

Business Continuity: How Resilient is Your Company?



Exceed Together

There is an assumption within the financial services industry that procuring telecommunications services from multiple providers ensures the separation of circuits required to ensure business

continuity. This, however, is not necessarily true. What resilience measures should financial institutions have in place to ensure business continuity?

The financial services industry has never before relied so heavily on the technical infrastructure that underpins its daily operations. Over the last five years, financial institutions have spent trillions of dollars further strengthening this 'plumbing' through sophisticated disaster recovery and business continuity planning strategies. Regulation has not taken long to catch up and numerous best practice guidelines and directives have been published to ensure ongoing stability of the financial markets.

Despite the increasing profile of resilience and ensuing expenditure, it is argued that the European financial sector is still plagued by multiple single points-of-failure, which even firms with advanced procedures may not be aware of.

The devil's advocate would say that financial institutions with sub-standard business continuity plans know who they are. The business community has had enough opportunity to test and refine these procedures since 9/11 in the US, in addition to both simulation exercises and real-life events. Many financial institutions have recently complemented this by drawing up business contingency plans to deal with the possibility of high levels of absenteeism in the event of a widespread outbreak of bird flu. But while the largest financial institutions have highly resilient IT systems that could recover critical functions quickly after a terrorist attack or natural disaster, there is worrying evidence which suggests that even financial institutions with complex and well-rehearsed disaster recovery plans in place are still very much at risk from infrastructure outages.

What is Separacy and Diversity?

Separacy refers to the actual physical separation of circuits, ensuring that no common paths or components are used end-to-end. This covers cable paths, exchanges and interconnection points.

Diversity refers to alternative routes in the event of an outage or service issue. Previous surveys have highlighted a number of financial institutions that are receiving diversity while under the impression that they have separacy, which is still a common occurrence.

Does a Dual Supplier Really Provide Diversity?

There are various recommendation papers in circulation promoting the benefits of resilient network architecture using dual providers and separate routes. The consolidation of the European telecommunications sector from approximately 4,000 firms in 1999 to about 400, coupled with the high profile demise of Global Crossing and WorldCom has made financial firms weary of reliance on a single supplier. A prime example of this occurred back in 2001 when SWIFT backed out of a single contact with Global Crossing to supply its global IP network and instead chose four network partners to carry the world's secure financial messaging.

The premise of dual-supplier resilience is starting to wear thin. While banks diligently place orders with separate carriers and ensure that points of entry to their facilities are separate, in many cases the diverse lines will loop round and then follow the same duct to their destination. To illustrate this point, next time you walk out of your office to get a triple espresso, take a note of the manhole covers along the street, which usually display their owners' names on the top. The likelihood is that you will pass multiple carriers along the same route, after all, telecom companies dig up the same roads and can share the same ducts. It is even likely that the carriers use the same contractors for the digging and laying of cable.

The implication for financial firms is that these are the same circuits providing the firm with inter-office connectivity, disaster recovery replication and data archival, market data, trading/order flow, e-mail and Internet access. In short, diverse carriers do not necessarily lead to diverse paths.



Business Continuity: How Resilient is Your Company?



Exceed Together

NISCC Good Practice

The National Infrastructure Security Co-ordination Centre (NISCC) raised awareness of these issues back in 2004 when it published the Good Practice Guide for Telecommunications Resilience. This report stressed the need for financial firms to take appropriate measures to ensure that their telecommunications systems were robust enough to continue provision of critical services in the event of any disruption.

Although network providers have on the whole invested heavily in their network backbone, ensuring full resilience and capacity, the last mile (the connection between the provider exchange and client site) is often overlooked and is the source of many single points of failure. Major 'high-density' city centres were outlined as being at risk of congestion between customer premises and local exchange or point of presence (POP).

While the 'unbundling' of the local loop has opened up the market for third parties to provide services over the last mile, there is no mandate for either provider or incumbent to discuss the intended use of these circuits with the other. As a result, either or both firms may be oblivious to the fact that the customer requires separacy of circuits.

Resilience has been improved through wide-scale usage of ring topologies by telecoms providers, which enable diverse paths in the event of a break in the connection. Although highly resilient synchronous digital hierarchy (SDH) ring topology is provided as standard in most major cities, single points of failure have still been highlighted at the point of entry to each site.

