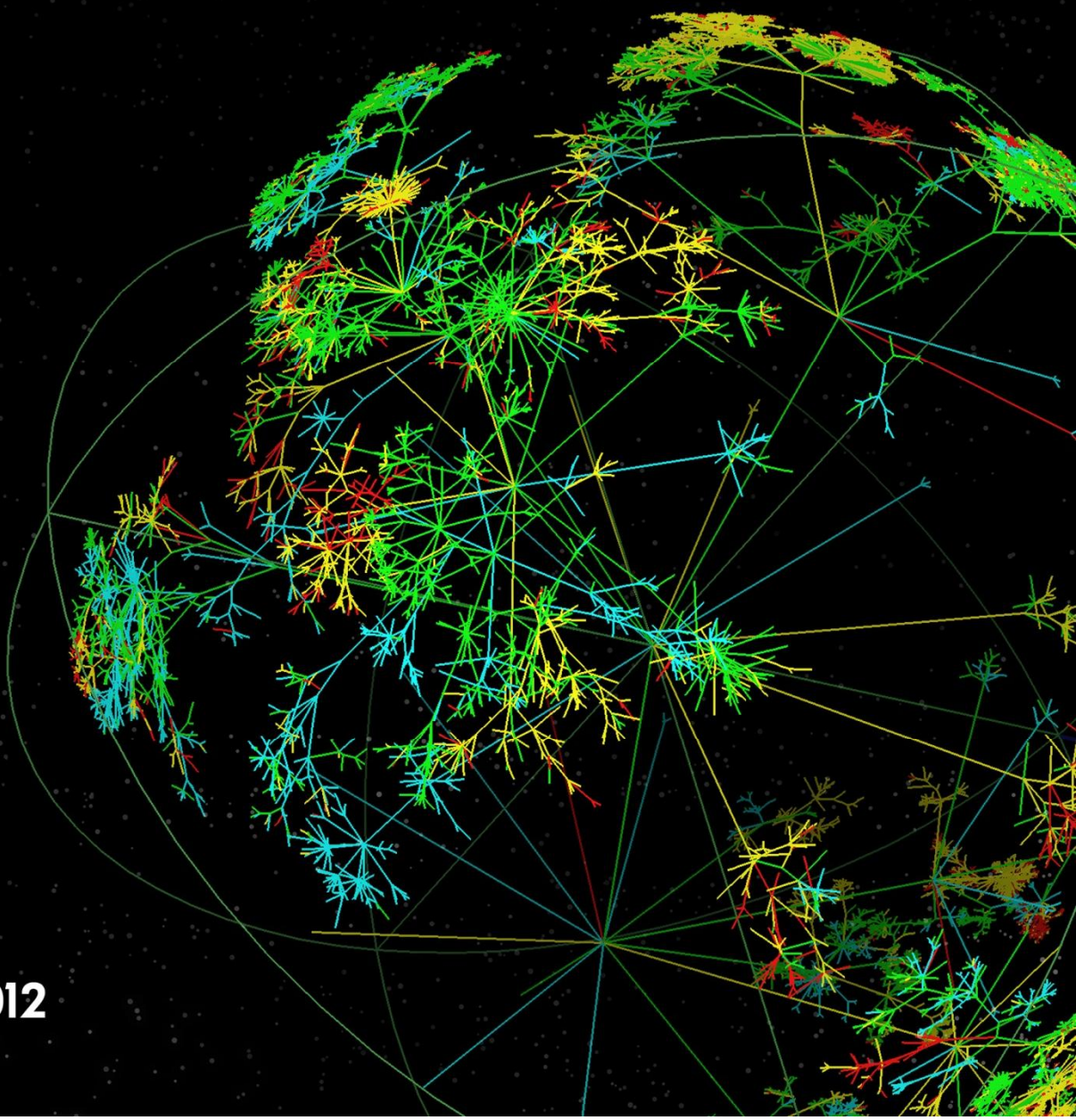
Deloitte.

MULTIVENDOR NETWORK ARCHITECTURES, TCO AND OPERATIONAL RISK



February 2012

Contents

1. Executive summary

Enterprises face increasingly complex choices in their network vendor strategies. IT leaders must introduce new technology for critical business functions, while managing IT costs and balancing operational risks.

This report summarizes the findings from a detailed customer survey conducted by Deloitte to examine the operational, financial, and risk factors associated with the use of single vendor and multivendor approaches in different types of enterprise networks. By providing a framework for understanding the overall value drivers associated with these networking strategies, this report is intended to help IT decision makers evaluate the potential impact of different approaches.

Through this survey, we examined how network vendor strategies align with important sources of business value, such as network performance and reliability, as well as operational functionality, maintainability, extensibility, security, interoperability, and risk. The survey results are based on a set of detailed interviews with customers currently using Cisco products along with other vendors' products in their networks.

