Business Continuity Planning: The Treasurer's Priorities

For the treasurer, disaster recovery and business continuity planning demands rigorous scrutiny of external providers as well as internal processes. Moreover, today's treasury technology brings both new risks and solutions. What questions should treasurers be asking themselves and their banks to safeguard the firm's finances in an unstable world?

External and internal readiness

For the treasury, disaster recovery / business continuity is not just a matter of maintaining and monitoring internal systems and processes. Nor is it solely a question of ensuring back-up facilities can be depended upon. It is also important to guarantee that the treasury has options in the event of a serious outage by primary banking providers. This should include securing the ability to switch to alternative providers as well as ensuring that the primary bank has robust capabilities.

The need for co-operation and a clear understanding of where responsibility lies for each link in the chain was important in bringing the financial infrastructure back up on September 11th 2001 and it is also a key part of the bank-client relationship when addressing business recovery issues. As such, treasurers should ensure that they know precisely where and when their responsibilities end for a transaction or process and the banks' begin.

In this article, we look at how recent trends have affected the treasury's business recovery plans, the key questions the treasurer should ask and the role of banks in limiting the impact of future disaster scenarios.

Impact of recent trends in treasury

IT-dependence

There has been a temptation for banks and corporates alike to grow complacent about business continuation at a time when their dependence on IT has grown in step with the drive for automation and efficiency. The power of modern communications technologies is awesome, but not limitless. We should remember that increased reliance on internet-based technologies simply changes the nature of operational risk rather than eliminates it: Yes, you can access balance and transaction data from around the world via a browser-based application, but only if all the links in the infrastructure chain that supports it are stable.

The ability for companies to connect — to their employees, banks and other critical vendors and business partners — is vital. From a business continuity perspective, businesses must ensure they have a flexible...
telecommunications infrastructure. This includes the ability to re-route voice and data communications across multiple channels. Also essential is the quick dissemination of information internally and externally as to the magnitude of a disaster and the response. Critical contact details must be accessible both electronically and manually.

**Concentration risk**

Increased use of technology also insidiously heightens concentration risk. The high cost of providing web-based services to corporates is thinning out the field of potential banking providers to multinational firms, whilst the solutions themselves make it easier for corporates to rely heavily on one-stop banking shops. Treasurers who are continually balancing the need to expand sources of credit whilst reducing their number of banking relationships will understand all about managing concentration risk. As if this were not already complex enough, September 11 added another dimension to the risk / reward balance.

The benefits of working closely with a primary bank (tailored solutions, high service levels, access to wide range of product specialists, mutually supportive levels of commitment etc.) are well established. But this should not blind the treasurer to the risks of over-reliance. What is your back-up position when your lead bank’s primary systems go down? What proportion of balances can you access without the latest version of your bank’s e-banking software?

Whilst the temptation is there to embrace the latest technology, remember that it can tie you much closer to the bank. On the other hand, many treasury systems and bank-supplied solutions are now web-based and can be accessed from multiple locations. This may offer the office portability required by global corporates to switch from one treasury centre to another in an emergency. Banks can provide flexibility by pushing payment data to a treasurer’s mobile phone or personal digital assistant (PDA). The key is to update your business recovery plans on a continuous basis in order to take on board the implications of all decisions that impact the treasury’s operations (i.e. if we use software vendor X, will they supply a back-up system at a remote site?)

**Additionally**

Other current trends in treasury organisation and technology also need to be taken into consideration. Most treasuries are leanly staffed these days and this can make it harder to manage business continuity risk. Outsourcing treasury processes can add another level of due diligence to your disaster recovery checklist — but shifting key treasury processes to a dedicated, specialist centre can also improve contingency and controls. Whether a process remains in-house or not, policy and procedure documentation needs to be sufficiently accessible to be reached in an emergency, but secure enough to guarantee version control.

