverage on online platforms** If you already have an online presence established for your business, take advantage of channels like Twitter or Facebook to communicate to your affected clientele directly and rapidly.

DON’T FALL INTO THE COMPETENCY TRAP

Here is the reality. According to Crisis Management expert, Johnathan Bernstein, most businesses do not engage in crisis planning until they have been badly burnt.
“Small businesses cannot afford that. They are much more likely to go out of business due to being ill-prepared.” Jonathan Bernstein, Owner, Bernstein Crisis Management

Most SMBs cannot afford a crisis simply because they will not survive one. A crisis can happen to any business in any industry and many fall into the "it will not happen to me" trap where they do not have a Plan B ready in times of a crisis. Less than five per cent of businesses do not have a crisis plan in place unless one has already occurred. It is important to note that a standard crisis agenda usually includes 10 to 15 scenarios. But in many cases, it is always the 16th one which strikes. Prevention, rather than reaction, is the key to success of any crisis management plan. Take a pro-active stance in anticipating every plausible scenario and ensure that your crisis preparation is perfect, if not, it has to be really close to it – because when disaster strikes, no amount of preparation is ever enough.

**KEY SUMMARY**

Many SMBs do not have a contingency plan or any response mechanisms to fall back on when crisis strikes.

A crisis is defined as any situation that threatens to harm people or property, interrupt business, damage reputation and/or negatively impact share value.

Business Continuity planning and Disaster Recovery planning are often used by businesses interchangeably to deal with crises.

The core elements of a Business Continuity Plan includes: business analysis, risk assessment, and crisis management.

Less than five per cent of businesses do not have a crisis plan in place unless one has already occurred.

---

6 Respond to crisis before they arise, Johnathan Bernstein, Crisis Management Blog  
http://bernsteincrisismanagement.com/docs/respond_to_crisis_before_they_arise.html  
7 Crisis Management: Execute Your Plan, O & P Business News, 1 Dec 2009  