U.S.
Resilience
Project

CASE STUDY

Cisco Systems
Based on an interview with
James Steele, Program Director,
Supply Chain Risk Management,
Cisco, August 8 2011

De-Risking the Supply Chain: Cisco's Risk Intelligence and Analytic Tools

In a Nutshell

Supply chain risk management is critical for Cisco Systems because it relies on outsourced manufacturing for more than 99 percent of the products it delivers, most of which are configure-to-order. According to James Steele, Cisco's program director for supply chain risk management: "In the past, supply chain operations was "care-about" only when things went wrong. The focus was not on growing the business, but on keeping the trains running on time. Over the past 15 years, there has been a sea change in supply chain management. It has become a strategic capability for many companies, and it continues to get the resources, visibility and focus needed to manage it as a platform for growth. Supply chain risk management is a key element in this evolution."

Cisco has built a risk management program focused on anticipating and mitigating any event or circumstance that could disrupt its global supply chain. The goal: to incorporate risk intelligence, agility and resiliency into the supply chain so that it is prepared to respond to any threat Examples of the program in action include:

- When Bangkok's airport was shut down by protestors in 2008, Cisco had truck convoys ready to move from their partner's nearby factory to an airport in Malaysia, sparing customers any disruption.

- Within 48 hours after the 2008 Chengdu earthquake in China, Cisco was able to conduct a full impact analysis, gain complete visibility into the supplier footprint in the area and initiate a crisis survey targeted at the suppliers emergency contacts.
- When the economic downturn worsened at the end of 2008, Cisco quickly launched a financial risk assessment (FRA) initiative to identify suppliers with single sourced parts that have high revenue implications for Cisco. Once the financial assessment was complete, the team separated suppliers into three categories: "Green," requiring no action; "Yellow," needing to be monitored; and "Red," needing mitigation. When two of the suppliers filed for bankruptcy protection, Cisco already had put in place "last time buys" and established second sources for their parts.
- When reports of an H1N1 outbreak in Mexico City surfaced in 2009, it took Cisco three days to put together detailed risk assessments of potential impact on orders, revenues and available contingency plans.
- Within 24 hours of the 2011 earthquake/tsunami in Japan, Cisco understood the key impacts to its extensive supplier base in the impacted area and formed a 100+ person war room that launched an intensive 70-day effort to mitigate the impacts.
- Cisco anticipated the escalating risk of the recent Thailand floods in October 2011 and formed a proactive war room that allowed the company to adjust its supply chain to minimize the impact to key suppliers in the region.

Cisco's supply chain risk management process pairs risk intelligence — knowing where their vulnerabilities are — with risk analytics — knowing where the highest probabilities for disruption are.

Key Tools for Supply Chain Risk Intelligence

Business Continuity Planning (BCP)

The BCP program collects information on key suppliers and key nodes in the supply chain. Although BCP has become a standard tool for many companies, the challenge for Cisco is simply its scope and scale — managing a global network of more than 900 suppliers, six EMS partners, multi-traffic lanes, hubs and carriers that the company uses — and that information is continually changing. Business continuity data gives Cisco insight into the impact of a disruption, creating an ability to identify which suppliers are affected by an event and its overall impact on the supply chain.

Cisco's BCP program gathers a variety of information from its key supply chain partners through a survey process that occurs several times per year.

