Business Transformation Through Architectures

Minimizing Business Risks

Organizations are constantly challenged with aligning technology investments to solve business needs. This article highlights the importance of integrating business strategies and technical architectures to achieve business transformation. It discusses general industry challenges and trends about minimizing business risks, and Cisco's internal experiences with related specific business opportunities and challenges.

By Jawahar Sivasankaran, Distinguished IT Engineer
IT Customer Strategy and Success, Cisco

Corporate Strategy

Businesses today are tightly connected within the corporation and with external stakeholders including customers and partners. A breakdown in one of the connecting links can have a serious, and in some cases, debilitating impact on the business. These links are often tied back to IT systems. A given risk is connected through two key parameters: uncertainty and the probability of an event occurring. In recent times, the world has seen businesses faltering as a result of a single security attack or a natural disaster in one country having a domino effect on entire industries.

Business leaders are constantly looking at various options to minimize risks. Classic risk management techniques, including risk avoidance, risk acceptance, risk mitigation, and risk transfer, have been core discussion topics of corporate boards and CXOs, and IT plays a primary role in each of these areas. Effective business continuity strategies are important for day-to-day enterprise operations. At Cisco, IT business continuity teams work closely with their business partners to ensure that the right levels of disaster recovery and business continuity strategies are put in place. Securing intellectual property can be the difference between success and failure of a business. At Cisco, the Computer Security and Incident Response (CSIRT) team works closely with the various business entities inside and outside the company to have the right monitoring and forensics technologies deployed. Business leaders also have to cope with an increasing number of regulatory requirements. This is compounded by global expansion, and businesses have to implement the right systems to comply with local regulations and requirements.

All of these business practices have to be executed correctly. It could take only one misstep or oversight to negatively impact a company's brand value or cause loss of shareholder value.

CEOs and business leaders are increasingly relying on CIOs, CSOs, and CISOs to keep the business operations flowing smoothly and provide adequate protection from disasters and security threats. Business leaders want to enable their employees with productivity tools, including social networking for enterprise, which when deployed without the appropriate IT and security control points could lead to business impacting incidents. Finally, business leaders want to make the right level of investment through risk assessment strategies based on the criticality of a business process and the probability of disruption

- Risk management strategies: risk avoidance, risk acceptance, risk mitigation, and risk transfer
- Enable business continuity
- Protect brand value
- Secure intellectual property
- Adhere to compliance and regulations (e.g., SOX, ISOX, OSHA, IS-14489)

or failure of the process.

At Cisco, through the IT as a Service (ITaaS) model, IT services are connected to the business offerings. Taking a service approach moves IT beyond the traditional technology- and product-centric approach to a more comprehensive method that makes the business view the core focus of IT strategy. The company has embraced collaboration tools, which are provided by IT with the appropriate level of security and user training to keep the risks under control. Security training for employees engaged in outbound communications through social networking has resulted in a streamlined process for utilizing these tools effectively.

Business Operations and IT Executive Considerations

Business operations leaders and IT executives must have insight into the business risks to ensure appropriate investments are made within IT to manage those risks. For instance, IT service-level agreements (SLAs) have to be commensurate with the risks. Clear definition of processes for incident management is also critical. Within Cisco, IT classifies various services offerings to different tiers of criticalities and priorities. A mission-imperative service classified as Criticality 1 (C1) is defined as: “Any outage results in immediate cessation of a primary function, equivalent to immediate and critical impact to revenue generation, brand name, and/or customer satisfaction; no downtime is acceptable under any circumstances.” On the other end, a Criticality 5 (C5) service would be a business service with which a sustained impact will have little or no affect on the primary function. Based on the criticality of the service, resources are appropriately allocated for monitoring, management, and incident response.

Cisco currently has more than 25,000 Cisco® Virtual Office solution users who have data, voice, video, and wireless access from their homes. While this solution continues to provide tremendous productivity benefits for the company and employee satisfaction, it has also become a key part of Cisco’s business continuity strategy. The first of the several business continuity benefits of this solution was realized during the SARS virus outbreak in 2003, followed by several other natural calamities that included many instances of severe weather conditions in the U.S., the volcano eruption in Northern Europe that crippled air travel, and the earthquake and subsequent Tsunami in Japan.

- Reduce planned and unplanned outages
- Provide appropriate disaster recovery systems (risk assessment)
- Build workforce enablement strategies during emergencies
- Mitigate risks: corporate security programs and practices

As Cisco continues to grow into emerging markets, IT management is constantly evaluating processes and technologies that would fulfill this business need, and keep costs under control. While the traditional model of terminating leased lines provides good resiliency, it might not be cost effective for a very small branch office with only a few sales employees. Cisco IT is rolling out broadband-based remote office solutions that rely on VPN technologies. But at these offices there is a higher level of risk due to Internet failure, and this strategy is negotiated with the business.

The growing trends of IT consumerization and bring your own device (BYOD) have resulted in enterprises having to manage risks in ways never before seen. With this model, IT organizations do not have control over the physical assets and the applications running on them. Cisco has decided to embrace BYOD, and Cisco IT has taken a balanced strategy to manage this risk by allowing access to first-level productivity tools such as email and calendar through a basic registration for mobile access. Richer applications that are dependent on accessing the

internal infrastructure and data require further steps and are controlled through the Cisco AnyConnect® application.

Cloud computing has emerged as an apt solution for IT risk management. Enterprises can create an elastic environment with which resources can be dynamically moved within a private cloud, or utilize the resources of a public cloud provider for proactive or reactive risk management. The Cisco IT Elastic Infrastructure Services (CITEIS) initiative has provided a solid private cloud solution for the enterprise and has positioned Cisco to create a truly dynamic environment, resulting in better business continuity options.