Our customer survey provided the following key findings:

1. Within the context of total IT spending, the *use of single-vendor or multivendor architectures does not present material cost differences on a long-term basis.* Initial cost savings realized in multivendor network implementations are mitigated by the incremental operating costs over the life of the equipment.
2. Enterprise networks are considered critical production systems, key to business operations. *Networks must be managed with an appropriate operational risk perspective*.
3. *Customers prefer a single vendor to be responsible for all network components and services*. The operational risk associated with network support, not the cost, is the primary factor when influencing the decisions to use single or multivendor architectures.
4. *Staffing costs are not significantly impacted* by the use of multiple vendors; it is more influenced by the mix of functions supported and the types of network services provided.
5. Using products from different vendors can bring down initial costs for certain products, but *adds higher operating risk in service, support, and operational integration.*
6. The *use of multiple networking vendors introduces additional operational risk* based on the need for customers to assume *increased risks for integration, interoperability and support*.
7. When using multiple vendors' products*, customers frequently do not recognize the interdependencies of functionality, long-term costs, and impact on operational risks*.

The details of our findings are described in the following sections.

2. Survey methodology

Deloitte surveyed a representative sample of enterprises with different complex network architectures to gather data for this report. Functional, operational, and financial data were collected to assess the cost, performance, and risk factors associated with single or multivendor implementations. Enterprises were selected based on their network structures, complexity, and site distribution, with a mix of organization types represented.

The following criteria were used to identify the organizations for participation in the survey.

- Size of network based on user ports:
  - A sampling of organizations with a network size between 1,000–2,000 end users,
  - A majority of organizations with a network between 2,000–10,000 end users, and
  - A sampling of organizations contained 20,000 or more end users.
- Distribution of network sites:
  - Most organizations were considered ‘large’, with a three-tier network, multiple distribution sites, and more than 30 remote sites.
  - Some organizations were considered ‘small’, with a more basic network, a single distribution, and less than five remote sites.
- Network services and diversity:
  - Organizations were selected based on their access, transport and workload capacity, with preference given to sites with ubiquitous wireless, desktop virtualization, and Voice over Internet Protocol (VoIP) capabilities.

With enterprises grouped in these categories, the organization’s CIO, Director of Infrastructure, and Network/Security leaders were interviewed.

Customer network types in the survey:

Our survey assumed different network architecture models are associated with certain cost, performance, and risk factors. In order to assess the relative cost, performance, and risk impacts, different types of networks were analyzed to compare the value of single or multivendor network architectures. These network types are described below.

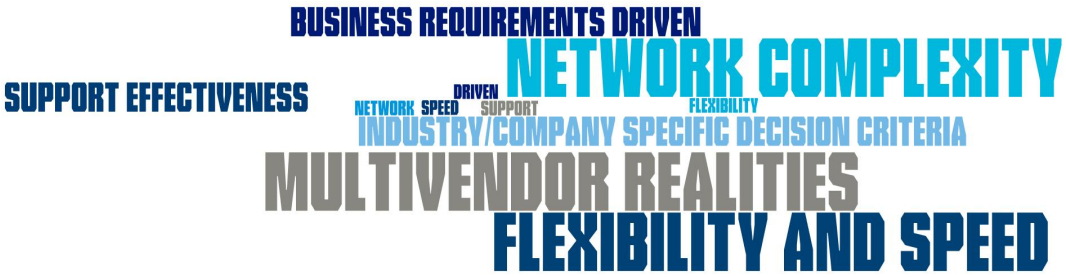
- Regionally distributed and supporting a centralized business function.
- Globally distributed network architecture, supporting decentralized business functions with centralized operations.
- Globally distributed network architecture, supporting decentralized business functions with complex regional network services.

This paper reflects the summary of findings derived from the customer interviews and data provided by customers, as well as the independent analysis and experience of Deloitte working with a broad variety of clients and their network strategies. The results of this study can be used as an input to allow further analysis of a customer's networking strategy decisions, based on the specific situation and appropriate balance of benefit and risk for a particular customer environment.

While this study seeks to reach general conclusions with respect to the benefits, costs, and tradeoffs of single-vendor and multivendor environments, customer are encouraged to evaluate their own business priorities and risk tolerance, in light of the available information and using the tools described in this analysis, in order to reach decisions which align with their overall strategies.

IT decision makers should be aware that the actual TCO, functional implications, and risk factors associated with vendor strategies are highly dependent on the specifics of the network and operating conditions of their organizations.

3. Functional considerations



The following functional considerations of single and multivendor network implementations were identified and evaluated in this survey:

Network functionality: Organizations prefer flexible network products that can meet changing business needs and growth requirements. To support growth over the long-term, networks must adapt to changing business priorities, enabling new services in a timely fashion. Key findings from the survey:

- Enterprises need to quickly and reliably add services to their networks, without introducing unnecessary risk to the production operations environment.
- Customers are most likely to deploy products from multiple vendors when a single vendor is not able to provide all needed network functions and features.
- The use of products from multiple vendors does not affect the ability to flexibly expand the network, and does not have a meaningful impact on network performance.
- Major network architecture decisions are based on the requirement to support business functions, and are not viewed as “single vendor” or “multivendor” decisions.
- Customers apply different weights to the value of network products based on their ability to satisfy key business requirements. For example, a financial services institution is likely to focus on a product’s ability to support uptime and security, whereas a manufacturing or transportation company is more likely to focus first on equipment costs.
- Enterprises typically use products from multiple vendors for wide area networks optimization, which drives additional ongoing operating expenses.
- When customers introduce multiple vendor products to satisfy functional requirements, they typically do not evaluate the tradeoff of additional functionality with the impact on long-term costs and overall business operations risks.

