



Network Cost of Ownership:
Benefits of Vendor Standardization
Financial Sector Case Studies

August 2003

220 North Main Street, Suite 203
Natick, MA 01760
508.655.5400
www.sageresearch.com

Case Studies

To expand on the findings of the enterprise survey, Sage Research conducted 10 in-depth phone interviews with select survey respondents. All 10 interviewees had already qualified for and completed the survey. Sage selected two interviewees from each of five industry verticals:

- 1) Finance
- 2) Healthcare
- 3) Manufacturing
- 4) Public Sector
- 5) Retail

Within each of these verticals, Sage recruited one participant that had a “Primary Vendor” network environment and another that had a “Multi-vendor” network. Beyond these specifications, Sage attempted to recruit IT executives from companies that have already deployed several advanced technologies on their core network. The primary objective of these case studies is to demonstrate different companies’ experiences deploying advanced technologies onto their core network using different approaches to network evolution.

Financial Case Study #1 (Primary Vendor)

Background and Network Approach

A large U.S. bank (approximately 130,000 employees) made an executive decision approximately five years ago to standardize on Cisco as their primary vendor whenever feasible. Prior to this decision, they had a much more heterogeneous network environment with decentralized decision-making authority for network purchases. The main data center would provide general guidelines, but each division of the bank managed its own IT staff and purchased equipment locally largely without regard to what other divisions were using. Network integration and management became increasingly difficult as the pace of mergers and acquisitions in the financial industry accelerated.

Exhibit 1: Financial Case Study #1 Snapshot

Industry Vertical	Finance
Company Size	Approximately 130,000 employees
Network Strategy	Primary vendor network (standardize on Cisco)
Top Benefits	<p>Manageability, integration, IT staff training, support, scalability, faster deployment at new sites:</p> <ul style="list-style-type: none"> • Annual savings of \$400,000 per year on IT staff training • Saves five weeks of time when installing an IP PBX system at new sites compared with previous PBX • Less than 10 hours of unscheduled downtime in any part of their network during the last 12 months • Spare parts obtained in 1-2 hours, on average • Saves 80 man-hours, on average, in integration time when deploying new equipment on the network
Current Concerns	Limited choice for new technologies; less flexibility to try different vendors for a given technology deployment

Key Findings

The main reasons for choosing Cisco as the standard networking vendor were its products' reliability, scalability, security, and performance. Additionally, the bank was looking for a vendor with financial stability, market share leadership, and strong technical support. The bank did *not* choose Cisco because of price savings. Although there is a certain amount of bargaining power gained by using bulk contracts, the bank's IT department was more concerned with the performance of the products and the after-sales support they would receive than with any bulk buying discounts. The top priority of the IT department is to minimize downtime. They were not interested in going with the lowest cost equipment if it would negatively impact opex spending, network efficiency, reliability, or customer service.

By taking a "preferred vendor" approach to its network evolution, the bank has realized multiple benefits in the past five years:

- (1) Increased manageability: The routers, LAN switches, IP PBX, wireless LAN, and security elements from Cisco all have common management interfaces based on the IOS software platform. This commonality enables the IT staff to spend less time managing and monitoring the network across different technologies and network elements than it would be with a variety of different vendors.
- (2) Less training time and expense: By standardizing on Cisco, the bank spends much less money sending IT staff to off-site training seminars for different equipment vendors. First, the bank benefits by not having to train IT staff on multiple vendor technologies. Second, it benefits from Cisco sending technical staff to the bank for on-site training sessions, which is only possible because of Cisco's size and because the bank purchases in bulk from Cisco. Cisco's wealth of online training resources helps minimize the time that IT staff must spend going off-site for training. The bank estimates that they would be spending approximately \$5,000 per IT staff member per year on training using a multi-vendor approach to the network and relying primarily on off-site training. By standardizing on Cisco and taking advantage of Cisco's on-site training offers, it spends approximately \$3,000 per IT staff member per year on training. They have approximately 200 engineers on their IT staff that require constant training and certification, resulting in an *annual savings of roughly \$400,000 per year company-wide*. Standardizing on a primary network vendor also reduces the time necessary to train new IT staff members on its network. It typically takes a new employee 3-4 weeks to be fully competent in their tasks. If they needed to understand different vendor equipment within or across technology categories, this time would increase accordingly.

