U.S.
Resilience
Project

CASE STUDY

Cisco Systems
Based on an interview with
John O'Connor, Senior Director,
Value Chain, Cisco Systems

Supply Chains in Crisis: Dealing with Disaster — Cisco's Response in Japan

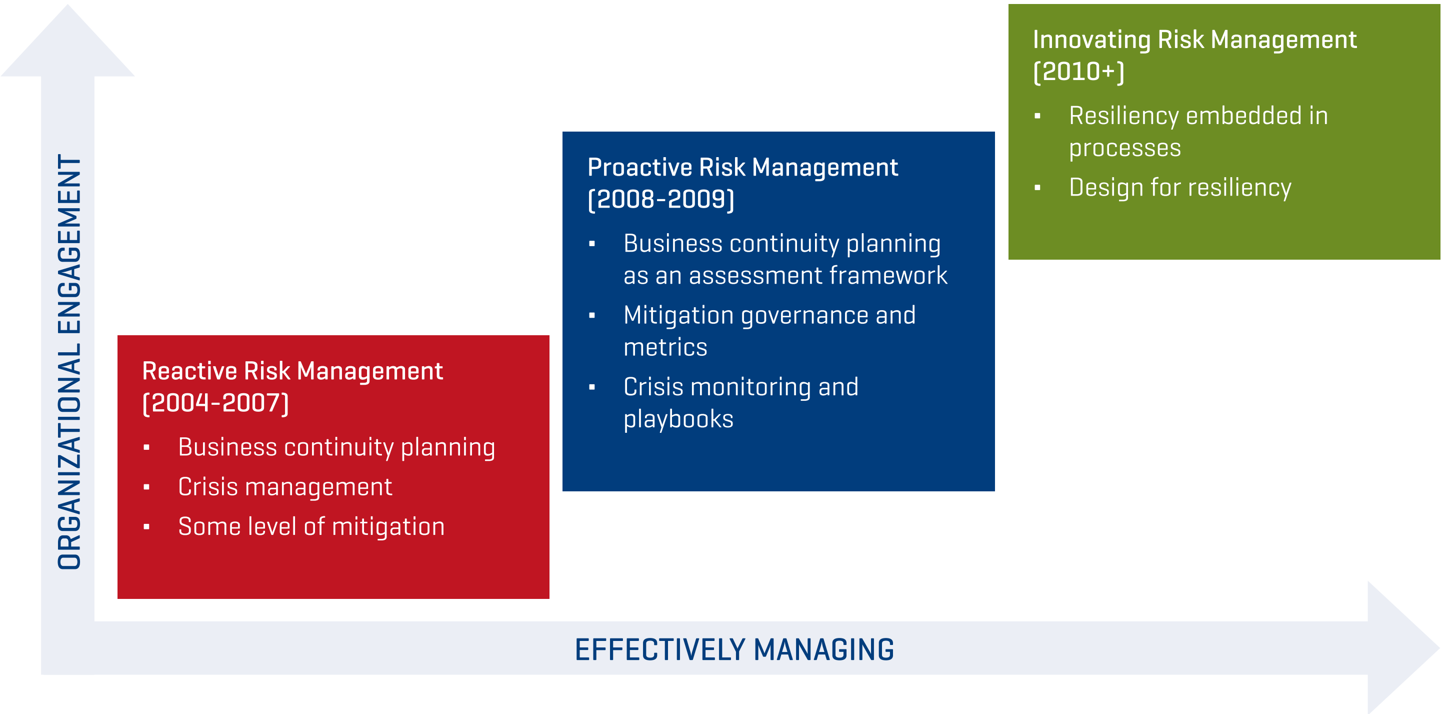
Evolution of Cisco's Value Chain Resiliency Management

Cisco has moved from a position of reactive supply chain risk management (2004-2007) to proactive risk management (2008-2009) to innovative risk management (2010). (See Chart 1.) In the same way, supply chain resilience has become a core business challenge across the enterprise, not just a logistics problem. New tools, processes and technologies were developed during the last decade to preserve the resilience of the supply chain — and the effectiveness and value of these tools were demonstrated during the crisis in Japan.

Background on the 2011 Japan Earthquake

The 9.0 magnitude earthquake that struck the Northeastern coast of Japan on March 11, 2011, was the most significant disruption that the global supply chain has experienced in modern times. This was based on the scope, scale and velocity of the evolution of the risk exposure and circumstances. What started as an extremely powerful earthquake quickly became a deadly tsunami that triggered an unprecedented nuclear facility disaster. This, in turn, further

Chart 1. Evolution of Value Chain Risk Management at Cisco



Reactive Risk Management (2004-2007)

- Business continuity planning
- Crisis management
- Some level of mitigation

Proactive Risk Management (2008-2009)

- Business continuity planning as an assessment framework
- Mitigation governance and metrics
- Crisis monitoring and playbooks

Innovating Risk Management (2010+)

- Resiliency embedded in processes
- Design for resiliency

compromised key elements of Japan's infrastructure, such as roadways, power transmission and electrical capacity for large portions of the impacted region. The crisis was a key test of the Cisco's Supply Chain Risk Management (SCRM) team and capabilities, as well as the overall end-to-end resiliency that the team and the Supply Chain Operations organization drives.

