

BCP In Asia: What I Learned On The Way To The Disaster

Nathaniel Forbes

Director, Forbes Calamity Prevention, Singapore

Email: nforbes@calamity.com.sg

ABSTRACT

After 10 years in Singapore, managing a business continuity planning consulting firm that he started from scratch in January 1996, the author discusses what he's learned and how it can help others complete contingency plans faster, better and with fewer obstacles.

1. Introduction

I started a BCP consulting company called Forbes Calamity Prevention¹ in Singapore in January 1996. Our firm helps multinational companies prepare business continuity, crisis management and emergency response plans, primarily in Asia. I started the company at a time when no one had ever used the words "business continuity planning." Few companies in Asia did much more for disaster recovery than backup their data, and even fewer thought contingency planning worthy of management attention.

The Central Bank of Sri Lanka was bombed the same month I started the company. The first World Trade Center bombing² in New York City was an even more recent memory than September 11, 2001 is to us today. Computer data was stored on tape reels³ in a "tape room," often right next to the data center in the same building. Whether or not disasters were less frequent ten years ago than they are today, it is fair to say we were all much less concerned about *man-made* disasters 10 years ago than we are now.

Ten years more experienced (if not wiser) than I was then, I've helped prepare contingency plans for companies all over the world (but not yet in Sri Lanka). I've had an entrepreneur's exhilarating journey, and I've learned some lessons. In preparing this paper and presentation for the CSSL, I've thought about what might help you move forward with your own contingency planning. Here are some lessons I've learned, not necessarily in the order in which I learned them, but in the order in which you might apply them to your own planning.

2. We are always prepared for the last disaster

Even my mother asks me, "What kind of disasters do you plan for?" We plan for all kinds, of course, but to be honest, we're like the proverbial generals who are always preparing to fight the previous war. We are

always one disaster behind. When we imagined that only weather or a computer crash could cause a calamity, we were surprised by acts of terrorism. So we started preparing for terrorism, and instead we got SARS. We responded to SARS and started planning for 'bird flu', and instead we got a tsunami.



My client, a bank, lost its office in the October 1997 World Trade Center bombing in Colombo⁴. After that incident, we often used bombing or fire as our disaster scenario. Little did we suspect that the next year, another bank would activate our contingency plan not because of a bombing, but because of riots in Jakarta in May 1998. Every business in Jakarta was closed, so serving their customers was not important. Instead, distributing payroll to employees was their most serious challenge: many employees in Indonesia don't have bank accounts, so payroll is distributed in cash. All banks where cash could be obtained were closed. As the Indonesian rupiah was grossly devalued at the time, the physical cash required to meet payroll weighed many kilograms. Asking expatriate managers to carry around and hand out large amounts of cash during a riot was not considered prudent. In our planning, we hadn't considered any of these difficulties: *both* the disaster scenario *and* resulting challenges were unexpected.

I did not guess on Monday, September 10, 2001 that airplanes would fly into America's tallest buildings the next morning. Nor did I have any idea in March, 2003 that chickens and ducks were about to cause \$15B in SARS damage to Asia's economies. I read that avian influenza may devastate populations in Asia in the future, but I'd bet that the next business disaster in Asia will be something that I cannot predict today.

3. Pictures & stories aren't persuasive

No one is persuaded to prepare a contingency plan by seeing pictures or hearing stories of disasters that happened to other people. No manager I know ever looked at pictures of a disaster – no matter how close to his own office – and said, “Gosh! Isn't that awful! I better prepare a business continuity plan.” There is no connection between the fact that “it happened to them” and the possibility that “therefore, it could happen to us.” People simply do not believe it, or don't want to believe it.



Heart-rending and award-winning as this tsunami photo is, few managers will be sufficiently moved to initiate a business continuity planning project because of it.

I know of a company in Singapore that lost US\$12 million in a fire in June 1997, had a substantial environmental clean-up liability and took years to rebuild its business – but when I called some time later, the owner had no interest in talking about BCP. A bank that had a fire in its headquarters in Europe *and* a fire in its trading room in Singapore only started preparing a BCP when regulations in the bank's European home country made it mandatory.

On the other hand, sometimes a disaster happening to a company *is* a motivator. ABN Amro Bank started its Asia BCP project in October 1997, just after the bombing of the World Trade Center here in Colombo. Futures and options broker Refco called us for help with their BCP in October 2001, because the company's New York office had been closed by the WTC bombing a month before. We started to prepare a BCP for a British bank's North American offices in early 2002; their employees had *walked* out of Manhattan on September 11.

There is at least one other motivator besides personal experience that gets management's attention: the prospect of going to jail. In the U.S., where 75% of companies now report⁵ having some form of recovery plan, a new law is the reason: a director or manager faces personal civil or criminal liability for failure to comply with Sarbanes Oxley. When the law in Sri Lanka requires a company's directors and managers to prove they have a viable continuity plan, or be hauled

off to jail, I expect you will notice renewed interest in BCP. When more governments in Asia adopt similar rules – and I believe strongly that they will – you will start to see widespread planning activity.