- (3) Superior technical support: Cisco has support engineers dedicated exclusively to the bank's account. This level of support is only possible because of the scope of the bank's relationship with Cisco and the support infrastructure that Cisco has to offer because of its large size. This results in faster time to discover the source of a problem when it occurs and to resolve it. *The bank's typical time to resolution for a trouble-ticket is less than one hour.*
- (4) Less unscheduled downtime: The bank reports that both the frequency of unscheduled downtime events and the mean time to repair have improved since they standardized their network on a single vendor. *In the past 12 months, across the entire network, the bank has only experienced 10 hours of unscheduled downtime that affected any given part of the network.* Given that the IT division offers SLAs to its internal clients (i.e., the other business divisions), this is an absolutely crucial benefit of standardizing on a primary networking vendor. "We have better control, and the vendor has very good knowledge of its full product line," the IT Director reports. Having a common network vendor has also done away with the finger pointing between different vendors when trouble-shooting was necessary. The most painful thing, the IT Director reports, was when they wanted to install a patch. Getting one-off vendors to help install and configure the patch and make sure it integrated with the rest of the network could be a very frustrating experience. Finally, the mean time to repair for those rare occasions when there *are* actually downtime events has fallen drastically since standardizing on a single vendor. Because spare parts are much easier to manage in a primary vendor network than in a multi-vendor network, the bank reports that—on average—*they can get spare parts within 1-2 hours.* This significantly reduces the IT staff's time spent on trouble-shooting and allows them to focus on more productive tasks.
- (5) Product integration: Having common interfaces across technology categories has facilitated the process of integrating the various network elements together. It has also enabled the company to integrate disparate business divisions into a common network with access to pan-enterprise applications. This cuts the staff time down considerably when deploying new equipment in the network. *For each new project, from planning to implementation, the IT Director estimates that they save a total of two weeks (80 staff-hours) in integration time by standardizing on a primary network vendor.* It also allows them to rely less on outside consultants and system integrators for new deployments. *Most of their network projects can now be done in-house, which saves the company approximately \$1 million annually in their budget for outside services.*

- (6) Adding new technologies to the core network: Since the bank standardized on a single vendor, adding new, emerging technologies onto the core network has been easier than it would have been with a “best-of-breed” approach.

Adding New Technologies to the Core Network

VPN

The bank began realizing a true pay-off from standardizing on a primary vendor when it started to add new technologies to its core network. One of the first “new” technologies the bank added on to its core network with its primary vendor was VPN. The VPN network for both wired and wireless networking has proved easily scalable as it has grown over the years. Using a preferred networking vendor enables a much more seamless integration of VPN gateways with the rest of the LAN infrastructure at a new site location. It has also made it much easier to manage user authentication centrally (PKI) across the entire VPN network.

Firewalls

In addition to Cisco VPN infrastructure, the bank standardizes its firewall infrastructure on Cisco PIX. While the company chose Cisco PIX primarily because of its features, the bank has also benefited from having the same interface for its firewalls as for its routers, switches, and other networking elements. This makes the deployment of firewalls to new site locations much faster than it would be with any other vendor, and it also reduces the complexity of managing the firewall infrastructure. Cisco PIX also integrates well with Microsoft applications such as MS Exchange and MQ Series, so it’s easy to establish firewalls between the bank’s external vendors and its internal corporate network to enable extranets.

IP PBX

The next major evolution of the corporate network was to deploy an IP PBX system. Once again, the bank used its primary networking vendor for this project. It deployed Cisco IP PBX systems approximately two years ago, and currently has roughly 20,000 users on the system (15% of their total employee base) at both the central headquarters and the divisional units. *The single most important factor in selecting its primary network vendor for IP PBX was the ease of integrating the system with the rest of the existing network.* One of the integrated applications the bank was able to deploy with the new IP PBX system was co-browsing with real-time phone conversations for the call centers. Customer service representatives can co-browse the company’s web resources with customers when they call in for support. In addition to the co-browsing, the bank’s new IP PBX system has allowed them to link ATM machines back to their call center.

