MICHIGAN
ROSS SCHOOL OF BUSINESS

WDI PUBLISHING

case 1-428-881
July 17, 2012

Supply Chain Risk Management at Cisco: Response to H1N1

Our customers, partners, and shareholders all rely on our ability to maintain business continuity regardless of world events, economic challenges, or unforeseen events.

—John Chambers, Chairman and CEO, Cisco Systems, Inc.[1]

It was October 8, 2009. Kevin Harrington had just come out of a meeting with his boss, Angel Mendez, senior vice president of Cisco's Customer Value Chain Management (CVCM) organization. Mendez was particularly concerned about whether Cisco was sufficiently prepared for a pandemic flu in the coming autumn, especially in Asia. The last such outbreak—severe acute respiratory syndrome (SARS) in 2002–03—had practically paralyzed businesses in Asia. "What contingency plans do we have in case of a full-blown pandemic this fall? Will we be able to continue to meet our customer demand?" he asked Harrington. Cisco has a significant presence in the China and Taiwan, with several manufacturing locations, demand fulfillment centers, as well as tier 1 and tier 2 suppliers from this region (see **Exhibit 1**).

As the vice president of global business operations in Cisco's CVCM organization, Harrington was ultimately responsible for ensuring that Cisco's extended supply chain was able to maintain continuity of supply. The H1N1 virus, originating in March 2009 with a few cases of the flu identified in North America, quickly spread eastward through Europe toward Asia, causing a great deal of concern about the risks it posed to human life as well as to business continuity. Fortunately, there had been very little disruption to Cisco's extended supply chain up until this point. However, the World Health Organization maintained a heightened state of alert and was preparing for a full pandemic beginning in June 2009.[2]

In early spring, as the virus broke, it was unclear if there was anything unusual about it. Not until April did the US Center for Disease Control and Prevention (CDC) and the World Health Organization (WHO) determine that this virus appeared to be a new strain that could potentially reach pandemic proportions. Unlike the regular virus, H1N1 did not affect the elderly disproportionately. A small percentage of previously healthy adults could develop viral pneumonia or acute respiratory distress syndrome, which manifested itself as increased breathing difficulty and typically occured three to six days after initial onset of flu symptoms. As the virus spread, response from countries varied. In early spring, Mexico briefly shut down all business

Published by WDI Publishing, a division of the William Davidson Institute (WDI) at the University of Michigan.

 This case was written by Ravi Anupindi, Professor of Operations and Management Science at the University of Michigan's Ross School of Business. He thanks the SCRM Team at Cisco for their support.

operations. In May, the United States shut more than 430 schools across 18 states. Hong Kong quarantined several guests in one of its hotels; later China briefly suspended flights between Mexico and Shanghai. By the end of summer, the WHO reported 163 deaths.[3] Vaccine development for this strain was in full swing but it was unclear whether one would be available by fall 2009.

Cisco Background

Cisco Systems Inc. was founded in 1984 by Leonard Bosack and Sandra Lerner, two computer scientists from Stanford University, with the "router" – a traffic cop for data on the Internet – as its primary product. The company shipped its first product in 1986 but remained in financial trouble in its early years. In 1988, Don Valentine, a partner in Sequoia Capital, invested in Cisco. To protect his investment, he negotiated the right to bring in outside management. Subsequently, he appointed John Morgridge as the CEO, who brought professional management to Cisco. In 1990 the company went public. By 1994 Cisco's revenues exceeded $1 billion for the first time. In 1995, Morgridge became chairman and hired John Chambers as the next CEO. Cisco Systems showed phenomenal growth under Chambers' leadership.

Headquartered in San Jose, CA, Cisco became the worldwide leader in networking for the Internet. Cisco offered a broad range of products and solutions in such categories as networking systems, data centers, collaboration voice and video, mobility/wireless, and security. Moreover, it maintained market leadership in all of these segments. Cisco focused on delivering networking products and solutions that simplified and secured customers' network infrastructures.

The organization conducted its business globally and was managed geographically in five segments: United States and Canada, Europe, emerging markets, Asia Pacific, and Japan. Cisco's customer base spanned virtually all types of public and private agencies, businesses, service providers, and consumers. In fiscal 2009 Cisco recorded $36.1 billion in revenue, boasted a market capitalization of $109 billion, and employed more than 65,000 people in 140 countries (see **Exhibit 2** and **Exhibit 3**).[4] According to Chambers:

> Cisco's strategy is based on catching market transitions — the market transitions that affect our customers. With the proliferation of video and collaborative Web 2.0 technologies, the network continues to evolve from the plumbing of the Internet — providing connectivity — to the platform that will change the way we work, live, play, and learn."[5]

To execute its strategy, Cisco ran one of the most complex supply chains in the global IT industry, with more than 1,000 suppliers, four contract manufacturers, and 50,000 purchased parts supporting more than 12,000 products and over 200 major product families. Cisco's supply chain relied heavily on outsourcing. Component production was outsourced to Cisco's suppliers, and the components were assembled into products at contract manufacturing locations. Furthermore, Cisco's active M&A culture resulted in over 130 acquisitions, so the supply chain had to constantly adjust to integrate its new members. With this complexity, managing relationships with customers, suppliers, contract manufacturers, and newly acquired firms was a complex, demanding, and ongoing process.