It has since been argued that the extensive adoption of dual provider relationships has lulled the financial services industry into a false sense of security and that, in reality, true separacy would be achievable by asking a single infrastructure provider for two separate circuits, albeit returning to single-supplier dependency.

Challenges

Today, many firms audit their connectivity to ensure that separate paths are suitably separate. This is a particularly labour intensive activity, especially as the onus is on the end customer to collate data from multiple providers. This is also a reactive measure; after all, an audit will only identify a loss of diversity after it has happened. Following this upfront cost and effort, firms may be dismayed to

find out that telecommunications providers are free to alter connection routes and third party contracts at any time, so firms have no guarantee that a successful audit from a few months ago still applies.

No system currently exists for multi-carrier provisioning of diverse circuits, which again places the responsibility on the end customer to manage routing. This activity is clearly not a financial firms' core competence and can represent a significant overhead to their business.

This area has recently been under further scrutiny from the Tripartite Authorities (HM Treasury, the FSA and the Bank of England) who published the results of a survey of the UK financial sector's ability to cope with major operational disruption in December 2005. The authorities found that on the whole progress was good, although again called for firms to collaborate with infrastructure providers to enable more co-ordinated risk mitigation. The survey highlighted the reliance on key telecommunications providers and the dangers of geographical concentration of critical business functions and back-up sites in London. Evidently some work is yet to be done in order to supply the market with a fully resilient model.

Lessons from the US

It is clear that in many respects the financial sector has been burying its head in the sand when it comes to resilience. It is also evident that a large amount of the regulation does not sufficiently tackle the real issues.

The financial sector in the US has already dealt with this issue for mission-critical traffic. The Securities Industry Automation Corporation (SIAC) was fast to react to 9/11 with the realisation that the multi-carrier system did not actually provide full resilience for stock exchange trading and market data.

By forming the Secure Financial Transaction Infrastructure (SFTI) in 2001, SIAC created a dedicated, separate resilient backbone for access to trading and market data from US exchanges. Not only is this a gateway to all of the major US exchanges (including NYSE, NASDAQ, ISE, US, Philadelphia and Boston Stock Exchanges) and electronic communication networks (e.g. ARCA, BRUT, Instinet and BRASS), SFTI has also seen an expansion in utility providers using the network hoping to leverage the mission-critical access, for example, the DTCC and more recently SWIFT access.



Business Continuity: How Resilient is Your Company?



Exceed Together

Connectivity via SFTI has alleviated firms from the audit burden of continually proving separacy, although covers only a subset of critical financial traffic, leaving other areas of the business exposed to traditional weaknesses.

Europe does not yet have a SFTI equivalent at present, although there is increasing pressure from the financial sector to provide one. Having said this, critical data does not simply amount to exchange trading - of equal concern could be the liquidity crisis that could be created by an outage of a high-value clearing and settlement network, or the risk arising from an outage of a key outsource service provider.

Ensuring Compliance

If they are to fully comply with national and European regulations regarding resilience (for example, operational risk outlined in the Basel II Accord) then financial firms will need to take a holistic view of the data flows and the underlying infrastructure. Firms will then need to face up to the reality that the multi-provider model does not assure separate circuits and undertake a connectivity audit to gain assurance that it is not exposed. Once the institution is satisfied with the current situation, steps need to be taken to ensure that paths do not change in the future. At the very least, the institution should gain a clear understanding of the relationship between its contracting parties.

Industry suppliers also have a significant role to play in contributing to the stability of the financial markets, both through participation in best-practice groups, such as ISC2, ISAC and NISCC, and ensuring compliance with established industry standards (ISO 27001 is a good example). The regulatory shift in considering outsourced providers as logical extensions to the financial institutions themselves represents a challenge which infrastructure and managed service providers must rise to and work in partnership with their clients to demonstrate compliance.

Conclusion

The industry assumption that a resilient communication infrastructure is a commodity item is incorrect. There is a cost associated with providing and proving network separacy, and the ongoing costs to ensure this. Taking this into account, firms should take stock of their communications infrastructure and identify the services requiring mission critical levels of service. This is certainly not a 'one size fits all' model for the future.