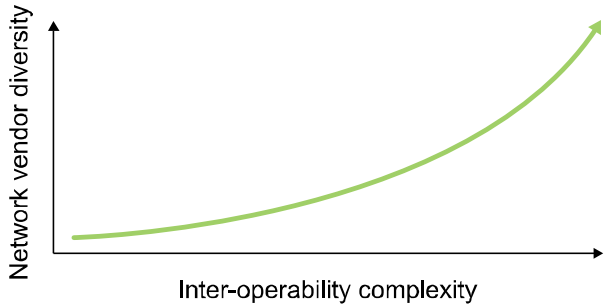


Figure 3.1: The number of network product vendors is correlated to interoperability complexity

Network interoperability: Network components provide greater value if they interoperate without affecting performance, security, manageability, or operational stability. Maintaining interoperability is crucial for an organization which operates a multivendor network, and this carries additional associated costs. Key findings from the survey:

- Networking equipment from different vendors is not designed to interoperate under all production conditions; when these products are implemented on a common network, greater customer effort is required around design, testing, and management.
- Customers maintain additional network facilities to test, diagnose, and resolve vendor interoperability issues, and validate multivendor architectures prior to use in production. This involves significant time and expense by customer organizations, and involves significant technical integration effort, responsibility, and operational risk, which must be assumed by the customer.
- Customers have difficulty getting vendors' support teams to work together, and experience operational impacts related to vendors' lack of understanding of each other's products.
- Even customers who prefer a single vendor network approach may occasionally be required to incorporate multiple vendors' products into their networks for certain periods of time, due to circumstances such as mergers and acquisitions, or where a non-incumbent vendor is the only supplier of a critical functional capability.

Network reliability and problem resolution effectiveness: Network reliability is critical to supporting ongoing business functions. Customers value networks that can sustain operations with minimal impact to network services when a network outage does occur. Network service levels are measured by the amount of unplanned network down time. Key findings from the survey:

- Product reliability is not a significantly point of differentiation when customers are considering network vendor product alternatives.
- Most customer networks are committed to SLAs of 99.99% availability. Organizations can fulfill this requirement using either single or multivendor architectures — although at different cost levels and with different levels of operational risk.
- Multivendor network architectures negatively impact interoperability, problem resolution effectiveness, and overall network service reliability.

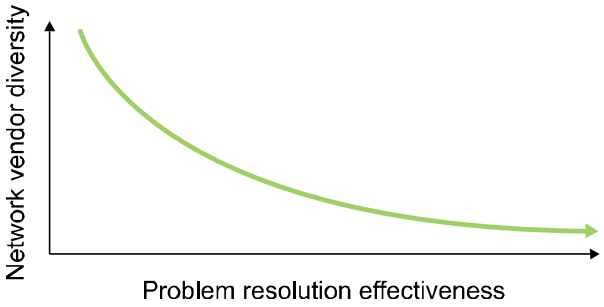


Figure 3.2: The number of network product from different vendors is inversely correlated to problem resolution effectiveness

Network staffing: Staffing is defined as direct labor costs of employees supporting the network architecture, design, and operations. Key internal resources are typically responsible for the design, implementation, and operations the network. These staff members generally provide front-line support and escalate to network vendors only when required. Attracting and retaining skilled staff to design and maintain the network is critical to effective network operations and risk management. Key findings from the survey:

- Staffing levels are not directly impacted by the use of multiple vendor products, but are primarily affected by the size and complexity of the network and frequency of changes to the network. Customers are able to obtain reasonable functional proficiency with multiple vendors' equipment based on existing knowledge. Where multivendor network implementations increase complexity, staffing costs will increase accordingly.
- Staffing levels are impacted by the availability of online information. The support information available from Cisco is extremely valuable to customers' staff for design, configure, support and troubleshooting activities; equivalent information is not generally available from other vendors. One enterprise reported that "the other manufacturers do not come close to Cisco's online resource documentation."
- Network engineering and support groups have issues finding experienced network architects for leadership roles; junior network resources are easier to hire. Most organizations have low staff turnover, which reduces operational risk in this area.

Organizations with single vendor implementations reported less staff time required to resolve operational issues related to interoperability and compatibility between products.

Network management: Effective network management is a key to successful operations and delivery of business services. Key findings from the survey:

- Managing network equipment from multiple vendors typically increases both operational complexity and management costs, since additional tools and upgraded skills are needed to operate multiple vendor devices. The increased cost and management complexity is caused by vendor product differences and the required addition of tools to manage a heterogeneous environment.
- More than half of the organizations relied on additional 3rd party tools to monitor and or manage their network when multiple vendors were involved.