Supply Chain Risk

Global supply chains face risks from natural events (e.g. earthquakes, fires, floods, pandemics, etc.), man-made events (e.g. acts of terrorism), financial crises, geopolitical events and more. These risks potentially inhibit a company's ability to satisfy customer demands in a cost-effective manner, sometimes resulting in severe financial consequences. In 1997, for example, Toyota halted production for 20 days after

a single supplier failed to provide promised components as a result of a fire. The Aisin Seiki Co. plant that was destroyed by the fire supplied brake proportioning valves for every Toyota model except two, forcing the automaker to shut down its 18 assembly plants in Japan due to lack of parts. The slowdown in production following the disruption cost Toyota approximately $195 million, representing 70,000 units of production.[6]

In 2000, a fire caused by lightning seriously damaged an electronics component plant in New Mexico. The plant was operated by Philips and supplied both Nokia and Ericsson – at the time two leading players in the cell phone business. Nokia reacted promptly to secure available components, thus minimizing the disruption caused by the supplier failure. Ericsson, however, was late to respond and unable to produce the promised products, which translated into direct losses in sales over $390 million.[7]

A research study by Kevin Hendricks and Vinod Singhal reported that in the year leading up to a supply chain disruption, firms experienced a 107% drop in operating income (profit), a 114% drop in return on sales, a 93% reduction in return on assets, and 6.9% lower sales growth relative to a control group of firms of similar size in similar industries. They observed that these numbers did not improve for two years after the announcement.[8]

Evolution of SCRM at Cisco

While 9/11 did not significantly impact Cisco's business operations, it did raise the alert level and brought new focus on the risks pertaining to Cisco's widely distributed global supply chain. In 2002, Cisco initiated business continuity planning (BCP) within its manufacturing facilities team that primarily focused on its manufacturing partners and quality issues in the supply chain. By late 2005-early 2006, BCP activities had been moved to Cisco's Supply Chain Architecture team, which developed a patented risk engine that later underwent considerable development. With the reorganization of Cisco's manufacturing group in 2006, the supply chain architecture team evolved into the Supply Chain Risk Management (SCRM) team. In the October 2006, Cisco launched the Supply Chain Risk Leadership Council to bring together leading practitioners of supply chain risk management to understand best practices.

The SCRM team learned some important real-world lessons on December 26, 2006, when the Hengchun earthquake struck in Taiwan, with an epicenter off Taiwan's southwest coast, approximately 22.8 kilometers west-southwest of Hengchun, Pingtung County, Taiwan. The earthquake's magnitude was recorded as 6.7.[9] Taiwan's Central News Agency reported that it was the strongest earthquake to hit Hengchun in one hundred years. The earthquake not only caused casualties and building damage, but also damaged several undersea cables, disrupting telecommunication services in various parts of Asia. When the vice president of manufacturing asked the SCRM team for the potential revenue impact of the earthquake on Cisco, the team could not give an estimate. This triggered the team to expand its initial BCP efforts to include complete mapping of all nodes in the global supply chain—manufacturing, transportation, component suppliers, etc. The team also began to reach out for more information to industry peers and experts facing similar issues around the world.

Cisco's Supply Chain Risk Management Framework[10]

The SCRM team was responsible for ensuring that Cisco had the most resilient supply chain in the industry – ensuring that Cisco could respond more quickly than any of its competitors in the event of an operational or catastrophic disruption. Cisco's SCRM team attempted to do this by incorporating resiliency requirements into the design and release process of new products, as well as by driving product and supply chain risk resiliency for sustaining products. The team pioneered an approach to managing supply chain

risk by defining ways to anticipate and measure risk, building a standards-based BCP program that actively measured and improved recoverability, and by developing and executing resiliency programs at the product and supply chain levels. Cisco developed an SCRM process framework, engagement models, metrics, and tool sets with the common goal of being best in class in all these areas.