Major Elements of Cisco's BCP Program

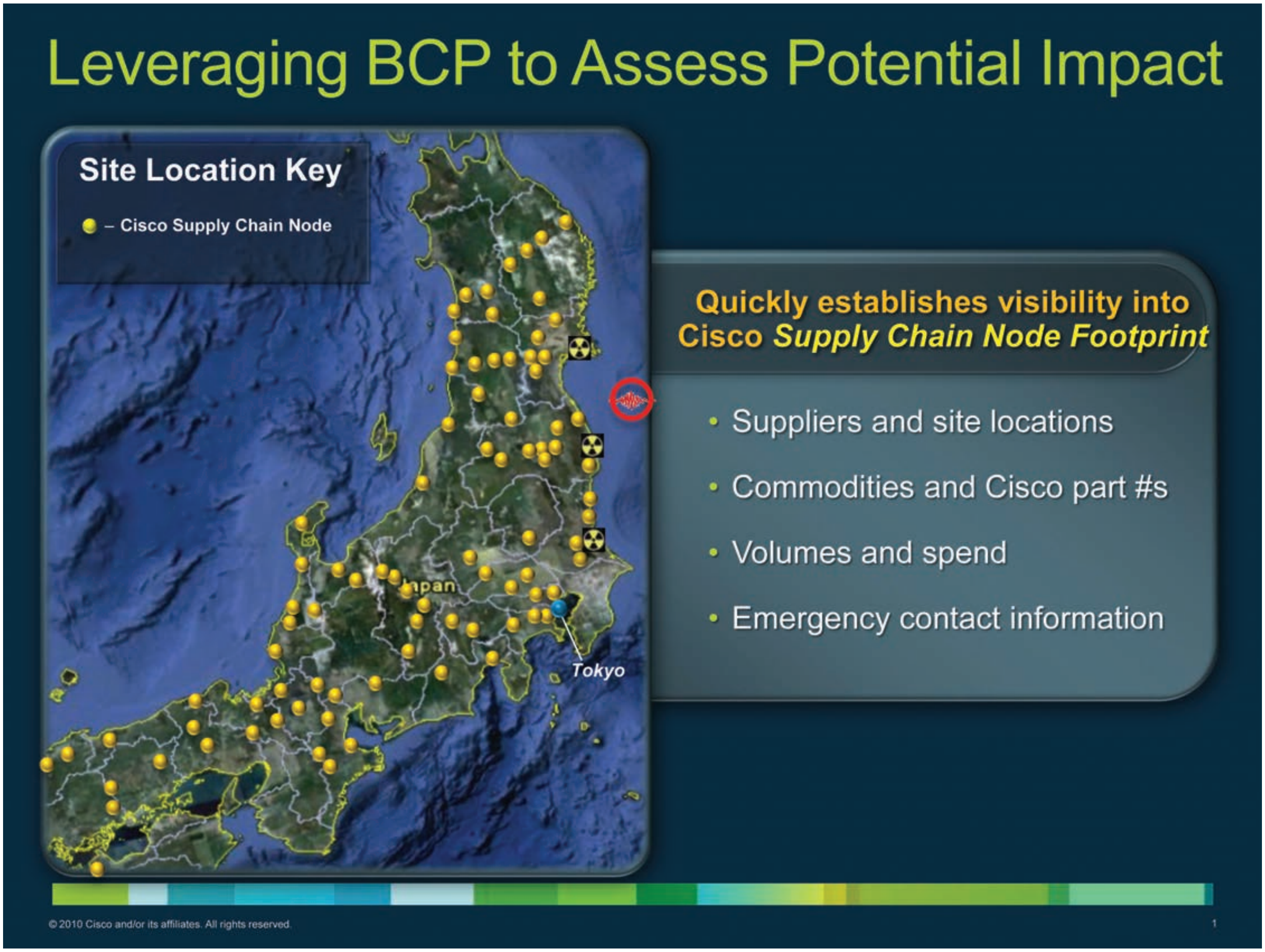
Collect, manage and utilize BCP information on all key supply chain nodes:

- Map critical components to supplier sites;
- Identify Time-to-Recover at the part and site levels;
- Evaluate preparedness based on an objective format;
- Validate Business Continuity Plans through audits and drills; and
- Utilize BCP data as the starting point for any incident response

The survey collects information on partners' business continuity practices, time to recover (TTR) in the event of a disruption and key emergency contact information, as well as financial information. With this data, Cisco can define the recovery profile of a product as characterized by the resilience of all component supplier factories, inventory hubs, partner (or internal) production facilities and logistics centers within that product's value chain.

BCP Visualization: Cisco's BCP Visualization capability provides a way to quickly assess the impact of an event — identifying which supply chain nodes are in the affected region, what parts and/or products are made there and what alternate sites can/should be engaged. This visualization and the underlying data becomes the starting point for any incident mitigation effort and allows Cisco to quickly qualify the potential impact an incident could have or is having on its supply chain operations.

Cisco Presentation Slide



Leveraging BCP to Assess Potential Impact

Site Location Key

● – Cisco Supply Chain Node

Quickly establishes visibility into Cisco *Supply Chain Node Footprint*

- Suppliers and site locations
- Commodities and Cisco part #s
- Volumes and spend
- Emergency contact information

© 2010 Cisco and/or its affiliates. All rights reserved.