Network Vendor Support: Product suppliers are typically contracted to provide maintenance and support services for network equipment and network services operations. Key findings from the survey:

- Multiple vendor network support is more complex and difficult, and involves additional indirect costs and risks. Vendors often are unable or unwilling to develop and maintain a working knowledge of the hardware, software features and functions, and platform-specific limitations that affect compatibility with other vendors' equipment in the network. This impacts customers' ability to operate their networks, contributing to longer issue resolution times, more complex change management, and more serious service impacts during network outages.
- When multiple vendors are contacted to diagnose and correct a network issue, it is not unusual for "finger pointing" and vendors' inability to work together to delay resolution of issues. The increased operational impact increases the burden on the customer's networking team. This results in substantial negative impact to business operations, and increased cost due to time and effort required to resolve problems.
- With multivendor designs, customers may not be able to leverage the long term relationships established with a primary vendor. With a single vendor, support is simpler and less costly — a benefit of a stronger supplier relationship. As one customer with a single vendor implementation reported, "I have never had to pay for information and advice. I have only had to pay for my overall products/software and support contracts."
- Customers assume additional operational risks when their primary vendors are contracted to support network equipment and services from other suppliers, when the primary vendors are not prepared to provide it. Enterprises are moving away from more complex multivendor designs in order to have a single provider accountable for complex network services delivery such as MPLS and ISP services.
- Enterprise network support agreements are structured with little distinction for multivendor network designs, which presents additional support risk to customers.
- Organizations are often offered "free" or heavily discounted support from "nonincumbent" vendors for the length of the support contract, in attempt to gain future business. This can provide a short-term cost benefit in reduced support contract fees when first introducing a multivendor network architecture.

Vendors often are challenged to maintain a working knowledge of other vendors' equipment, software, and services. Competing vendors are not always aware of the capabilities of other suppliers' products, and how they interoperate with their own.

Network security: Security policies are established and enforced to protect the availability, access, operational security, data privacy, and integrity of the network. Security controls are typically managed by specialized groups responsible for maintaining security across the network, regardless of network vendor. Key findings from the survey:

- Organizations have different tolerances for security risks, based on the nature of the financial impact, burden to end-users, business objectives, data sensitivity, and company reputation.
- For many customers, growth through acquisitions requires network equipment from different vendors to be integrated. Integrating these networks into a single multivendor network provides special security challenges for these customers, which contribute to higher cost, complexity, and operational challenges.

- Managing security of network equipment from multiple vendors requires sophisticated skills, and understanding of security and network architectures from all vendors involved. Additional product training may be required, but this is not a significant cost factor.
- When network changes are minimal, organizations are generally able to meet their network security requirements equally well in single or multivendor network environments.
- Organizations were most active defining and implementing new security policies associated with expanding mobility and internet capabilities, based on priorities of risk/threat assessments.

Wireless and mobility: Organizations increasingly consider wireless access to be a central component of the network. Key findings from the survey:

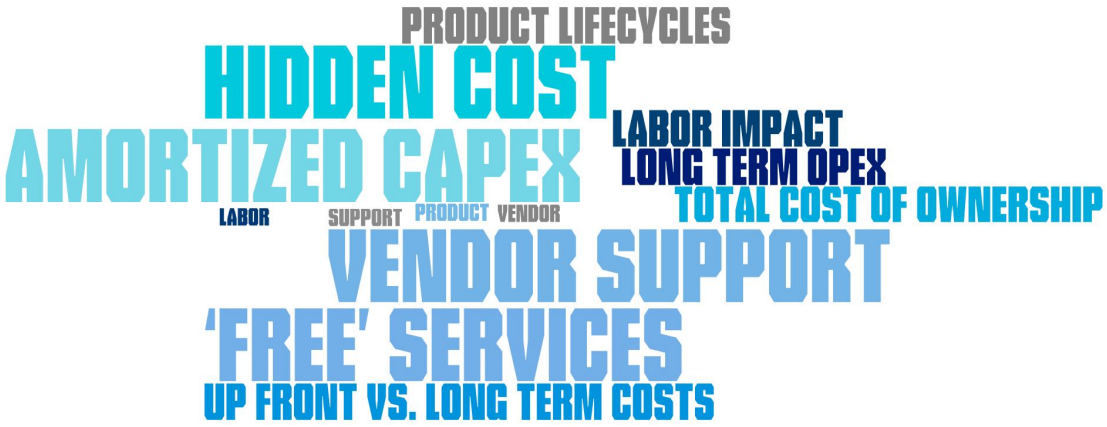
- Many organizations are implementing wireless services in order to deploy unified communications services to the business. Neither single nor multivendor network architectures significantly impact the initial product cost of deployment of wireless services.
- Using multiple vendors marginally impacts installation costs and the ongoing operational costs of supporting wireless services; adding wireless services may not significantly increase the complexity of the network, but the introduction of new devices from multiple vendors requires investments in support, security, and testing.

Analysis of functional considerations

The survey results showed that the use of products from multiple vendors may provide some additional functionality, but also introduces new functional and operational complexities and support challenges. Multivendor networks create interoperability challenges, and add functional complexity in the areas of network management, security, and support, and driving the need for additional training and staff sophistication.

Key Observation: Important functional and operational impacts can result from multivendor network implementations, and enterprises must understand and mitigate these potential effects on their network services delivery capabilities.

