

11 June 2004 CIO Asia

The Business of Security

How two financial services giants tied business continuity planning to the business--not to security. By Ann Toh

FEAR, UNCERTAINTY AND DOUBT--for years that was how CIOs sold security. Today, as two best-practice financial services organisations show, there are more effective ways to get that security spend and keep people's eyelids from drooping than by painting disaster scenarios.

BUSINESS CONTINUITY CHAMPION

Global financial services provider Deutsche Bank AG was a survivor of the Sept 11 terrorist attacks in New York on Sept 11, 2001. The Singapore branch of the bank, its Asia Pacific headquarters, has since been facing the challenging task of getting the bank and its employees interested in business continuity planning, and high on disaster recovery readiness.

An employee who knows a disaster when he sees one is Kenny Seow, head of Business Continuity Management (Asia Pacific), who has been facing the quiet challenge of getting his colleagues excited about business continuity planning at the bank for the last five years. The 14-year business continuity planning (BCP) veteran heads the bank's BCP function, which liaises with and brings together various internal units and experts dealing with risk--be it information risk, physical risk or business risk--to coordinate plans and strategies that address the loss of facilities, personnel or critical systems, and get them implemented.

"The work of business continuity planning requires a diverse set of skills," says Seow. That is why the bank harnesses individual teams of experts--from people who are responsible for the business lines and operations to those dealing with IT and physical security--to formulate a total protection programme.

Seow is lucky to work for an organisation that has always cared about business continuity planning, even before the horrific events of Sept 11 and Severe Acute Respiratory Syndrome (SARS). The Bank takes an integrated, risk-centric approach to information security, physical security and business continuity. It has created a structure to manage and govern business continuity management (BCM). BCM is a board-level concern at Deutsche Bank. It has full-time teams in Singapore, the bank's Asia Pacific headquarters, and in its bigger locations, Hong Kong, Japan, Australia and India, to manage BCM. The role of these units is to ensure that processes and resources are in place so that when an incident occurs, the bank can respond effectively, says Seow. He adds: "In Deutsche Bank, because BCM is recognised as such an important function, it has a direct line of reporting to the regional Chief Operating Officer. Business continuity risk is considered one aspect of the various risks we manage, such as operational risk, market risk or credit risk."

The self-professed optimist believes that incidents can happen but the bank can do something about them through business continuity planning, "which revolves around planning for different scenarios of incidents to make sure business can continue." At the epicentre of its business continuity plan is its new 12,000-sq ft Disaster Recovery Centre (DRC) outside the Singapore Central Business District, a "lights-out facility" (meaning no staff is housed within during normal operations). The facility houses work space to support critical business functions and operations for over 200 staff, and all backup computer and network equipment required for disaster recovery. The data centre also acts as a backup regional processing hub for Asia Pacific; its aim is to protect the Asia Pacific region from outage at the production data centre. The systems are monitored and controlled remotely, either at the production data centre or at Deutsche Bank's office premises where its IT Infrastructure staff work.

The carrier-neutral facility uses 240 kilometres of cabling, covering a distance six times that from eastern to western Singapore. Resiliency is provided by a dual power feed, dual power distribution and dual telco risers. The UPS uses a generator with a 10-hour refillable fuel tank. The site is also fire regulation

compliant, with smoke detection using VESDA, pre-action water sprinklers and water detection, and has an environmental monitoring system.

CIO Asia speaks with Seow about how security and IT chiefs can position disaster recovery to get their colleagues and management's attention with regards to security and business continuity planning.

CIO Asia: What is a disaster to your company? What incidents do you address in your business continuity planning (BCP)?

Kenny Seow: An incident is any event that might prevent us from doing business. It doesn't have to be a bomb explosion or an earthquake but can be for instance a flu bug. Our approach for BCP is to drive our planning according to the worst-case scenario. As long as we cannot operate our business, for whatever reason, our plans must be robust enough to [get us back up and running as soon as possible.] There are two levels to our planning: first we ensure preventive measures are in place, such as having backup power for critical systems in the event that the main power supply goes down. The second level is looking at recovering from the actual loss of premises or IT services and how to ensure continuity of business.

Did the recent events such as Sept 11 and SARS change your company's approach to, and focus on, business continuity?

The recent incidents have highlighted the importance of business continuity planning, but they have not significantly changed our emphasis on BCP as it has been a focus at the bank for many years now. BCP is a result of management prudence that says that we have to protect the interests of our stakeholders--customers, employees, partners, regulators and shareholders--and protect the company against reputation loss and potential revenue loss. However, each incident did give us new learning experiences that we use to improve our plans. For example, in managing SARS, we learnt to formalise World Health Organisation and Ministry of Health guidelines within the organisation so that our staff were aware of them, and the importance of communicating factual information to educate employees, put the record straight and squelch uncertainty and rumours. We also looked at the segregation of staff by making sure critical staff were working from different buildings.

(For lessons it learnt from these incidents and details on its best practices, see Deutsche Bank's Best Practices.)

How do you make a persuasive case for business continuity planning?

The level of awareness for the need for business continuity planning has gone up in the financial services industry, which has made it easier for us to justify the expense of business continuity to management who together with the regulators are more aware of it and are paying more attention to it. But that doesn't mean that we get a blank cheque. We still have to justify spending millions of dollars on recovery just like any prudent budgeting process. We sell it by talking about the potential business impact to the bank should something happen. What is the best strategy to manage risk? Should it be spent on preventive measures or recovery measures?

You mentioned that business impact analysis is the starting point of your entire BCM process to find out what your critical activities are. How do you find out what functions you need to have for you to continue business in the event of a major disaster?