1

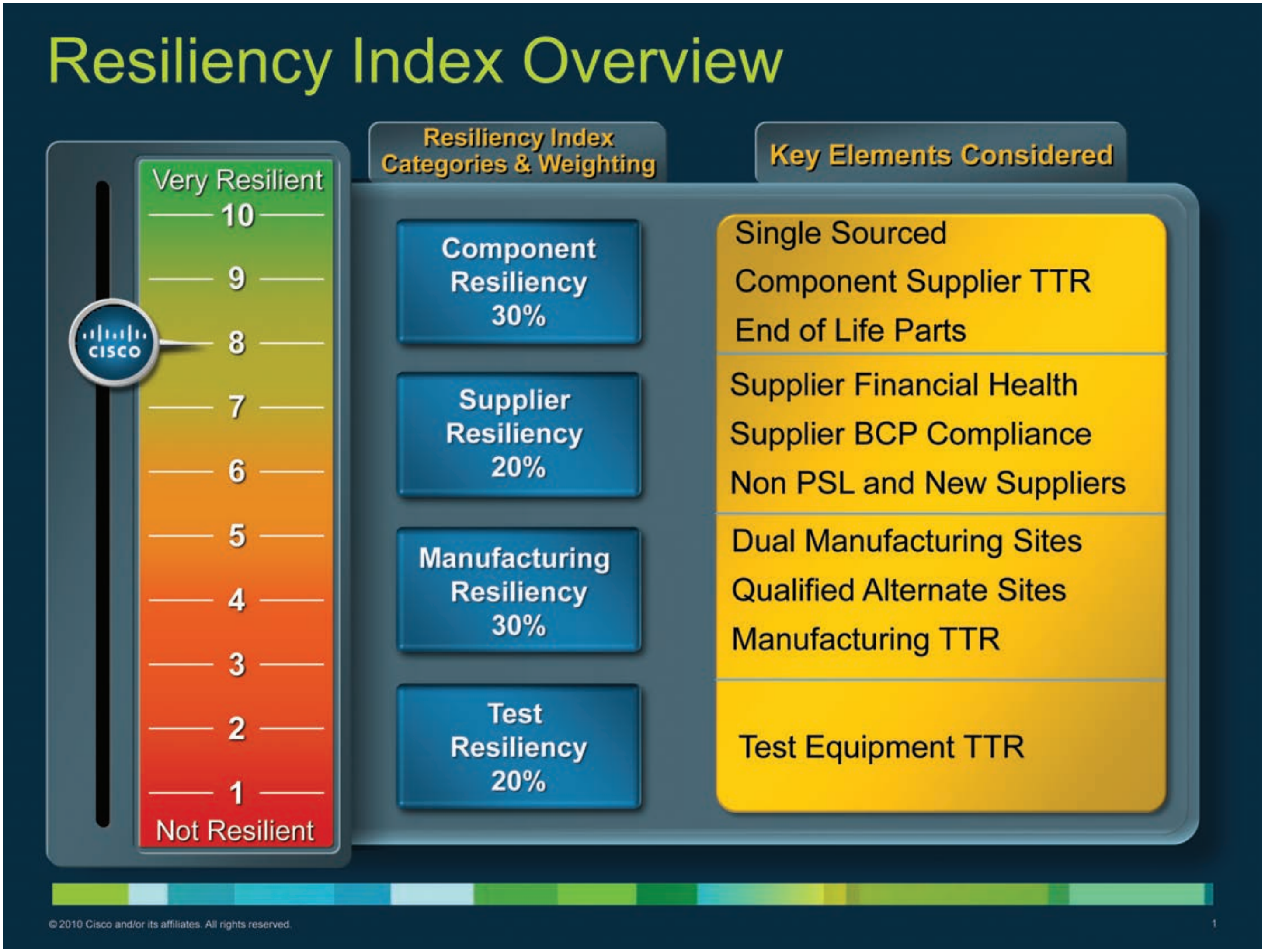
Crisis Monitoring: Cisco contracts with the National Center for Crisis and Continuity Coordination (NC4) to provide round-the-clock global monitoring to achieve its goal of "sense and respond" situational readiness. Alert profiles are constructed to capture the information on global incidents and events that Cisco monitors generally and in specific regions. Cisco has worked with NC4 to map all of its critical supply chain nodes worldwide and has set criteria for when alarms need to be sounded (for example, when an earthquake occurs within 200 miles of a site). The Cisco Supply Chain Risk Management Team is responsible for utilizing these alerts, as well as open source information to anticipate, sense and identify a potential risk to operations and to initiate the appropriate response.