4. Financial considerations



The survey also examined financial considerations when implementing single vendor and multivendor networks. Our analysis focused the impact on capital expenses and ongoing operating expenses, at the time of purchase and over the longer term. The following considerations were identified and evaluated in this survey:

Initial product costs and ongoing operational costs: Enterprises weigh their purchasing decisions on initial product costs and ongoing operational costs. Key findings from the survey:

- Initial pricing for products from nonincumbent vendors is typically heavily discounted, with initial support services and training included with the cost of the products, in order to reduce the perceived up-front cost and impact of procurement decisions.
- Incumbent vendors typically reduce ongoing operational costs by providing "free" advisory services for network architecture changes, designs, and implementation. One customer reported they "did not spend a single dime on consulting services since initial implementation."
- The cost of providing business continuity is not affected by the use of a single or multivendor implementation.
- The use of multivendor networks carries incremental ongoing costs of network management tools and additional complexity of network operations.
- The incremental cost associated with multiple vendors reduces the net savings gained from the lower costs of equipment from new vendors.

- When analyzing direct costs, enterprises need to consider three factors together to assess full financial impact of a product purchase: direct product costs amortized over the product lifecycle; installation, support, and operational expenses; and labor.

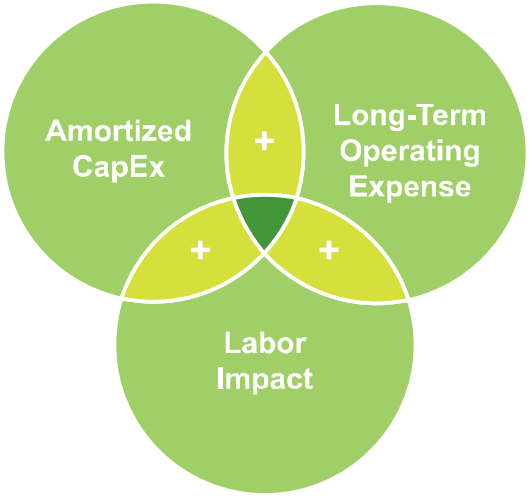


Figure 4.1: Total cost of any infrastructure purchase must account for the combined long term effect of amortized capital, long-term expenses, and labor impact.

Product lifecycle costs: Enterprises can take advantage of extended equipment lifecycles to save costs over the long run. Key findings from the survey:

- Differences in refresh strategy for network products were not associated with the use of multivendor network architectures. This is almost always a financial decision, not a technology design decision. Extended network lifecycle management programs are used to defer capital investments, and are not influenced by network vendor decisions.
- Costs comparisons must be amortized across the actual useful life of the products. Products that are “expensive” at the time of purchase, but which also have a longer lifecycle, can be less expensive on an amortized basis compared to other products with lower initial costs and shorter lifecycles.
- New products from “nonincumbent” vendors may offer an initial CAPEX incentive due to discounted product pricing, but any potential savings may be reduced or eliminated by accelerated depreciation losses caused by retiring older equipment before it has reached the end of its useful life.
- Enterprises refresh network equipment on an “as-needed” basis, according to specific functional capabilities of the products, rather than following a fixed capital depreciation schedule. Network equipment in production use is frequently fully depreciated and past the end of the depreciation cycle.

Products from certain vendors are more likely than others to be maintained past their full depreciation periods. Not all vendors invest similarly in developing “long lifecycle” products which will meet service requirements for five or more years.

Analysis of financial considerations

To understand the full capital costs and ongoing operating expenses for multivendor networks, enterprises must take the following into consideration:

- The incremental cost savings of the purchased products.
- The incremental additional internal and external costs of staffing, supporting, maintaining, and integrating “nonincumbent” products.
- The incremental cost of operational risk mitigation, specifically the costs to remediate potential increases in frequency and duration of network outages and service interruptions, as well as the direct costs of outages, including lost revenue.

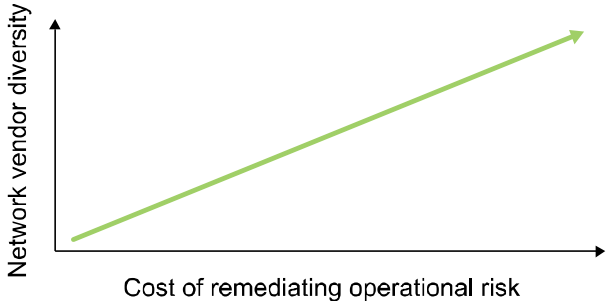


Figure 4.2: As network vendor diversity increases, the cost of remediating operational risk increases

Key Observation: Customers do not see material cost differences between single and multivendor networks. Network purchases which bring potentially lower initial product costs are frequently canceled out over time with higher long-term costs associated with service, support, and remediating additional operational risk. The cost of an unmediated business impact can be significantly larger than the product cost savings from network vendor diversity.

