

# I D C T O P L I N E

## Balancing DIY and Managed Network Services: Blueprint for Financial Services Success

March 2010

by Sherlin Pang and Adrian Dominic Ho

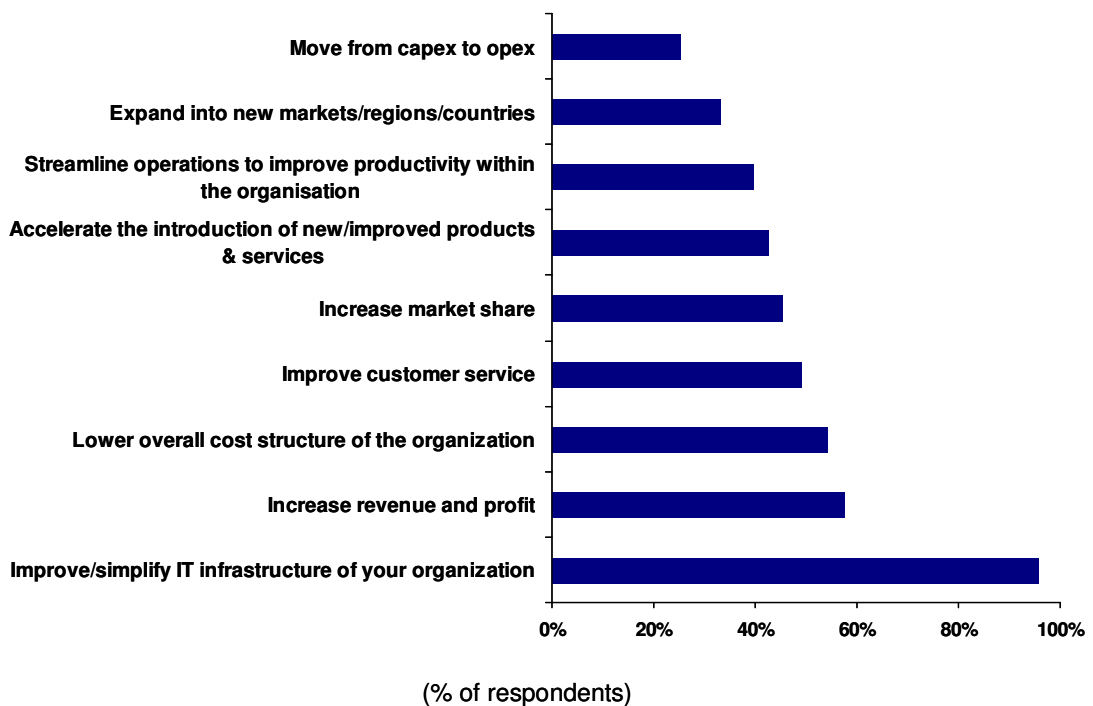
Sponsored by Telstra International

Since 2008, authorities across the globe have imposed tougher regulations over financial institutions to avoid a repeat of the worst financial crisis since the Great Depression. Throughout 2009, the financial sector likewise focused on putting their house in order by further streamlining their operations such as tightening processes and gaining efficiencies. With a market recovery underway in 2010, financial services firms plan to focus on increasing revenue by accelerating the introduction of new products and services, entering new markets, and improving customer service (such as offering 24/7 online and mobile banking services), as found in IDC's *Managed Services Survey* (see Figure 1).

**FIGURE 1**

### Financial Institutions' Corporate Goals Over the Next 12 Months

Q. What are your immediate corporate goals over the next 12 months given the economic climate?



N=181 (multiple responses allowed)

Source: IDC's *Managed Services Survey*, April 2009

Financial institutions will need to reexamine their ICT infrastructure capabilities and find ways to effectively manage the network to meet these business requirements and the increased bandwidth demands. Firms leveraging new applications, such as collaborative tools (e.g., Web/audio/videoconferencing and telepresence), and cloud services to transform their business operations should also realize that building more applications on top of the network adds to the complexity. Indeed, network resiliency is vital as networks become more complex and sophisticated. Financial institutions will need to tap a larger pool of IT expertise to manage all that technology, and gain a better understanding of their impact on the network so that they do not run into latency or unavailability issues. One solution to ease the IT labor crunch is managed network services (MNS).