Playbooks: Cisco has developed a set of response playbooks that provide a framework for organizing an incident response team, as well as a process for assessing the ground-level impact of a disruption, translating that into an actionable set of mitigation actions and identifying potential impacts to specific products, customer orders and ultimately to customer operations. Cisco maintains a "risk agnostic" master playbook that is applicable to any type of supply chain disruption regardless of its location and nature, as well as risk-specific playbooks that focus on recurring events such as hurricanes and typhoons.

Resiliency Index: Cisco invented the *Resiliency Index* and the TTR metric because it was not able to find any pre-existing standards or metrics to meet its needs. The *Resiliency Index* is a composite of resiliency attributes for the key "care-abouts" at Cisco — these include product resiliency, supplier resiliency, manufacturing resiliency and test equipment resiliency, which is a key control point given the globally outsourced supply chain. Each of these four elements of the *Resiliency Index* is in turn measured by an additional level of resiliency criteria. At the component level, for instance, the criteria includes the number of alternative sources, component suppliers' TTR and end of life plans and processes. At the supplier level, resiliency is linked to the financial health of suppliers and partners. Manufacturing resiliency is similar to component resiliency in that it is correlated with the availability of back-up or secondary sourcing and the manufacturers TTR following an event. Test resiliency is measured by the availability of inventories for long-lead test equipment parts.

The *Resiliency Index* is applied automatically to Cisco's top 100 products that, in aggregate, account for about 50 percent of Cisco's revenue. This version of the *Resiliency Index* is updated quarterly and is a key item on the overall Cisco Supply Chain Operations Executive Dashboard. However, the *Index* can be applied to a single product, a product line or a group of related products. The *Index* is tracked not only to illustrate the impact of Cisco's investments in supply chain resiliency, but also can be utilized to identify opportunities to improve resiliency in existing and new products.

Cisco Presentation Slide



Resiliency Index Overview

Resiliency Index Categories & Weighting	Key Elements Considered
Component Resiliency 30%	Single Sourced Component Supplier TTR End of Life Parts
Supplier Resiliency 20%	Supplier Financial Health Supplier BCP Compliance Non PSL and New Suppliers
Manufacturing Resiliency 30%	Dual Manufacturing Sites Qualified Alternate Sites Manufacturing TTR
Test Resiliency 20%	Test Equipment TTR

1

New Product Resiliency: Going forward, Cisco is moving the resiliency metrics upstream to new product introductions, each of which now has a risk and resiliency target. While design teams traditionally concentrated on cost and schedule, they now focus on risk and resiliency targets concerning choices about partners, components and sourcing choices. This allows Cisco to build supply chain resilience into the design of the product, rather than trying to de-risk the supply chain after the product launch.

New Tools/Next Steps

New Business Software Tools: The recent Japan earthquake/tsunami in March 2011 was a key test for Cisco’s supply chain risk management capability. Overall, Cisco had a very successful mitigation response and was able to ensure no downstream impact to customers or revenue despite the fact that more than 100 of Cisco’s suppliers were impacted by the event. The enormous scale and scope of the incident, however, was a key learning opportunity to improve Cisco’s supply chain risk management capability and processes. Based on key lessons from its Japan response, Cisco is continuing to invest in increasing the automation of its crisis management workflow process — essentially the process of identifying all impacted components and translating these impacts into actionable mitigation plans and proactive visibility into downstream customer impacts.

Sub-Tier Resiliency Visibility: A key for additional risk management is to increase risk intelligence on supply chain resilience capabilities deeper into the supplier sub-tiers. This opportunity was identified clearly by Cisco during their Japan response in that, while impacts to their first tier of suppliers were highly visible, it was more challenging to identify impacts on the supplier sub-tiers. Such information is particularly important for highly engineered components in critical commodity areas such as semiconductors and optical components. Cisco is continuing to expand its supply chain risk management efforts into BCP coverage for select portions of its supply chain sub-tiers in order to be even more prepared for the inevitable next crisis.