What my team does at the bank to facilitate this process is to organise and conduct interviews and meetings with business heads to identify what is critical to them. This could be revenue loss, reputational risk, potential loss of customer confidence, or even violations of certain regulations. From there the businesses themselves will identify and prioritise the processes they must focus on to minimise the impact of the identified risks. The approvals and sign offs must come from the heads. It's important this is done by a senior person because you want an organisation-wide view of what is important.

We've found that there are two broad groups of critical processes: the business survival processes and processes critical to crisis support. The first comprises processes important to the objectives of the organisation; for instance, the trading folks who are trading money markets and foreign exchange would need to make sure that that business continues because it is a major revenue stream for the bank. So we have a trading room in our disaster recovery site that ensures that continuity. But that alone is not enough, because once they trade, they need to be able to settle, so we have to make sure that they have the backoffice operations to support the trading activity. In banking we call this "front to back" recovery. So all the functions related to the entire value chain need to be recovered.

The second set of processes is the functions critical in crisis management, such as HR. From the recovery point of view, day-to-day HR functions may not be viewed as critical but they provide a very important crisis support function because they need to look after staff welfare and staff counselling. So does Corporate Communications. Most likely, marketing is relatively less important than these two functions in a crisis situation.

Is the concept of risk a hard-to-grapple concept for your business colleagues?

No, we are talking about bankers who handle risk all the time, whether it's market risk, credit risk, fiduciary risk or operational risk.

Insuring Against Disasters

James Kang, CIO of Singapore's largest general insurer NTUC Income Insurance Co-operative Ltd, once watched his company nearly go away. The incident, which Kang would only say occurred in the last two years, happened because hardware running its business-critical insurance systems went down, threatening to lose the day's data as Kang's disaster recovery system only did daily backups, at the end of each day, as opposed to doing "live" backups.

Amidst the pressure of having to answer to his CEO and business colleagues about work stoppage at Income's headquarters and branches, a result of the hardware crash, Kang had to make the judgement call of whether to activate his disaster recovery system so that operations could continue--but that would mean losing the day's data, a task that would take a year to reconcile. His vendors who came down to offer technical assistance to revive the machine said there was a 50-50 chance that they could bring the machine up and restore lost data, and so Kang made a decision not to activate his disaster recovery system.

The next day, operations at the HQ and branches remained shut as engineers from the vendor company attempted to resuscitate the machine. "The pressure was tremendous," says Kang. "Not only had I to keep my CEO informed, as the hours ticked by, we stood to lose half a million each day, and we made a decision that by the evening of the second day, if we could not bring the system up, we would bite the bullet and activate disaster recovery." Fortunately, in the late afternoon of the second day, the engineers managed to bring the machine up and avoid any loss of data. The only casualty from that incident was two days of lost operations.

Today, Kang does not have to worry about the risk of losing data in that way. His company recently built a disaster recovery infrastructure based on Oracle Corp. Database and Real Application Clusters running on Hewlett-Packard's HP rp7410 servers. With the system, Kang says he now has a "real-time, fully redundant" disaster recovery system that can be placed on "24 x 7 hot standby for immediate cutover in the event of system breakdown". (See Income's Disaster Recovery Infrastructure.)

Kang calls himself a realistic optimist where business continuity management is concerned. The realist in him acknowledges that the world has gotten "quite risky" with the close calls of terrorist threats such as Jemaah Islamiah and infectious bugs such as SARS, but the optimist in him believes that technology has advanced very quickly to help mitigate those risks, with "open systems, connectivity, high availability and 'hot' disaster recovery." He adds: "Even the legal infrastructure has kept up to support these technological

advances. For instance, the Evidence Act now allows paper-based legal documents to be converted to electronic legal documents so that they can be used in court."

As such, starting last year, Income has been converting its 40 million paper-based insurance policies, which used to occupy three warehouses, into digital records. This is expected to be completed by the end of this year. It has outsourced the conversion work to Trusted Hub Ltd, a member of the Singapore Technologies Group, which Kang says is certified to comply with the guidelines spelt out in the Evidence Act to transform legal documents into imaged copies so that they are admissible in court.

Now that every policy has a digital counterpart, Income no longer has to fret over the very real scenario of floods and fires destroying age-old legal insurance policies. "We can also access the records anywhere regardless of time zone," says Kang. He adds: "Lastly, it will bring our costs down, as it has been very costly to keep insurance policies in a warehouse for as long as 80 years, as in the case of a life insurance policy. Warehousing is labour-, land- and energy-intensive, but the price of a hard disk decreases by half every year even as land costs go up."

The forward-thinking organisation believes its business continuity strategy will transform its business. "It will make us more robust. We'll never be caught red handed when disaster strikes, and our cost will be lowered by millions--so we took advantage of technology and the legal framework to move ahead," says Kang.

CRYING WOLF

For years, CIOs like Kang has sold security by crying wolf, using fear tactics and causing uncertainty and doubt. Now, Kang likes to sell senior executives on how disaster recovery will make doing business easier for the company. "We operate in an industry where customer trust and confidence are important to our business," he explains. "When a major system goes down, it can cost us half a million a day, not counting the negative brand impact. That's how we justify the expense of our disaster recovery systems."

Business continuity planning involves first being able to account for the critical applications they have on their networks. "We have identified the critical applications core to keeping our operations going. Even among these, we have had to prioritise the more critical. For instance, in a disaster, the issuing of claims is more important than the collection of premiums, as a delay in paying our claimants when they make a claim is less acceptable than a delay in accepting premiums." It has also involved contracting a cybercafe as a disaster recovery site for the use of its broadband facilities."

Ann Toh is Associate Editor with CIO Asia.

Source: <http://cio-asia.com>