SCRM resided within the Global Business Operations organization headed by Kevin Harrington. His responsibilities included developing Cisco's capabilities in business planning, business operations, leadership and people, and supply chain enablement (see **Exhibit 4**). Reporting to Harrington, John O'Connor, director of global supply chain management, was responsible for the SCRM program. The core SCRM team consisted of Joe McMorrow, Lance Solomon, Jane Khoury, Bindiya Vakil, Maalika Manoharan, Tam Quach, Komal Chandiramani, and Mohammad Salimi.

SCRM consisted of the following five key elements:

1. Business Continuity Planning
2. Crisis Management
3. Product and Supply Chain Resiliency
4. Risk Analytics
5. Design for Resiliency

Business Continuity Planning

Business Continuity Planning (BCP) focused on Cisco's suppliers, electronic manufacturing services partners, and transportation and logistics providers to document recovery plans, speed recovery times, and drive resiliency standards. Cisco's BCP program identified critical business processes, resources, and systems within the supply chain and assessed the time-to-recover (TTR) for each. TTR was based on the longest recovery time for any critical capability within the supply chain, and was a measure of the time required to restore 100% output at that node following a disruption. Cisco's BCP program was unique in that Cisco was able to build a BCP dashboard with data that played two key roles: (1) it was used by the crisis management team to assess the impact of any disruption and (2) it illuminated vulnerabilities in the supply chain that Cisco could then mitigate.

The continuity program at Cisco had two main areas of focus: external, which concentrated on Cisco's suppliers, contract manufacturers, and logistics partners, and internal, which focused on Cisco's people and internal applications critical to the supply chain.

External Business Continuity Planning: On a semi-annual basis, Cisco collected data on its top suppliers and partners from around the world via a formal process. Approximately 95% of Cisco's production was outsourced. Cisco had hundreds of suppliers producing components at thousands of sites around the world, several partners assembling and testing the products, and logistics service providers moving the components and products. In order to monitor the supply chain, Cisco first attempted to identify the global footprint of its suppliers and partners. The SCRM team then evaluated supplier and site resiliency through an elaborate data collection process. The data collected from suppliers and partners included their emergency contact information, addresses of primary sites, alternative manufacturing locations, and information related to part-recovery mapping. The suppliers and partners were also required to answer questions related to their site's resiliency in accordance with Cisco's BCP standards, which included questions related to the supplier's site TTR after a catastrophic disruption.[11]

A guiding principle for the SCRM team at Cisco was that data was valuable only if it was accurate. The SCRM team understood that the suppliers might at times try to provide information that "Cisco wants to hear," and a key challenge was making sure the data was reliable. Cisco tried to ensure supplier's information was as accurate as possible by including clear language in the survey that communicated that the supplier would be held accountable for the accuracy of the information provided; the survey also pointed out that the information was contractually binding. In addition, the SCRM team conducted drills and audits in order to ensure that the data provided by the suppliers was accurate and up to date (see **Appendix 1**).[12]

Cisco recognized that suppliers varied in their maturity level on BCP standards. While some might have robust BCP programs in place, others might not have any. The SCRM team helped suppliers put together effective BCP programs and become better prepared for a major disruption. Cisco created a best-practice guide that assisted suppliers in understanding the importance of each of Cisco's BCP assessment standards and provided the suppliers with templates and resources to start heading in the direction of resiliency (see **Appendix 2**).[13]

The BCP information collected on various suppliers was utilized across multiple departments at Cisco. The suppliers entered their responses to surveys via a BCP data collection tool and the information was then automatically transferred into Cisco's secure BCP dashboard (see **Exhibit 5**). The appropriate Cisco staff at various departments could filter the information in the BCP dashboard by fields that included supplier name, supplier location, TTR, type of supplier, etc. Combined with supply chain mapping capability and bill of materials explosion, it allowed Cisco to reveal critical information to appropriate stakeholders at the moment of truth (see **Exhibit 6**).[14]

Internal Business Continuity Management, referred to simply as BCM, focused on Cisco's internal applications and human resources critical to the supply chain. Cisco's processes were embedded in its internal applications. Therefore, BCM at Cisco started with a business impact assessment that identified critical applications. Then objectives for recovery point and time were established for each critical application. The recovery point objective was the amount of time that an application could be down before it affected Cisco's revenue. The recovery time objective answered the question of how much data could be lost from a critical application without significantly impacting Cisco's revenue. Finally, an application recovery plan was created that outlined the process of recovery for each critical application in the event of a crisis. The IT staff at Cisco was responsible for documenting the application recovery plans.[15]

Ultimately, it was the people that determined the effectiveness of the supply chain. The analysis of the critical roles in the supply chain was an essential component of internal business continuity preparation. The process identified roles in Cisco that were vital for revenue generation. Furthermore, an analysis was conducted to see if critical positions had designated backups, and if the primary employees and their backups had the capability to work from home. Cisco considered pandemic planning as a vital part of protecting the people and processes involved in supply chain operations.[16]