Due to easier accessibility, internet and intranet sites are more popular for actively storing contingency plans and for crisis communications. Technologies that enable hot back-up of data ensure that mission-critical data is stored in more than one location. As well as increased use of digital storage and image archiving, we also see companies streamlining their operations processes to digitize at the point of entrance, rather than simply archiving documents electronically at the end.
Physical impact of disaster

The need to revisit business continuity plans on a regular basis was underlined by the scale and nature of the September 11th attack. Whilst many firms upgraded their disaster recovery capabilities in the lead-up to Y2K, the threat they now face is different. The millennium bug may have threatened to put banks’ and corporates’ systems out of action, but it posed little physical danger to buildings or people. In the current unstable political environment, all organisations must deal with the real possibility that key staff may be lost in the event of a disaster. Furthermore, additional staff may be unable to travel to a back-up site due to disruption to the transport system.

Historically, contingency planning concerned the loss of a building or specific power or telecommunications grid. Now plans must cover the potential loss of a larger geographic area or sub-region. At the same time, while it was previously acceptable to maintain separate contingency and data center sites, in today's environment this is no longer adequate. Distance between sites must accommodate the possibility that employees might need to travel by foot. Moreover, previous plans were built to address an outage of up to 20 days. Current plans must now address a six to nine-month scenario. Issues include the warehousing of staff and the need to gain additional skilled labor.

People, geographic location, communication and technology are the four critical dimensions to a rapid recovery. The key is to stretch each aspect to the limit in determining what you can do. Plans must be communicated to staff and regularly tested.

Employees are of primary concern — the well-being of staff members and their families, the ability to safely change locations and stay in communication.

Following is a questionnaire intended as a tool for assessing your treasury readiness in the event of future business disruption or crisis.

1. Have you reviewed your account information and account structures, as well as authorized signers, security administrators, user IDs, and entitlements with each of your banks to ensure accuracy and do you maintain this information off-site, in addition to on-site?

2. Do you have contingency procedures in place to process payments in the event of a crisis, and do you conduct monthly tests by logging-on to your back-up system and generating at least one live transaction? Also, do you maintain a laptop with updated software, do you review your repetitive lines, have you created a plan for the storage and portability of digital certificates, and do you keep copies of passwords and security token cards readily available both off-site and on?

3. Have you formed an emergency management team and do you have a clear, predetermined chain of command in the event of an emergency? And has this chain of command been documented and widely distributed throughout your organization?

4. Do you have an internal and external crisis communications plan? And have you provided your clients, colleagues, suppliers and other key business contacts with an emergency contact telephone number in the event they cannot reach you during a crisis?
Companies are taking measures to supply more employees with cell phones and to consider a dispersed working arrangement, which includes home offices.

**Role of the banks**

**Banks’ capabilities**

If September 11th has taught us anything it is this: disaster recovery is a collective event. When a disaster of that magnitude strikes, banks must safeguard the flow of liquidity to ensure the survival of the economy. The banking community can succeed in doing what is necessary only if each participant stands ready to respond. That is why individual companies — and treasury groups within — besides enhancing their own disaster preparedness efforts, are also revisiting the contingency and recovery capabilities of banking providers and other critical business partners on which they rely for mission-critical operations.

So how did financial systems cope on September 11th? Processing of paper-based items such as cheques were delayed by the disruption to transportation, but with the value of cheques now minimal a more serious threat was the imbalance that arose between the cash and securities markets as liquidity was trapped by system failure. JPMorgan, which fortunately did not experience a significant outage to its mission-critical payments operation, took on additional volume that led to a record $1.939 trillion in U.S. dollar wire transfers cleared in a single day. Unprecedented efforts by bank staff limited the impact on...
the payments infrastructure, but the WTC attack undoubtedly exposed serious flaws.

Led by the Federal Reserve, many banks have already responded to the broader threat. In some cases, banks now have multiple processing centres in disparate geographical locations, typically with RTGS capabilities. But whilst the Fed and other regulators can play an important role, they can only force banks to a certain point. This is why the bank request for proposal (RFP) document is now seen as a crucial tool of business continuity.