Electrical Power Risk

This is a 10-year-old office complex with two towers of 40 storeys each in Bangkok, Thailand. We were surprised to discover that the only source of electrical power to our client's tower came in on this power pole, standing by the kerb of a busy thoroughfare. The cables were easily accessible to anyone with malicious intent. We'd expected electrical power to a modern building to have been buried below grade.

4. Risks: Don't Ask, Don't Tell

All contingency planning methodologies tell you to start by completing a risk assessment or analysis to determine and rank threats in order to prioritize risks to the business. The risk calculation is done by multiplying a quantitative measurement of likelihood by a quantitative measure of impact, and expressing the result over a period, usually measured in years. So, a proper risk statement looks like: “There is 1:2 (or 50%) chance that (we) will experience a power outage lasting longer than two (2) hours in the next four (4) years.” Simple enough, but is it useful for decision-making?

I remember exchanging email in 1996 with a colleague in the U.S. about a prospective bank client in Asia that wanted to skip a risk analysis: the bank told me, “You should know what risks banks face from your past experience.” “Ridiculous!” retorted my colleague. “No two banks are alike, and no two locations are alike. Assuming the risks in one location will be the same in another – particularly between the U.S. and Asia – is crazy!”

True perhaps, but I found that companies in Asia won't spend time or money on risk analysis. Managers already know – or believe they know - what risks they face, and experience is their chief guide. If you ask

about the risk of earthquake Singapore, everyone laughs. Ask about it in China or the Philippines, and everyone nods knowingly. Companies don't even pay their insurance companies for risk analysis: they expect their insurance companies (or re-insurers) to provide risk assessments at no charge. And when we ask about a worst-case scenario, everyone has a different opinion.



Power & Flooding Risk

In 1992 Thailand passed and began enforcement of a National Environmental Quality Act⁶ which specified "Building Effluent Standards"⁷. In effect, this legislation requires owners of office buildings constructed after that date to treat sewage effluent from the building before releasing it into an over-burdened municipal sewer system. During a risk review of that building, we came upon this sight - 50,000 litres of raw sewage in treatment tank in the basement parking garage. We learned there was no backup power for the pumps which empty this effluent into the municipal sewage system. If the power failed, the basement could flood with untreated sewage. This photograph cannot convey the overwhelming fragrance in this room.

5. What's the worst that could happen?

What is the worst case scenario for most companies? What's the worst that could happen to *your* company? And is *your* worst case scenario much different than your competitor's? I don't think so.

I learned that most managers consider their greatest risk **any event that would render their company's office unusable, but that would allow their competitors and customers to continue to function.** In short, the disaster would be very localized. This is called a 'denial-of-access' scenario, and it can be caused by fire, flood, power outage or terrorism, among others. Yes, a tsunami could hit, but you will agree that it is unlikely to wash away only your

building. Even if you *don't* agree, the consequences of a tsunami and of a power outage are the same to a business: the business could not use its facilities.

So we've learned to use risk *assumptions* instead, which require no calculations, no research, and very little historical evidence. We ask managers to *assume* they would be unable to get into their buildings, and would be unable to use anything in those buildings, including any IT systems hosted there. For most companies in Asia who do not have a BCP, this is a plausible, useful way to start a BCP – and to skip or postpone a time-consuming risk analysis.



Fire Risk

This is a picture of the loading dock in the basement of a new office tower in Singapore⁸ in 1998, when we did a facility risk review for a client in that building. That's a devotional altar, quite common in countries with large Chinese populations. Note the burning oil lamps and the brown streak of residue on the wall above the altar. That's a cable tray running across the top of the picture, and in it was cabling carrying all our client's voice and data traffic. The company never imagined that its business was at risk from an oil lamp in the basement.

If the disaster assumption, then, is a denial-of-use or denial-of-access, how likely is your building to "fail" in some way? To answer that question, we conduct a **facility risk review**. We examine a building's infrastructure and services:

- Air conditioning & ventilation
- Voice and data lines into the building
- Fire monitoring, suppression systems
- Automated security system, guards
- Vehicle access & parking

- Building Automation System
- Exit route, escape route, assembly areas
- Insurance coverage for tenants

I assumed that in a modern office building in any major Asian city, the likelihood of a building's infrastructure or utilities failing would be low. What I've learned is that simply walking around a building with a checklist, accompanied by the property manager, nearly always turns up surprises. These surprises often turn out to be a much greater threat (and therefore a risk) than most companies imagine. There are pictures throughout this paper of some of the surprises I've found in Asia. There are probably some in your office building, too.