5. Operational risk considerations

In addition to functionality and costs, the survey examined operational risk considerations of single vendor and multivendor network implementations. The following considerations where identified and evaluated in this survey:

Network criticality: Organizations interviewed reported that operational risk considerations associated with the production network were extremely important. Organizations consider the continuous operation of the network to be critical to business operations, an important component of their most valuable core computing systems. Impact and severity of an outage depends on the type of business functions dependent on network services, and the structure and reach of the network. Key findings include:

- In many cases, the level of risk is the key determining factor in evaluating the potential value of a single vendor or multivendor architecture.
- If the network is unavailable, part or all of the business may not be able to operate, with significant direct costs, financial losses, and in many cases very large potential revenue impacts.
- Some enterprises have quantified the impact of network outages in terms of the direct cost impact to the business in the event of a network outage. The direct cost of network outages ranged from $20,000 to $200,000 per hour, in labor and services costs.

Risk analysis: A key question for organizations is the level of increased risk associated with a given network design and product mix. Key findings include:

- Due to the nature of product designs and interoperability considerations, deploying multiple vendors' products involves increased interoperation and integration risk, assumed by the customer organizations.
- The incremental cost savings achieved by using a "nonincumbent" vendor product is counterbalanced by the costs associated with additional operational risk: interoperability and support problems can increase downtime, cost impacts, and loss of business function.

- In multivendor network implementations, mitigation of operational risk is effectively transferred from the vendor to the customer. The burden is on the customer to manage the different vendors to satisfy interoperability requirements and to resolve incompatibility issues, configuration problems, etc. Customers are not well positioned to assume this risk, given their focus on the business and not on the technology. As a result, they are typically not equipped to address these complex risk mitigation challenges.

Framing risk: Customers must carefully evaluate the tradeoffs of gains and potential losses associated with risk transfers. The cost savings achieved by using different vendor products in a single integrated business-critical network must be properly balanced against the risk of potentially large losses associated with higher probability of outages attributed to reduced interoperability and increased integration complexity. In a single-vendor environment, customers rely on vendors to support the interoperability of their products, but this becomes the customer's responsibility when more than one vendor is involved. The net costs of these risks are assumed by the customers.

Customers keep in mind the "simplicity principle:" a more complex system, such as a multivendor network, is more likely to break down, often in unanticipated ways, and will influence decisions regarding the balance of functionality, cost, and business risk.

Focus on correlated risk

The survey findings support more general observations on the correlation of risk, and balancing decisions to account for overall risk management.

Interdependencies among risks often cross business unit and functional boundaries. Attempts to mitigate costs or risks in one area, such as network products or vendors, may affect risk exposure in other areas, such as network operations, and vice versa. Different areas of the business may independently pursue activities that, while remaining within each group's individual risk tolerance, create unacceptable risks for the company as a whole. Sometimes, organizational silos can mask important connections even in closely related areas such as network engineering and network operations, which may be managed in different parts of the organization.

Decisions involving the network must consider business services operations risk. Examining services operations risk might fail to account for dependent risks that are often managed in silos, such as activities related to network operations, support issues, intangible assets such vendor relationships, or deployment of highly skilled staff. A risk event in any of these areas can create a ripple effect through the others, leading to unintended consequences.

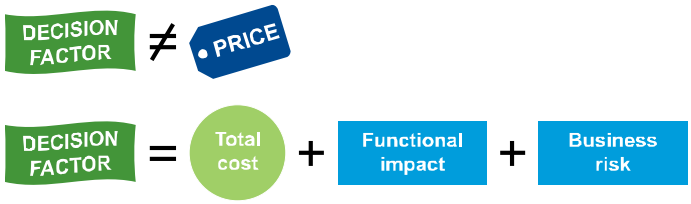


Figure 5.1: Network vendor strategies should be based the total costs, functional impact, and potential business risk

For example, a significant network operations support services decision could wipe out the economic benefit of an otherwise rational and cash-efficient network vendor strategy. Strained relationships with a key supplier could put a valuable link in the business services operations chain in jeopardy. Failing to appreciate key technology interdependencies of vendor equipment – perhaps never before used in a specific configuration and under specific operating conditions – introduces unknown risk into the service operations environment upon which key business processes depend. Lack of preparation in the implementation or maintenance phases throughout an organization's network asset management cycle may also result in unknown operating risk and unanticipated risk burden.

If risks are examined individually but not considered together as companies assess their business operations strategy, the extent of the upside gain and downside risk in the services operations chain cannot be fully understood. Excluding considerations for any one area could lead to a business decision that doesn't contemplate risk holistically across the organization. Mitigation in one area could also increase the significance of the risk in the other, and failing to aggregate the risk could mean that mitigation is not properly effective.

Example of estimation of risk tradeoffs: When evaluating business risk tradeoffs, and the introduction of new elements which increase risk potential, an appropriate frame of reference is useful. To analyze the relative savings available from using multivendor networks, the context of overall business revenues put at risk is important. As reported by our survey, total IT costs are a small fraction of total business revenues — typically between 2 and 5 percent. Network costs are also a small fraction of total IT costs, usually between 15 and 25 percent. The savings available from new vendor products, even under aggressive scenarios, is less than 20 percent, and would be applied to a subset of network spending. From this perspective, when compared to total company revenues, an example of the total potential cost savings of using "non-incumbent" network products would be:

Savings potential => 4% * 20% * 20% * 50% = .08%

In this example, for an enterprise with total annual revenues of $1,000,000,000, the three-year cost savings for non-incumbent network equipment would be $800,000. For an enterprise of this scale, a single outage of a few hours over a three year period could easily result in direct costs exceeding the cost savings, with much higher potential losses of revenue. The losses generated by one event in three years would eliminate all gains achieved by introducing the new equipment in the network.