The new system also takes less effort and time to deploy to new sites than the old PBX did. With all of the mergers, acquisitions, and consolidations, the bank finds itself relocating and adding locations fairly frequently. Much of the advantage of installing new sites is inherent in IP PBX technology, regardless of the vendor. The fact that the bank used its preferred networking vendor, however, further reduces the time necessary to install, configure, and integrate the system with the rest of the IT network. *On average, the company estimates that they save approximately 5 weeks of time when installing the system for new site locations compared to the PBX system they were using previously.* Now, the company realizes the time savings by using a single team of engineers (either a consulting firm or internal staff) for the whole deployment rather than a hodgepodge of consultants for different elements of the voice and data network. “It gets easier each time we set up a new network,” according to the IT Director. “[Cisco] has a very streamlined implementation plan now. Everything is well documented, and the interfaces to other network elements are all standardized.”

Conclusion

While the bank acknowledges that it hasn't saved on hardware costs alone by standardizing on Cisco, the benefits in terms of manageability, integration, IT staff training, ease of monitoring, and scalability have reduced the bank's total network cost of ownership considerably. The benefits of this standardization have accumulated and grown as the bank has expanded its network geographically, merged with other banks, and added on new network technologies to the network core.

Financial Case Study #2 (Multi-vendor)

Background and Network Approach

A large financial services company headquartered in the southeast has traditionally taken a “best-of-breed” approach to its enterprise network with a decentralized IT and networking procurement process. This approach was partly a legacy of growing through mergers and acquisitions, but it also afforded each office the flexibility to choose the system that best met its particular needs. As the company started to consolidate site locations, however, it has found that its decentralized approach has made it very difficult and very costly to integrate the disparate systems in place across its network. As the organization’s IT Director puts it, “What’s best for the Toronto office and what’s best for the London office might not be the same thing, and so over time you have a hodgepodge of different technologies that you’re later forced to rationalize through costly integration projects.”

Exhibit 2: Financial Case Study #2 Snapshot

Industry Vertical	Finance
Company Size	Over 5,000 employees
Network Strategy	Decentralized decision-making authority for networking purchases; “best-of-breed” approach to emerging technologies
Top Benefits	Flexibility: ability to select equipment that best meets functionality requirements for each situation
Current Concerns	<p>Too much money spent on individual annual maintenance contracts; costly integration projects now that the company is consolidating site locations; no-economies-of scale in IT staff training and certification.</p> <ul style="list-style-type: none"> • Spends \$850,000 per year in maintenance contracts (\$60/employee) • Spends over \$2 million per year on “outside services,” much of which is integration consulting • The internal IT staff spends 25% of its time on “change management” associated with integration projects (equivalent of \$470,000 in salary) • Spends \$220,000 per year on IT staff training

Key Findings

By taking a “best-of-breed” approach to its network evolution, the company has realized multiple **benefits**:

- (1) Flexibility: The main benefit the best-of-breed approach has afforded the company is flexibility. Each office is unconstrained by corporate-wide policies or “approved vendor lists” when selecting a solution that best meets their needs and fits their priorities.
- (2) Up-front equipment costs: In certain situations, having multiple vendors bid for a project can result in lower up-front capital costs for equipment. On the other hand, the IT director says that their company does not take nearly enough advantage of its buying power that it could be leveraging by purchasing in bulk from a preferred vendor:

Conversely, the IT staff acknowledges several **sources of pain** associated with taking a best-of-breed approach:

- (1) Costly maintenance contracts: The company pays much more than necessary every year in maintenance contracts because of the multiplicity of vendors it uses at various site locations. *It pays over \$850,000 every year in maintenance contracts* (approximately \$60/employee/year), but expects to reduce this significantly as it consolidates to a primary vendor network with global agreements.
- (2) Integration difficulties: Now that the company is consolidating, it has found integrating the various components of the existing network extremely difficult and costly. Part of the response to this has been to outsource significant portions of their network under global contracts with service providers. For instance, the company has now switched to an AT&T managed network service that will go across all of their sites using standard WAN connectivity infrastructure from common vendors. For its VPN networks, similarly, it is moving to a global managed service from iPass to replace the site-by-site, piecemeal approach to remote VPN access that they have in place currently. The integration projects and the outsourcing have significant impacts on the company’s operational expenditures (opex). *They spend \$2.125 million annually (25% of their total networking budget; \$142/employee/year), on “outside services,” which includes outsourcing and consultants.* This is quite separate from all the staff time the company spends on “change management.” *The IT staff of the company is spending 25% of its time managing change during the current fiscal year, which equates to nearly \$470,000 per year in IT staff salary.*