Crisis Management

Cisco's SCRM team was responsible for monitoring disruptions globally on a 24/7 basis. If a disruption was potentially impactful to Cisco's supply chain, the SCRM team used the BCP dashboard to quickly conduct an impact assessment—assessing what supply chain nodes were in the affected region, what parts and/or products were made within the affected area, what alternate and/or fail-over sites should be engaged, and what customers and revenue might be impacted. The SCRM team then engaged a broad cross-functional

team to execute response playbooks that had been tailored to the disruption type, location, and anticipated duration.[17]

A typical crisis lifecycle had the following stages: warning, assessment, response, management, resolution, and recovery (see **Figure 1**).[18]

Warning

The crisis manager on the SCRM team was responsible for keeping aware of what was happening around the world. Cisco utilized an external service provider to receive relevant notifications of certain events. The supplier locations collected in the BCP surveys were mapped out, and whenever a Cisco-specified event occured in close proximity to a node or link in its supply chain, Cisco's SCRM team was notified via a global event monitoring service (see **Exhibit 7**).

In addition, the SCRM team utilized an event dashboard to collect intelligence from multiple sources in order to quickly learn if any events around the world might be a threat. Events were recorded on the crisis dashboard (middle section of **Exhibit 8**), and a mapping capability (lower section of **Exhibit 8**) allowed Cisco to see all affected locations.[19]

Figure 1
Crisis Lifecycle

Source: McMorrow, Joe. program manager, Supply Chain Risk Management, Cisco Systems, Inc., unpublished Cisco document, 2009.

Assessment

The assessment phase determined the potential impact of an event to Cisco. Assessment encompassed impact on nodes and links in the supply chain, products, and revenues. A comprehensive assessment was completed in partnership with affected suppliers, partners, and customers. If it was determined that an event was of serious concern, it was moved to an incident category (top section of **Exhibit 8**).[20]

Response

Depending on the nature of the event and the impact it could have, different levels of Cisco's crisis engagement structure were activated; these levels corresponded to corporate, geographic, and functional areas, as well as teams to handle "one off" incidents. Once it was determined that the event could have serious consequence, crisis management teams at appropriate levels engaged a broad cross-functional team to execute response playbooks which had been tailored to the disruption type, location, and anticipated duration.[21]

Management

If it was decided after further monitoring that the incident presented serious danger to the supply chain, the incident was labeled a crisis. A manufacturing crisis management team (MCMT; see **Exhibit 9**) was assembled and activated to deal with the crisis. The membership of the crisis management team varied based on the type of crisis and the region impacted. For example, for a regional disruption such as a hurricane, team members would represent the impacted functions of manufacturing, logistics, transportation, and component supplier operations. A more localized disruption could impact a specific building and would require a much smaller team to manage the crisis. After a crisis had been declared by Cisco, the MCMT assumed control of the situation and became the sole source of information to customers, suppliers, partners, and employees. The MCMT was also responsible for coordinating and communicating with the crisis management teams at the corporate level.[22]

Resolution and Recovery

The crisis management team met as required until the situation was resolved. All the information related to the crisis was posted on an internal dashboard, available to all the crisis management team members around the world. A situation was considered resolved once the supply chain had a clear path to recovery. After the situation was resolved, the recovery stage could last as little as a few hours or as long as many weeks. The recovery stage was complete once operations returned to normal capacity.[23]

Product and Supply Chain Resiliency[24]

Cisco's product resiliency program focused on components and suppliers of components, and its supply chain resiliency focused on manufacturing partners, test equipment, logistics providers, and other nodes in the supply chain. Regardless, resiliency entailed risk assessment and mitigation.

Product Resiliency

The product resiliency program had three main elements: component risk assessment and prioritization, supplier risk assessment, and risk mitigation. Cisco's Global Component Risk Management program had the responsibility to mitigate the risks associated with the components inside Cisco's products. Components and suppliers together influenced the resiliency profile of a product. The program consisted of a cyclical process to identify risky components, prioritize parts to mitigate, identify appropriate mitigation strategies for different parts, and review mitigation completion.

Component Risk Assessment and Prioritization

Cisco used three factors to determine the overall riskiness of a component. Single-sourced components were considered more risky than multiple-sourced components. As part of the BCP process, suppliers provided TTR data that specified how long it would take the supplier to recover at an alternate site, should the primary site suffer from a major failure. The length of TTR beyond a predetermined threshold determined the degree of risk associated with a part. A final risk consideration was the revenue impact that would result if production of a certain component were disrupted.