6. Methodology madness

Most professions have standard professional practices and an accepted methodology to the practice of the profession. In BCP there are the **Professional Practices of the Disaster Recovery Institute**⁹ (DRII) and the **Business Continuity Institute's** Good Practice Guidelines¹⁰. They are widely promoted as the "correct" way to do BCP.

I discovered there is no one, correct BCP methodology that works everywhere. Examples of successful – and unsuccessful - deviations from DRII and BCI methodologies abound. Perhaps it is more accurate to say that BCP methodologies are *evolving*.

For example, it seems logical, and the DRII methodology specifies, that testing should follow preparation of your BCP. I recently attended a conference in the U.S., however, at which several BCP professionals advocated testing first and then developing a BCP based on the results of the test. They argued that this methodology can speed up the planning process, and get management's attention by having them discover how ill-prepared they are. This turns the standard methodology on its head – but it may turn out to be very effective.

Even our own methods for conducting a business impact analysis¹¹ (BIA), for example, have changed significantly over the years. At first we interviewed at length one manager from every department to obtain Recovery Time Objectives¹¹ and Minimum Operating Requirements¹¹ for every activity in his or her department. This was time-consuming and expensive. To save time (and therefore cost) for our clients, we began to limit our interviews only to senior executives, and instead we distributed written BIA questionnaires that department representatives could complete on their own time. This saved time initially, but we found ourselves spending a lot more time chasing respondents to explain insufficiently-detailed answers

to questionnaires. We've learned that interviews are better for some situations, questionnaires better for others.

No matter how we collected it, eventually we distilled the BIA information we collected into a table format¹², and presented it to management orally. This process took weeks, sometimes months, but we imagined our BIA conclusions to be unassailable, because they devolved from our elaborately documented investigation. I was stunned the first time a CEO looked at our meticulously-prepared results and blurted out, "Who told you we needed *that* many people in Customer Service?!" With a pen stroke, he revised several months of our work. Now our methodology *starts* all projects with the senior managers setting recovery objectives and parameters for the company, and only refines their decisions with information collected in the questionnaires and interviews.



Communication Risk

The insurance business of our client in Tianjin, China depended heavily on voice and data communication. In our review of the company's office building, we discovered that all voice and data traffic ran through the cables on the roof of an outbuilding (above) on the adjacent property. Not only were the cables entirely unprotected from the trees above them, neither our client nor its landlord could do anything about the risk without the cooperation of its neighbor.

Just as we've found that there is no single acceptable methodology, we've also learned there is no single outcome that applies uniformly, for example, to all accounting and finance departments, even though their business activities may be very similar. There is no "right" recovery strategy that applies to all manufacturing companies or to all supply chain logistics companies. There is no internationally-accepted Recovery Time Objective for a bank treasury department.

7. BCP needs inspiration and perspiration

I've learned that to complete and sustain an effective BCP, there is no substitute for a dedicated, impassioned, full-time BCP coordinator. Business managers and staff can and should be responsible for making BCP decisions for their departments, but that doesn't mean they actually have to prepare or write their own plans. To expect department heads to write their own contingency plans is, in my view, a bit like asking them to write their own software. They own the responsibility and the results, but they can outsource the work.

Nor does it make sense to me to have specialists for security, human resources, facilities management or corporate communications, but not for BCP. Preparing a BCP requires training, experience and judgment no less than any of these professions. Many companies in Asia can't afford to have full-time BCP professionals on staff, and so they contract with outside experts who can devote their full attention to planning. In a large company, developing a BCP, testing it and maintaining it is a full-time job. In some multinational companies, it's a department.

BCP is not, and should not be, a responsibility of the IT department. In many companies we've helped, BCP was initiated by - sometimes even sponsored by - the IT department, but IT's only responsibility was to ensure that business managers made the required decisions to complete the BCP. Thereafter, IT should be responsible only for ensuring that IT recovery capabilities meet the recovery requirements set by the business.

I've slowly concluded that maintaining separate departments for BCP, security, facilities (property management), corporate communications, IT security and risk management will eventually prove unworkable. A good continuity plan provides for emergency response, crisis management and business recovery, and those cannot be comprehensively managed without all of these departments - and the rest of the business - working together. I have come to the conclusion that large organizations will one day appoint a **Chief Continuity Officer** to whom most or all of these departments will report, and who will be report to the Board of Directors, as Internal Audit does.

8. BCP software

Eventually, every company trying to manage a large number of written plans wonders if BCP-specific software is a worthwhile investment. I don't see BCP software in use in Asia, for several reasons, of which high price is often the first: software from the major publishers, Strohl Systems¹³ and Sungard¹⁴, costs several thousand US dollars for a single-user license, and can easily cost more than US\$100,000 for a large

company. The software and support are available only in English. Until recently, that support was only by phone or email, and only from North America; Strohl now has an office in Singapore. BCP software is by nature used irregularly and so training (more precisely, re-training) and support can be challenging.