- (3) Fragmented network management: With each office location selecting and managing its own networking equipment, there has been virtually no centralized control over the global network. Even documenting the systems that each office location runs has proved challenging. According to the IT Director, “We’ve operated as separate organizations within the company umbrella for quite some time, which means we have no central repository with documentation as to which systems everyone is running.” Before, when they operated in a decentralized mode, this was not a serious problem. Now that they are consolidating their offices and business units, however, it has involved significant network staff time.
- (4) Inefficiencies in staff training and certification: With each office running its own networking gear, there must be trained employees at each location that can support this equipment. The training and certification that IT staff receive in the corporate headquarters cannot necessarily be applied across the global network because of the variety of systems that are in place. *Overall, the company spends approximately \$220,000 per year on IT staff training (\$15/employee on a company-wide level, including non-IT and IT staff), and this does not include the time and training costs that individual offices incur by having local non-IT staff ready to provide a minimum level of support to the local network.*

Adding New Technologies to the Core Network

IP PBX

The companies’ traditional approach to network development has had significant impacts as it adds new, emerging technologies onto the core network. For instance, the Toronto office deployed a 500-phone IP-enabled PBX system from Avaya in 2002, with the first live traffic running on it in January 2003. They added on the IP-enabled PBX to their traditional Lucent PBX, which helped keep the project on time (three months to deploy) and on budget (\$500,000).

While the Toronto office has been very happy with the deployment, it is not integrated at all with their global WAN, which primarily runs on Cisco equipment. The company as a whole is conducting a more in-depth review before deciding which system to standardize on for a global IP PBX system.

VPN

The company’s VPN network also grew out of local initiatives. Virtually every office has remote-access VPNs for their local staff, but the systems and the software used vary widely by office. The total amount of staff-time spent on supporting these systems remotely was extremely high, and the arrangement did not facilitate staff moving between offices seamlessly. As a result, the organization is in the process of moving to a managed iPass system for VPNs around the globe. It is currently deployed in their

London office, and they are moving to consolidate all offices under this managed service. Once this is complete, they will be able to manage and support all employees that use the VPN centrally, and they will have traffic management and QoS capabilities across the network.

Firewalls

The company has already standardized their firewall hardware on the Check Point brand, but currently they have no centralized management of their firewalls across the entire network. The result of this has been inefficiency in staff training and support. Most of the people at these site locations aren't Check Point certified, and they don't have the expertise necessary to secure the site properly, according to the IT Director. By moving towards centralized management of these systems, the company expects that the whole security apparatus will be much more stable and secure because qualified IT staff will be able to support all offices remotely from the main data center.

IDS

With Intrusion Detection Systems (IDS), the company is currently working with a variety of different brands. As with the firewalls, they are evaluating different vendors now with the goal of standardizing their IDS infrastructure on a single vendor platform globally. The main reason for doing is to have properly certified people with extensive product knowledge that can handle all of the issues that arise in an IDS system. It is neither economical nor efficient to have local staff doing this for different systems at each site location.

Conclusion

The company's traditionally decentralized approach to network planning has led to a variety of problems that it is now addressing. The main issues with the decentralized approach are high exposure to maintenance contract expenses, costly integration projects when different office locations consolidate, fragmented network management, and inefficiencies in IT staff training and support. The company has already standardized on Cisco for its core network (routers and switches) and Check Point for its firewalls, but it is looking to consolidate down to one vendor in each product category and, to the extent possible, maintain a primary vendor across different product categories.

"Best-of-breed means different things to different people, so you end up with a lot of disparate systems," the IT Director of the company explains. "We're going to a consolidated mode to save operating expenses." The company also expects to realize some gains on the capital expenditure (capex) side of the budget through bulk contract discounts.