Technical Architectures and Solutions

When looking at architectures for business resiliency, an important consideration is dependency mapping. A business service can traverse cross-functional boundaries, and it is important to identify the dependencies between different services in IT. For a business systems owner, there is nothing more frustrating than seeing his or her service experience a failure when the individual IT teams report that specific technologies are functioning fine.

- Balance high availability with costs (e.g., dual circuits, protected versus unprotected WAN circuits)
- Provide remote working capabilities for employees
- Enforce security policies, monitoring, and audit
- Consider active-active data center architecture

The architecture should look at various risk management strategies. Utilizing service providers through a “clean pipe” solution is a good example of risk transfer strategy. In addition to using on-premises, enterprise-wide solutions for protecting against Distributed Denial of Service (DDoS) attacks, Cisco IT also “transfers” some of the risk to its service provider partners to ensure that DDoS attacks are blocked before they infiltrate the enterprise. Another popular strategy among enterprises with risk transfer of security functionalities is the use of cloud-based security solutions. The ScanSafe solution offers comprehensive web-based security with both software (working with Cisco AnyConnect) as well as through integration with the Cisco ISR G2 Routers for branch offices.

There are times when enterprises have to accept risks, at least in the short term. Based on the criticality of the risk, temporary workaround architectures are usually put in place if a permanent solution is not technically feasible.

The design and build of a global WAN is a great example of balancing the right level of risk with the appropriate investment strategies. An enterprise has to carefully weigh the cost versus benefits of building redundant links through transoceanic circuits that will limit oversubscription in the event of a link failure. Similarly, the decision to buy protected circuits (which could be 10 to 20 percent more expensive) over unprotected circuits is a decision to be made based on the business needs.

Data centers are the heart of today’s IT environments. For its production needs, Cisco IT has implemented a Metro Virtual Data Center in active-active architecture. This approach ensures the highest availability and business resiliency for the enterprise.

Products and Services

Based on the business needs and the architectural components, specific products and services should be chosen to help solve business risks. A major risk to enterprise infrastructures would be products that are end of sale and end of support. Cisco IT follows a rigorous end-of-life product management strategy to keep the infrastructure up to date, through the use of the Cisco Network Collector tool from Advanced Services. As Cisco Prime™

architecture rollout progresses, the work center within Cisco Prime Management will enable end-to-end lifecycle of key borderless networks functionalities.

A major part of Cisco's internal risk management strategy for the infrastructure is the use of Focused Technical Support (FTS) from Cisco Services. With this service, Cisco IT gets best-in-class support to protect its infrastructure investments. Through the use of complementary offerings such as the Network Optimization Service, Cisco IT has been able to significantly reduce network-related Critical 1 and 2 incidents.

An important consideration with globalization is security and compliance. With web-based security attacks on the rise, Cisco IT has globally deployed IronPort® Web Security Appliances in an on-premises design and is in the process of complementing it with the cloud-based ScanSafe solution. Branch office solutions in the future for enterprises would include additional requirements for secure, direct access to the cloud and the Internet. Not having to backhaul all the traffic to the nearest data center would result In significant savings for enterprises.

- Cisco Virtual Office (25,000+ Cisco employees deployed) for remote working
- Cisco Unified Computing System, Nexus switches for optimized design; Nexus 1000, Virtual Security Gateway for workload mobility
- Hardware and software updates / refresh through Remote Management Services (outdated software and hardware major cause for IT downtime)
- High-definition video for business continuity
- Intrusion prevention, next-generation firewalls, web/email security, and integrated security practices

However, this approach could result in security implications with relaxed rules for split tunneling. To solve this challenge, Cisco branch offices will have an integrated architecture with ISR G2 Routers and cloud-based ScanSafe to provide the required security solution. Cisco is also implementing an expanded Identity Management Framework with Cisco TrustSec® and Identity Services Engine (ISE) solutions to offer enhanced security with an Any Device/BYOD solution allowing employees, partners, and customers in global locations seamless access to the enterprise. Through the use of security technologies such as the Adaptive Security Appliances, email security systems, and Intrusion Prevention Systems, Cisco is able to protect its global infrastructure.

For its data centers, through the use of Cisco Unified Computing System and other innovations such as unified fabric, Cisco IT is able to provide a highly resilient enterprise solution. The Cisco Nexus® 1000 and the Virtual Security Gateway provide the workload mobility when moving virtual machines between different areas of the data centers.

To help solve business problems, an architectural approach that looks at the end-to-end enterprise value can bring business and financial results that far exceed a company's investments. A structured process has to be in place to align business requirements with the right technical architectures, with a strong connection to business and IT processes. Integrating business strategies with technical architectures, and implementing associated IT best practices, can go a long way toward minimizing business risks. This integration can also lead to other significant business transformations. We will continue to share information on the topic of business transformation through architectures with lessons learned from Cisco's own experiences.

For More Information

To read Cisco IT case studies on a variety of business solutions, visit Cisco on Cisco: Inside Cisco IT www.cisco.com/go/ciscoit.

Note

This publication describes how Cisco has benefited from the deployment of its own products. Many factors may have contributed to the results and benefits described; Cisco does not guarantee comparable results elsewhere.

CISCO PROVIDES THIS PUBLICATION AS IS WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some jurisdictions do not allow disclaimer of express or implied warranties, therefore this disclaimer may not apply to you.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**