**Evaluate your banks**

A comprehensive disaster recovery / business continuity evaluation must include regular review of banking providers and other crucial vendors and partners. Increasingly, clients want to understand the contingency plans of their banks in greater detail and participate in testing. (It has been JPMorgan’s longstanding policy to invite clients to participate in our contingency testing. Now we are receiving more calls from clients who want to be included.) Ongoing assessment should be part of the RFP and annual review process. Treasurers regularly measure their banks on how quickly they resolve the small percentage of payment errors.

Equally, banks should be judged on how well they are equipped to recover quickly and capably from a disaster. Not only are corporates asking banks to respond to operational risk questions in RFPs as a basic requirement, banks’ responses are being quizzed in detail by risk management experts. For example, banks are being asked to give evidence on the frequency of systems testing regimes and measures taken to fix weak links.

Price and service levels are still paramount to treasurers, but the new focus on operational risk questions in RFPs reflects a clear shift in purchasing behaviour. Now banks must explain what happens when a service cannot be supplied due to infrastructure failure and are being asked to walk treasurers through dummy transactions step-by-step to help identify potential risks.

Take electronic banking systems as an example of the potential pitfalls. Electronic banking interfaces are often customised so much by users that they can be extremely difficult to replicate in a disaster scenario. And if the system has multi-bank functionality, how will it be affected if one or more banks go down? For the financial infrastructure to survive a terror attack, all banks must be prepared. This realisation is forcing banks to work together more closely.

**Conclusions**

The future of disaster preparedness is one of enhanced collaboration among financial institutions and more active participation by clients in understanding and testing contingency plans with banking providers. Financial institutions and companies alike are enhancing their flexibility for dealing with a broader range of potential scenarios. Banks are taking the lead in collectively discussing vital issues and enhancing a coordinated response.

In times of need, corporates should be able to look to their banks with confidence. Whilst the range of services offered to wholesale and retail customers continues to change, ‘trust’ is a quality that has historically lent a sense of continuity to banks’ other activities. Since the very first, banks have always provided a place of safe keeping for customers’ funds; there is no reason this should change in the future.

9 January 2003
Ms. McLaughlin-Moore is Senior Vice President at J.P. MorganChase Bank and responsible for Treasury Services Global Clearing business. Linda joined Chase in 1984 and has held numerous management, strategy and operations positions during her tenure. Linda’s experience with Chase includes the development and management of the global market strategy and business architecture function in support of Treasury Services growth in the new economy. She has been a keynote speaker at EuroFinance Conferences and EIU’s Risk Management Conferences. She has published articles in a broad array of periodicals. She also served as a content expert to several Doctoral Programs in the specialties of international payments, treasury management structures and the evolution of EDI.

J.P. Morgan Chase & Co. is a premier global financial services firm with assets of $714 billion and operations in over 60 countries. The firm is a leader in investment banking, asset management, private equity, consumer banking, private banking, e-finance, and custody and processing services. Headquartered in New York, J.P. Morgan Chase serves 32 million consumer customers and over 5,000 corporate, institutional, and government clients.

To achieve this, JPMorgan Treasury Services is a global leader in providing cash management, clearing, trade finance, liquidity, information and web-enabled solutions. We enjoy a position as trusted advisor to our key clients, deploying our intellectual capital to meet their particular needs. We provide world-class end-to-end solutions that enable corporates and financial institutions to maximise their cash efficiency.

Treasury Services, formerly Chase Treasury Solutions, is proud of its history in cash and treasury processing. We take a partnership approach to ensure that clients receive comprehensive support and technical assistance, from solutions design to product implementation. We are determined to offer the best solutions, delivered in the most efficient way - from exploring the possibilities of the internet to optimising working capital to enable corporations to utilise liquidity investment vehicles.

This article first appeared in www.gtnews.com, the number one global information resource for finance and treasury professionals. Updated weekly, GTNews provides informed commentary, news and analysis from hundreds of key players throughout the finance and treasury sector. Topics covered include banking, risk, cash management, working capital, outsourcing, capital markets, online trading, and systems. GTNews also features surveys, job listings, directories, guides, news, ratings, Q&A forums & events diaries. GTNews is FREE to read so register today at www.gtnews.com.