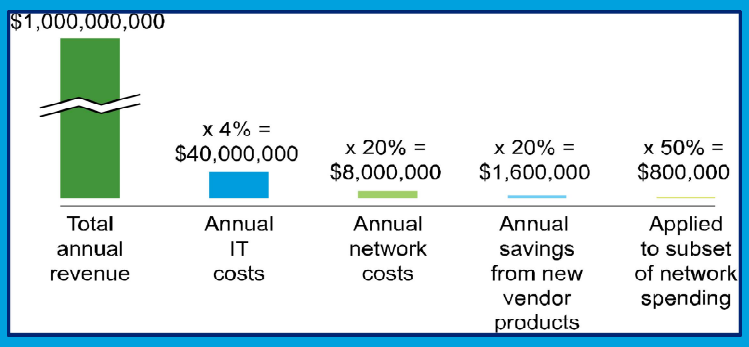


Figure 5.2: Relationship of total spending to savings from network products

Analysis of risk considerations

An analysis of business operations risks illustrates the decision factors which must be considered. As indicated in the example above, incremental operational risk can result in disproportionally large costs and losses of revenues. When considering a strategy, decision makers must evaluate the small increased potential for very large downside risks involving business interruptions, lost revenue, and reputational damage. This potential risk must be weighed against the relatively small savings gained with introducing a nonincumbent product in a single vendor network environment. For this reason, most organizations are reluctant to deploy a multivendor architecture.

With a single vendor, the risk of interoperability is primarily borne by the vendor. The vendor takes responsibility for the functional integration of its own products. Enterprises using multivendor networks assume the “integration risk” of using products from different suppliers. This shifts the risk from the vendors to the customers, who must now bear the risk of ensuring end-to-end interoperability of products that were not necessarily designed to work together. The probability of risks associated with multivendor interoperability and unforeseen network outages can rarely be predicted outside of distinct conditions of a specific organization’s production operations. The only method of eliminating this risk completely is through the use of a single vendor network architecture.

Key Observation: Enterprises are risk averse to the probability of large downside risk. Decision makers should evaluate the modest cost savings of a multivendor product implementation against the small but increased operational risks. Most organizations are willing to pay marginally higher product costs for a single vendor network to eliminate the downside risks associated with interoperability, support, and reliability.

6. Summary

The survey showed that when comparing single-vendor and multivendor networks, organizations can achieve comparable network functionality. Despite initial pricing incentives, customers do not see significant cost differences over the long term between single and multivendor network deployments. However, a multivendor approach brings significant factors that increase business operations risk.

Customers regularly look at multivendor network options to address specific functional needs, but they do not always understand the implication of long-term costs, operational complexity, and business risk. The survey found that multivendor network implementations may offer lower initial product costs, but they are frequently associated with higher indirect costs in the areas of service, support, and staffing, and they carry significant additional operational risk. The potential risks of large losses caused by failure of critical infrastructure services causes most organizations to forgo the relatively small initial cost savings of multiple vendors and stay with a single network vendor.

Organizations look for a primary network vendor to help them deploy required services in a way that minimizes overall risk to their business. They strongly prefer one vendor to support all of their network needs. Organizations stated that even though they consider the possible savings in direct costs, having a single long-term network supplier with a broad array of diverse products and services to support their needs is worth paying a “risk reduction” price premium, particularly to reduce the possibility of operational issues which present large business risks.

Summary of Findings:

- Networks are seen as critical to enterprise business operations
- Use of multiple network vendors may bring initial cost saving, but gains are not meaningful within the overall financial context, and can introduce disproportionate operational risk
- Network vendor decisions involve enterprise risk management: balancing the functional considerations of network products, the full cost over their lifecycle, and the business risk of interoperability and complexity

Our survey found that as networks become more complex and integrated with critical business functions, IT leaders will need to judge the overall enterprise impact of network vendor decisions. We expect enterprises to continue to favor strategies which use a single network vendor, in order to minimize operational complexity and manage business risk.

Appendix A: TCO data

When considering "Total Cost of Ownership" ("TCO") for networking equipment, software, and services, it is important to consider all relevant factors which impact the cost of owning and operating the network. The table below shows a summary structure used in this survey to capture the different aspects of cost impact for network purchases, over the expected planning horizon.