Flood Risk

Seasonal flooding is an issue in many countries in Asia, but no where else in Asia has urban infrastructure been built as extensively to mitigate its effects as it has been in Taipei. We performed risk reviews of four buildings in Taipei in 2002 and 2003, and every building we visited had a flood-control gate at the street-level entrance to the below-grade parking garage. The gates were about 80 centimeters in height when raised. Some of them were manually operated; a security guard was expected to rush out to swing, pull or crank the gate into place in a storm. Some operated automatically. This one, at a bank building, had sensors in the storm drains in front of the building which automatically raised the gate when the water reached a certain level.

I've found BCP-specific software of value primarily to an organization's BCP coordinator, because the software's database features permit consistency and synchronization across the organization. The "users" of the plans - department staff - benefit no more from using BCP software to write their plans, in my experience, than from using Microsoft® Office® software.

As a result, only multinational, primarily North American Fortune 500 companies buy and use BCP software in Asia¹⁵ - and most of them use MS Office software instead. For creating large volumes of paper BCP's to store in notebooks, or to show to internal auditors, Microsoft Word and Excel seem to work just fine and are, in my experience, the most widely-used BCP software programs in Asia.

9. Public-Private Partnership

My last observation is that dialog and cooperation between the public and private sectors in Asia are non-existent; at least I've never seen any. In the U.S. plans and exercises are very often developed jointly by specialists from private industry with leaders of local, state and federal emergency response agencies. In Asia, not only is there little dialog, but the public authorities don't seem to see any need to reach out to the private sector until *after* a disaster like the December 2004 tsunami.

Why is this important? Public authorities would be overwhelmed in any Asian city or country – as they were in Sri Lanka – by an event of the scale of the tsunami. Public authorities depend on the resources that private companies can contribute to a recovery effort. Without cooperation and joint planning in advance, those efforts will overlap in some areas, overlook other areas, and conflict in still others. A simple example: you set an assembly point outside your building to which evacuating employees should escape in an emergency. Will the emergency authorities permit you to assemble at that spot in a real emergency at your building? Have you mistakenly selected the spot where the fire department plans to set-up its command post? Can you call them up to ask? And if not, why not?

Another example: as the BCP manager for your company, you will want to assess any damage to your

office as soon as possible after an incident, or you may want to retrieve important papers from the building. Under what circumstances will emergency responders permit you to do that? This question is of sufficient concern that major U.S. cities have established a Corporate Emergency Access System¹⁶ (CEAS), which permits credentialed representatives of companies to cross police and fire lines specifically for business continuity purposes. A similar system is, in my opinion, desperately needed in the major cities of Asia.

I commend to your attention the International Association of Emergency Managers¹⁷ (IAEM), which offers professional certification for emergency managers and includes members from both the public and private sectors. Efforts are under way to form a chapter of the IAEM in Asia, based in Singapore.

10. Final Thought

What is the single, most valuable BCP lesson I've learned in the last 10 years? It is this: never argue about what disaster might happen. As I stated at the outset, I'm very poor at predictions. Moreover, I don't think the *cause* of a disaster is as important as the *consequences* of a disaster, in particular to the businesses of my clients. So I've reduced the sum of my experience to three words, which I urge you to remember when someone wants to challenge your desire to commence or improve contingency plans at your company: **Consequences, Not Causes.**

Hyperlinks in this Article:

1. www.calamity.com.sg/Forbes%20Calamity%20Prevention%20Profile%202005.pdf
2. news.bbc.co.uk/onthisday/hi/dates/stories/february/26/newsid_2516000/2516469.stm
3. en.wikipedia.org/wiki/Tape_storage
4. brcsproject.gn.apc.org/slmonitor/october97/truck.html
5. www.business.att.com/nx_resource.jsp?repid=Topic&rtype=Whitepaper&rvalue=riding_the_storm_business_continuity&repoitem=business_continuity
6. www.deqp.go.th/english/greendata/env_standard/124122.html
7. www.deqp.go.th/english/greendata/env_standard/main_env_std.html
8. www.thehighrisepages.de/hhkartei/sincennt.htm
9. www.drii.org/displaycommon.cfm?an=2
10. thebci.org/design2005/gpgdownloadpage.htm
11. www.calamityprevention.com/bcp_terms_eng.php
12. www.calamityprevention.com/bcp_docs.php
13. www.strohl.com
14. www.sungard.com
15. www.continuitycentral.com/news0235.htm
16. www.securitymanagement.com/library/001652.html
17. www.iaem.com

The full text of this article, with hyperlinks, can be viewed at www.calamityprevention.com

Nathaniel's full biography can be viewed at www.calamityprevention.com/Nathaniel_Forbes.PDF