Cisco's Supply Chain Risk Management: Leading Practices Applied to the Japan Response

Supply Chain Incident Management Activation: Within 30 minutes of the initial NC4 alert of the 9.0 magnitude earthquake (NC4 is a third-party notification service that sends alerts based on a mapping of all critical supply chain nodes), the supply chain incident manager (on the SCRM team) was made aware of the event, alerted both the SCRM team lead, team members and the Supply Chain Operations senior leadership team. Within 12 hours, the primary supply chain incident management team was activated. This team consists of an extended group of operations functional leaders that represent their functional organizations during an incident.

Business Continuity Planning (BCP) Leverage: Utilizing SCRM's BCP data and processes, the SCRM BCP program manager was able to identify all direct suppliers, their associated sites and components (manufacturing parts numbers) and other critical supply chain nodes in the impacted area within 12 hours of the initial earthquake. The manager was also able to profile each supplier site from various resiliency perspectives. These included the expected time-to-recover (TTR) for the site, back-up power generation capabilities, and whether the supplier's components were single sourced or had alternate sites available.

Leveraging the BCP emergency contact information at the supplier site level, the incident management team was able to quickly establish (over the course of the first few days of the incident) contact with suppliers to assess the impact of the incident on site capacity, prognosis of their ability to continue to produce and distribute components. Utilizing Cisco's BCP Resiliency Visualization capability, the incident management team was able to develop a snapshot of the supplier impact and status over the entire region.

This snapshot was refreshed on a daily basis based on the evolution of the crisis circumstances (e.g. addition of the nuclear exclusion zone around the Fukushima nuclear facility, changing electrical power capacity projections, etc.) and facilitated faster, more informed executive decision making on mitigation activities and prioritization.

Supply Chain Incident Management Team War Room: Within 2 days of the initial earthquake, a formal war room was established to provide a central management point and decision making forum for all Supply Chain Operations personnel involved in the mitigation effort. The war room approach, structure and operations were based on the SCRM Incident Management playbooks.

These playbooks create a predefined reference for bringing together the Customer Value Chain Management (CVCM) organizational leaders to assess, mitigate and resolve a disruptive supply chain incident. The playbooks define a functional track structure, key contacts related to various types of incidents, templates and other collateral to assist in running and managing an incident response. Through these playbooks and the overall SCRM incident management process, CVCM was able to very quickly mobilize and get out ahead of the crisis from a mitigation and customer communication standpoint.

Bottom Line: In a very short period, the crisis management system was able to assess more than 300 Tier 1–Tier 5 suppliers — including site inspections and more than 7,000 part numbers — and complete a risk rating and mitigation plan. And, the largest supply chain disruption in modern times created virtually no revenue impact for the company.

Key Lessons Learned

- Information and visibility is the backbone of a major incident response. When a crisis hits, it is extremely important to have the systems and processes in place that can assist with understanding and assessing the situation. In Cisco's case, this included quickly understanding who has been impacted (supply chain nodes), how this impact affects Cisco (components/products/customers/revenue), and what recovery path to pursue (2nd and alternative source availability, TTR). Each of these questions were addressed through the BCP capability and data. Utilizing the output of this program allowed Cisco to focus on mitigation rather than scrambling for visibility in the early stages of the incident and accelerated overall time to results.

- Incident preparation and process are non-negotiable for success. Given the scale of the impact and the velocity of the evolution of the threat, Cisco's response involved every part of the Supply Chain Organization across 100+ people. Without a structured response process and an extended team that is trained in how this process is utilized, Cisco would have spent valuable time in the early stages of the incident just to form a functional response team. Anecdotal evidence from discussions across a wide variety of industries indicated that Cisco, from a response standpoint, was functioning at a level within 2 days that took many companies over 2 weeks to accomplish. The SCRM Incident Management Playbooks, in conjunction with drills, training sessions and incident postmortems, creates a level of preparedness that allows Cisco to get out in front of any type of supply chain disruption quickly and effectively regardless of its nature and scale.

- It is important to quickly identify and manage your "unknowns" during an incident. There is really no way to have infinite information and visibility into impacts from a crisis, nor is it possible to anticipate and prepare for every potential threat situation. Information and preparedness are investments, and at a certain point a balance must be found. It is possible, however, to at least identify and recognize key gaps. Proactive knowledge of these key gaps is important such that resources can be prioritized early in a response. For Cisco, the key gap was visibility into sub-tier supply chain (suppliers that supply Tier 1 component manufacturers). Having this as a "known unknown" was critical to quickly resourcing a team to investigate key impacts and ramifications in this area and to mitigate where possible.

- Communication is crucial. A structured communications plan is, in many ways, just as important as the actual incident response management program. For Cisco, communications is the key interface with customers who need to have information regarding the status of their orders and an incident's overall impact to the continuity of their order pipeline. Internal stakeholders, including sales, marketing, engineering and the business units that own the P&L need answers as well. A successful communications program will provide consistent and appropriate messaging in a timely fashion based on what is known from the incident response. Having a dedicated communications team embedded in an incident response program is a necessary element of making communications successful.