The example below shows a typical summary view of total costs for network products, services, and support, over a five year period. Several key factors to consider when evaluating total costs include:

- TCO is best evaluated within the context of the overall network; equipment and software costs alone do capture the overall cost impact, and pricing comparisons of products do not provide sufficient information
- TCO must be calculated from the perspective of a designated (and typically arbitrary) time period, covering a minimum of three years, and preferably a five year period
- TCO is best captured using a view of total cash flow impact based on capital depreciation and all expenses incurred relating to the services delivered
- TCO comparisons of network design scenarios and product alternatives are more meaningful within the context of the full network cost summary shown below, averaged over a 3-5 year period

Network Total Cost Summary - Example	**Baseline**	**Year 1**	**Year 2**	**Year 3**	**Year 4**	**Year 5**
Cashflow Impact	***Annualized Costs***	***Cumulative Total***	***Cumulative Total***	***Cumulative Total***	***Cumulative Total***	***Cumulative Total***
Software License - Annual	$1,000,000	$1,000,000	$2,000,000	$3,000,000	$4,000,000	$5,000,000
Hardware Depreciation - Annual	$2,000,000	$2,000,000	$4,000,000	$6,000,000	$8,000,000	$10,000,000
Direct Expenses: Facilities/Power/Space	$500,000	$500,000	$1,000,000	$1,500,000	$2,000,000	$2,500,000
External Labor	$750,000	$750,000	$1,500,000	$2,250,000	$3,000,000	$3,750,000
Internal Labor	$350,000	$350,000	$700,000	$1,050,000	$1,400,000	$1,750,000
Training & Communication	$250,000	$250,000	$500,000	$750,000	$1,000,000	$1,250,000
Software Maintenance	$190,000	$190,000	$380,000	$570,000	$760,000	$950,000
Hardware Maintenance	$1,900,000	$1,900,000	$3,800,000	$5,700,000	$7,600,000	$9,500,000
Other Expense - Miscellaneous	$500,000	$500,000	$1,000,000	$1,500,000	$2,000,000	$2,500,000
Total P&L Cash Flow Impact		$7,440,000	$14,880,000	$22,320,000	$29,760,000	$37,200,000

Figure A.1: Example Summary of Total Cost of Ownership Analysis, total network view over 5-year period

Appendix B: Risk management

Deloitte recommends enterprise risk management activities that may include the following:

- Align risk governance with strategy: management should consider whether risk oversight and management are aligned with management's strategy. Enterprises vary widely in their business models, risk appetite, and approaches to risk management. A key consideration is that the board, management, and business units be aligned in their approach to risk and strategy — to promote risk-taking for reward in the context of sound risk governance.
- Set the tone and develop a culture of the enterprise risk management, promoting open discussion regarding risk, integrating risk management into the organization's goals and compensation structure, and creating a corporate culture such that people at all levels manage risks rather than reflexively avoid or heedlessly take them
- Provide input to management regarding the enterprise's risk appetite and tolerance and, ultimately, approve risk appetite and the statement of risk appetite and tolerance messaged throughout the company and by line of business
- Monitor the organization's risk profile, ongoing and potential exposure to risks of various types; review and approve the risk management infrastructure and the critical risk management policies adopted by the organization
- Periodically review and evaluate the company's policies and practices with respect to risk assessment and risk management and annually present to the full board a report summarizing the committee's review of the company's methods for identifying, managing, and reporting risks and risk management deficiencies
- Continually, as well as at specific intervals, monitor risks and risk management capabilities within the organization, including communication about escalating risk and crisis preparedness and recovery plans
- Continually obtain reasonable assurance from management that all known and emerging risks have been identified and mitigated or managed
- Communicate formally and informally with the executive team and risk management regarding risk governance and oversight
- Discuss with management the company's major risk exposures and review the steps management has taken to monitor and control such exposures, including the company's risk assessment and risk management policies
- Review and assess the effectiveness of the company's enterprise-wide risk assessment processes and recommend improvements, where appropriate; review and address, as appropriate, management's corrective actions for deficiencies that arise with respect to the effectiveness of such programs

Appendix C: Disclosures

Deloitte Consulting LLP (“Deloitte Consulting”) was commissioned by Cisco Systems, Inc. (“Cisco”) to develop and conduct this survey. The majority of the customers interviewed by Deloitte Consulting were provided and selected by Deloitte Consulting. Cisco did not participate in the interviews, and was not involved in the analysis of the customer data, or development of the study observations or conclusions. Deloitte Consulting provided this study and its materials to Cisco without input or direction received from Cisco, and maintained full control of the content of the report, its analysis, and conclusions.

Deloitte Consulting makes no specific claims for the potential financial, operational, or risk factors involved with the management decisions taken by a specific organization. Deloitte Consulting advises customers to perform appropriate financial, operational, and risk management evaluations based on their own analysis of their situations and environments, based on the general framework outlined in this study.

Please note that where the results of analysis are discussed in this publication, the results are based on the application of economic logic and specific assumptions. These results are not intended to be predictions of events or future outcomes and have been provided solely for the reader’s consideration.

Deloitte Consulting is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services to any person. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte Consulting shall not be responsible for any loss sustained by any person who uses or relies on this publication.

As used in this document, "Deloitte" means Deloitte Consulting LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Cover image:
Visualization: Young Hyun, youngh@caida.org
Data Analysis: Bradley Huffaker, brad@caida.org
Walrus is a CAIDA tool developed with support of DARPA NGI N66001-98-2-8922, DARPA NMS N66001-01-1-8909, NSF ANI-9996248, NSF N66001-01-1-8909, and the support of CAIDA members.
CAIDA is based at the University of California's San Diego Supercomputer Center.