Using the three factors, high-risk components were identified. The next step consisted of prioritizing the identified high-risk parts to be mitigated. Cisco considered the following factors in its prioritization efforts:

- Product – Risk mitigation for all parts that went into the top 100 products.
- Revenue – Risk mitigation for components that had the highest revenue impact because they were used across a wide variety of Cisco products.

- Geography – Risk mitigation for high-risk areas prone to natural disasters.
- Customers – Risk mitigation for products utilized by high-priority customers.

Supplier Risk Assessment

In parallel, Cisco made an assessment of supplier risk using a two-pronged approach. The global supplier management team first developed an approved vendor list of all suppliers approved for a certain part. The team then classified suppliers as either "preferred" or "non-preferred" using considerations such as technology, operational flexibility, metrics (quality, TTR, etc.), BCP compliance to Cisco standards, and financial capability. Sourcing was usually restricted to preferred suppliers unless there was a technology dependency situation. In that case a non-preferred supplier might be used. In addition, with assistance from supply chain finance, a periodic financial due diligence of suppliers was conducted and suppliers categorized as either "red," "yellow," or "green."

Based on the assessment of component risks (using the several prioritization criteria) and supplier risks, mitigation decisions were made. For example, suppliers classified as "red" were always mitigated and "yellow" suppliers were put on a monitor list. While "green" suppliers were financially healthy, their need for mitigation depended on the level of risk of the components they made; if the component made by a "green" supplier was considered high risk, then a mitigation action was taken.

Risk Mitigation Strategies

Risk mitigation strategies were tailored to the type of risk the product faced. Some of the more frequent product risk mitigation strategies included:

- Dual sourcing – ensuring there were at least two sources of supply for certain components.
- Alternate site qualification with same supplier – making sure suppliers were able to produce their components from more than one location.
- Inventory buffer – maintaining the products or supplies in storage or in transit to stabilize variations in supply, demand, production, or lead time. Buffer mitigation strategy also entailed determining where the buffer should be held (at a Cisco distribution hub or manufacturing site), determining the size of buffers, negotiating a letter of intent, getting approvals, and executing and performing periodic reviews.
- Last time buy – If a part could not be second sourced, then an internally generated last time buy was initiated. This notified the appropriate business unit to determine the lifetime demand for the component based on the products that used it, source the appropriate inventory, and place it at a hub location.
- Contractual mitigation (manufacturing rights agreements)—For certain commodities, where second sourcing or last time buy were not feasible, Cisco implemented a manufacturing rights agreement with the affected supplier under which the supplier agreed to let Cisco take control of its operations with its subcontractors if the supplier's financials hit certain predefined trigger conditions.
- Standardization – Cisco could establish common criteria, terms, principles, practices, materials, items, processes, equipment parts, and components. Standardization allowed Cisco to design resilient processes and products.

Supply Chain Resiliency

Cisco's supply chain resiliency program worked closely with Cisco's manufacturing operations, manufacturing partners, logistics and transportation providers, inventory hubs, and order consolidation centers to identify nodes with recovery times that were outside Cisco's established TTR tolerances and to develop resiliency plans.

Cisco validated the actual TTR by comparing it to the TTR provided by the contract manufacturers in the BCP data collection process. Gaps were identified and an analysis conducted to see if the TTR was in line with Cisco's goals and requirements. Cisco also looked to identify alternate sites by product family. The alternate site then underwent a qualification step whereby Cisco validated whether there were available backup sites capable of producing products during disruptions at primary manufacturing sites. As necessary, capacity reservations or allocation priorities were negotiated with the contract manufacturer or inventory buffers were established.

Testing was a critical step in Cisco's manufacturing operations. Cisco provided the contract manufacturers with the necessary specialized test equipment, while the contract manufacturers were responsible for running the tests and maintaining the equipment. Making sure the contract manufacturers were using properly functioning test equipment was critical for ensuring Cisco's products were of the highest quality, and this step was taken very seriously. With this in mind, as with other critical parts of the supply chain, a TTR analysis for the test equipment was conducted. Mitigation plans included negotiating a replacement lead time agreement with test equipment suppliers to be within Cisco's TTR goal, developing alternate test infrastructure, or investigating a buffer mitigation strategy. In case of a catastrophic event, Cisco either provided the contract manufacturers with replacement equipment within the established TTR goals, or worked with other Cisco departments to develop a new test infrastructure.

Business interruption insurance covered Cisco's lost profits during a disruption. Cisco utilized the expertise of insurance providers to conduct an analysis of facilities in its supply chain to advise Cisco on which facilities were most vulnerable and what improvements should be made based on a risk versus cost tradeoff.

Risk Analytics[25]

Cisco's supply chain risk management was supported by strong risk analytics, a process of gathering, modeling, and transforming data with the goal of highlighting useful information, suggesting conclusions, and providing support for key SCRM programs and initiatives. Risk engine and resiliency scorecard were two of the main components of the risk analytics program.