## Why Use Managed Network Services?

Network resiliency and performance is critical, especially with a higher adoption of bandwidth-intensive collaboration tools and cloud services. Any downtime in the network can result in millions of dollars lost in transactions, decrease productivity and negatively affect the firm's reputation. To ensure network resiliency and performance, financial institutions have a choice to either manage the network in-house or out-task the management to MNS providers. There are definite advantages in choosing the latter:

- **The "collaborative global headquarters"**: As financial institutions expand their market and regional footprint, effective communication between the headquarters (HQ) and the regional offices becomes increasingly important. The HQ should leverage collaborative tools such as telepresence, high-definition videoconferencing or unified communication services to reduce traveling costs, launch new products faster, ensure regional sales staff receive timely and accurate product training as well as obtain feedback for product development or enhancement. As the HQ and branch offices adopt these tools which also sit on top of the networks, networks become more critical than ever. This requires IT managers to have a good understanding of how these applications work, and their impact on their networks in order to ensure high network resiliency and performance. MNS with a wide technology portfolio and experience in managing these network-based applications can help to design and migrate legacy systems to a next-generation network that meets future business needs.
- **Ensuring business continuity**: With IT infrastructure simplification a key priority in the next 12 months, financial institutions will seek ways to free up IT infrastructure investments by moving applications into the "cloud" and increasing their virtualization adoption. This means network security becomes ever more important to ensure business continuity. Financial institutions can leverage MNS to simplify IT and build a well-connected workforce without compromising on network performance and business continuity. MNS providers offering up-to-date online management tools with security features are able to ensure good network performance and deliver on expectations outlined in the service level agreement (SLA).
- **Reduce opex**: Financial institutions that manage their networks in-house require a dedicated IT team to continually monitor their network utilization and take care of the day-to-day operations. Ongoing training is essential for them to keep up with the latest technologies, accreditation standards and security threats. However, an experienced IT professional is costly to hire. In contrast, financial institutions that opt for managed services will be able to leverage the expertise and resources of MNS providers. Besides undertaking the day-to-day operations, maintenance and upgrades of the network, the MNS provider also provides proactive monitoring to ensure high network availability and performance.
- **Reduce capex and network investment risk**: With fewer IT and network operation staff to hire, financial institutions can release IT office space for other usage. Financial institutions also do not need to maintain and invest in costly network management systems, negating the need for upfront investment. MNS providers enjoy economies of scales and are therefore able to maintain up-to-date network management and ensure high performance. MNS also makes IT costs more predictable. Financial institutions need only to pay a monthly fee to the MNS provider for the maintenance of their network, which enables them to move their cost structure from a capex to an opex model, which is more predictable and easier to manage.

- **Single point of accountability:** In a DIY model, IT managers have to engage in multiple networks, technologies and third-party contracts. In MNS, besides leveraging the provider's expertise in managing networks, it offers an added advantage of a single point of accountability for network utilization and upgrades. Besides being responsible for the day-to-day maintenance and operations, MNS providers can also provide configuration management, hardware and software maintenance and repair, advice on end-of-life equipment replacement, and network design consultancy. In the MNS approach, the IT manager has only "one neck to choke" since the MNS provider is responsible for engaging with the network technologies providers and router vendors.
- **Better control over the network through a robust SLA:** One main concern of financial institutions is the potential loss of control over critical business operations. Unlike outsourcing where the entire business function is handled by a third party, in out-tasking, the financial institution can choose to out-task the management of the network and day-to-day operations to the degree of their comfort. A well-defined and robust SLA by the MNS provider, good network performance tracking and reporting systems can actually increase the financial institution's control over their critical operations.
- **Minimize threats to data loss and maintain network security:** The other concern for financial institutions is data security and network unavailability. MNS providers can install firewalls and intrusion detection systems (IDS) and use encryption to ensure sensitive data is secured during transmission. The MNS provider is expected to stay ahead of any security threats and provide proactive monitoring and alerts on the network to ensure high network availability and performance. A MNS provider that has a good understanding of the financial sector will also ensure that the organization's network meets all regulatory demands and security guidelines.

## Essential Guidance

IDC believes that financial institutions should leverage MNS to help manage complex networks and, in turn, lower operational costs and release limited resources for more revenue-generating operations. MNS should be more "all encompassing", providing an end-to-end solution that help financial institutions leverage network-based applications to improve overall productivity and realize higher cost savings.

When selecting a MNS provider, financial institutions should examine the SLA of the managed service contract, ensuring it covers key aspects such as network availability, fault management and restoration, level of operations support, network performance reporting process, disaster recovery, and backup. The MNS provider should be flexible with the SLA and its solutions to meet the financial institution's needs for future expansion and business demands.

As data security and high network resiliency are important, and even more critical now with the adoption of collaboration tools, social media and cloud services, the MNS provider must be able to ensure that the network is fully secured. This is especially important for critical applications and for the financial institution to respond to downtime in the shortest time. The provider must be well-versed in the financial industry's mandatory regulations and security standards to ensure the network infrastructure meets regulatory requirements on network availability and performance.

The MNS provider should also have wide knowledge of different network technologies and network-based applications, and have extensive network coverage. A good understanding of how network-based applications work and their impact on the networks, as well as having a broad range of access technologies will ensure that the financial institution has accessibility to best-of-breed technologies that can meet their future demands. As financial institutions grow their market footprint in the region, they should ensure that the MNS provider has the network coverage in these regions and be able to provide end-to-end visibility and restoration of the whole network.