Risk Engine

Cisco developed a "risk engine" which incorporated many data sets—including 100-year flood data, actuary data, geological and geopolitical data, incident data on specific locations, and data on suppliers' past performance—to assess the likelihood of a disruption (see **Exhibit 10**). These disruptions were correlated to Cisco supply chain locations including the supplier sites, contract manufacturing facilities, and logistics centers. The impact of a disruption was determined based on the revenue enabled by each node in the supply chain and that node's TTR. A quantity called revenue at risk was determined; it equaled the revenue times the TTR. Cisco used simulation capabilities to integrate all of this information into a single model that generated "heat maps" based on likelihood of impact (see **Exhibit 10**).

Resiliency Scorecard

To demonstrate Cisco's supply chain resiliency as well as show progress with mitigation efforts and be able to compare it across different products, Cisco developed a resiliency scorecard. The scorecard was made up of four key Level 1 categories: component, supplier, manufacturing, and test resiliency. Component resiliency score measured how resilient were the components that went into the specific product or set of products. Supplier resiliency score measured the resiliency of the suppliers responsible for producing the components. Manufacturing resiliency score measured the resiliency of the contract manufacturers, and test resiliency measured the resiliency of the test equipment (see **Exhibit 11**).

Scorecards were used to measure risk using an executive level metric that was standardized across products, business units, and customers. As of 2009, a resiliency scorecard was generated for:

- Top five business units for sustaining products, with the scorecard based on the given set of products from each unit, within the top 100 revenue generating products for Cisco's entire product portfolio. This maintained focus on resiliency for the highest revenue products with a trickle-down effect to lower revenue products from the same business unit.
- New products within a business unit that had $10 million in projected revenue per quarter at peak volume.

Design for Resiliency

The SCRM team realized that mitigation strategies such as building up an inventory buffer were very important, but they could be expensive and sometimes did not provide long-term protection. In order to truly impact a product's resiliency, it was important for the team to be involved from the beginning of a product's life cycle in the product design stage, when decisions about components and suppliers were being made. The SCRM team became actively engaged with colleagues responsible for selecting components and suppliers for future products. It hoped to utilize its expertise to advise co-workers on selecting components and products with resiliency in mind.

H1N1 Outbreak and Cisco's Response: A Drill[26]

Kevin Harrington and his supply chain director, John O'Connor, met to discuss Harrington's meeting with his boss Angel Mendez. Harrington articulated Mendez's concern to O'Connor. While O'Connor was confident that his team was fully prepared for such a pandemic, he knew the team had never been fully tested before. The continued unfolding of events with an unknown cause for the H1N1 virus and potential to spread worldwide was disconcerting. He thought that a drill mimicking his team's response to a potential outbreak in fall 2009 would be very useful and also build some confidence among the Cisco senior management in his team's ability to handle the situation. Subsequently, the SCRM team went through a drill that unfolded as follows.

H1N1 Drill Timeline

Thursday, October 15, 2009:

China: The government of China notifies a regional arm of the World Health Organization (WHO) of an unusual increase in the number of cases of acute respiratory infections in the Guangdong Province, Beijing, and Shanghai.

Wednesday, October 21, 2009:

China: The Chinese minister of health Chen Zhu declares the country has a crisis in a form of an influenza epidemic.

Friday, October 23, 2009:

Global: World coverage of the epidemic in China begins.

China: The Chinese health minister announces that schools and universities in Guangdong Province and the surrounding area will be temporarily closed. The health minister also advises people with flu symptoms to stay home from work.

WHO: The World Health Organization announces that it is calling an emergency committee meeting to decide whether the outbreak of swine flu in humans in the southern United States and in China constitutes an international public health threat.

Cisco: A manufacturing crisis management team (MCMT) is assembled, alerted, and placed on standby. A monitor-only incident is created, and an initial risk assessment kicked off with key organizations in the supply chain.

Sunday, October 25, 2009:

Cisco: The MCMT is activated. The SCRM team is charged to conduct a detailed risk assessment to understand possible impact and be prepared to discuss mitigation strategy on Monday. The MCMT's initial risk assessment includes the following:

1. Internal BCP (Responsibility: Jane N. Khoury)
    - Previously collected data utilized to conduct an assessment in order to identify critical applications related to the spread of the influenza. The importance of each related internal application and interdependencies between the applications analyzed.
    - Process dependencies and potential business impact of related internal applications studied.
    - Formerly collected information on critical job roles and trained backups gathered; customized analysis related to the swine flu outbreak carried out.
    - Various recovery related processes prioritized.
2. External BCP (Responsibility: Khoury)
    - Supply chain global footprint of related supplier sites and contract manufacturers (see **Exhibit 1**) pulled up via Google Earth and internal crisis dashboard.
    - Supplier and contract manufacturer importance for recovery prioritized.
    - The on-file BCP assigned contacts for the priority suppliers and contract manufacturers organized.
    - Updated pandemic plans from suppliers and contract manufacturers requested.
3. Product/Supply Chain Resiliency (Responsibility: Lance Solomon and Bindiya Vakil)
    - Inventory of components produced in the impacted region analyzed.
    - Orders on the horizon for the manufacturing sites in the region pulled up and the revenue tied to those orders calculated.
    - Current product assembly sites and potential alternative contract manufacturer locations scrutinized.
    - TTR to alternate locations for possibly impacted products probed.

- Revenue exposure associated with products or components produced in the influenza breakout region examined.

Monday, October 26, 2009:

China: Chinese minster of education announces all classes will be closed until November 6, 2009.

Cisco:

- MCMT meets for a briefing on the situation and to discuss the results of the initial risk assessment.
- The materials managers at particular facilities analyze whether the inventory levels are high enough to build ahead; extra orders are placed for products built/shipped in China. A decision is made to allow certain facilities to work maximum overtime and build-ahead/ship-ahead in order to build up inventory and create a buffer to minimize impact of possible plant closure.
- Cisco starts a comprehensive communication plan. MCMT members begin contacting suppliers and manufacturing partners in order to find out the status of their operations and whether they have been impacted by the swine-flu outbreak.
- Cisco leverages its industry contacts within the Supply Chain Risk Leadership Council (see **Exhibit 12**) to conduct a real-time cross-industry best practices sharing in response to the swine flu crisis.

Tuesday, October 27, 2009:

WHO: The organization raises alert to Phase 4 (see **Appendix 3** for WHO's six-phased approach to pandemic alert system).

Cisco:

- A "refresh" of critical roles within Cisco carried out. Examination conducted for the purpose of understanding critical functions, region, trained backups, and work from home capabilities.
- Continuation of previous MCMT activities.

Wednesday, October 28, 2009:

WHO: Alert raised to Phase 5.

Cisco: Continuation of previous MCMT activities.

Thursday, October 29, 2009:

China: To stop spread of virus, the Chinese government recommends that all businesses close for five days, suspends government services, and tells the public to stay home.

WHO: The organization says it will stop using the term "swine flu" to avoid confusion over the danger posed by pigs; use of "H1N1 influenza A" is recommended.

United States: The Obama administration announces that the air traffic corridor between China and the US will remain open.

Cisco:

- The company decides to close its Guangzhou site until November 2, as the risk assessment showed there was enough inventory to shut down the site without impact on revenue.

- Upon further investigation it appears that while there seem to be serious outbreaks in Guangzhou other cities in the region do not have a single outbreak. The SCRM team begins to pay less attention to the WHO phases and more attention to the city-by-city situation.

Friday, October 30, 2009:

China: By evening, China's government adjusts its previous message and makes it clear that the recommendation to shut down businesses is simply a recommendation and that firms will not be held legally liable for not following the recommendation.

Tuesday, November 3, 2009:

WHO: The alert level remains at Phase 5.

China: President Hu JinTao announces that full economic activity will resume Thursday, November 5. He also says universities and high schools will resume activities starting November 9 and elementary schools will resume classes November 12.

Chinese authorities realize that, overall to this point, the H1N1 outbreak has not been as deadly as some experts believed. Based on the data collected around the world, they point out that the mortality rates for H1N1 are no worse than for the common flu. Consequently, the flu alert is lowered in Guangzhou as Chinese officials say the threat has leveled off. There is news that the virus has spread to Taiwan as the first confirmed case in South Asia, where the flu season is about to begin.

Cisco:

- Given the most recent information that suggests activities in China are returning to normal, Cisco instructs suppliers and contract manufacturers to plan for no more than a two-week disruption for components and materials procured from China. Overtime and build-ahead/ship-ahead are discontinued.
- The MCMT team deactivates and resumes monitor-only activity.

Friday, November 6, 2009:

Cisco: Initial post-mortem; team members meet to discuss the key learning takeaways.

Thursday, December 10, 2009:

WHO: Alert raised to Phase 6. H1N1 labeled a pandemic, meaning that its spread is unstoppable.

Thursday, January 14, 2010:

WHO: The organization says it is no longer counting individual cases of H1N1 as the pandemic continues to spread.

Continued State of Alert

While it appeared that the impact of the initial H1N1 outbreak was contained, WHO kept its alert level at Phase 6, the first such pandemic designation in 41 years.[27] While detection of new cases would fade as warmer weather arrived, government and business leaders around the world stayed alert to a likely resurgence during the peak flu season that usually arrives in the fall season in the Northern Hemisphere.

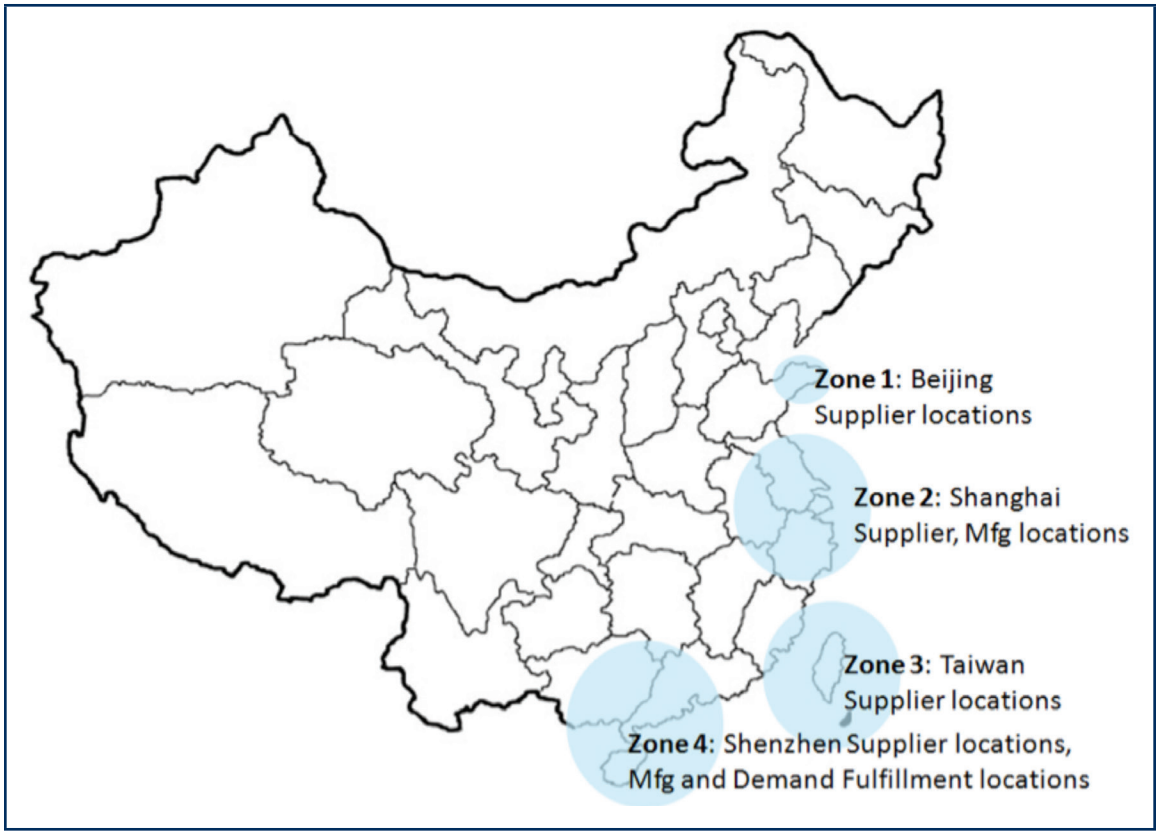
The actions taken in response to the H1N1 drill led the SCRM team to take a closer look at other risks related to Cisco's businesses in other parts of the word. For example, Cisco's deepening engagement with

Mexico reflected the increased importance the company was placing on the globalization of its business and its expansion into developing economies. In 2008, Cisco identified Mexico as one of the top emerging markets where potential existed for rapid business growth in the company's information and communications technology. In addition, Cisco saw the opportunity to expand on its already strong presence in Mexico.

Cisco employed almost 7,000 people in the country, most of them working at a major factory in Ciudad Juarez producing video and cable TV equipment for the global market, and others at sales offices in Mexico City, Guadalajara, Ciudad Juarez, Monterrey, and San Pedro Garza Garcia. Cisco also had strategically important outsourced supply chain operations in Mexico, including several dozen supplier and partner sites throughout the country (see **Exhibit 13**). However, the gulf region in Mexico faced the potential risks of hurricanes. Hurricanes also had the potential to impact Cisco operations in the United States. The SCRM team wondered if the company was sufficiently prepared for disruption by such storms. Based on the BCP data, Jane Khoury identified key partners and suppliers in the region (see **Exhibit 14**). Lance Solomon got the SCRM team together to brainstorm pre-emptive actions it could now take, and how to maintain continuity of supply if a hurricane hit a critical region.

Exhibit 1

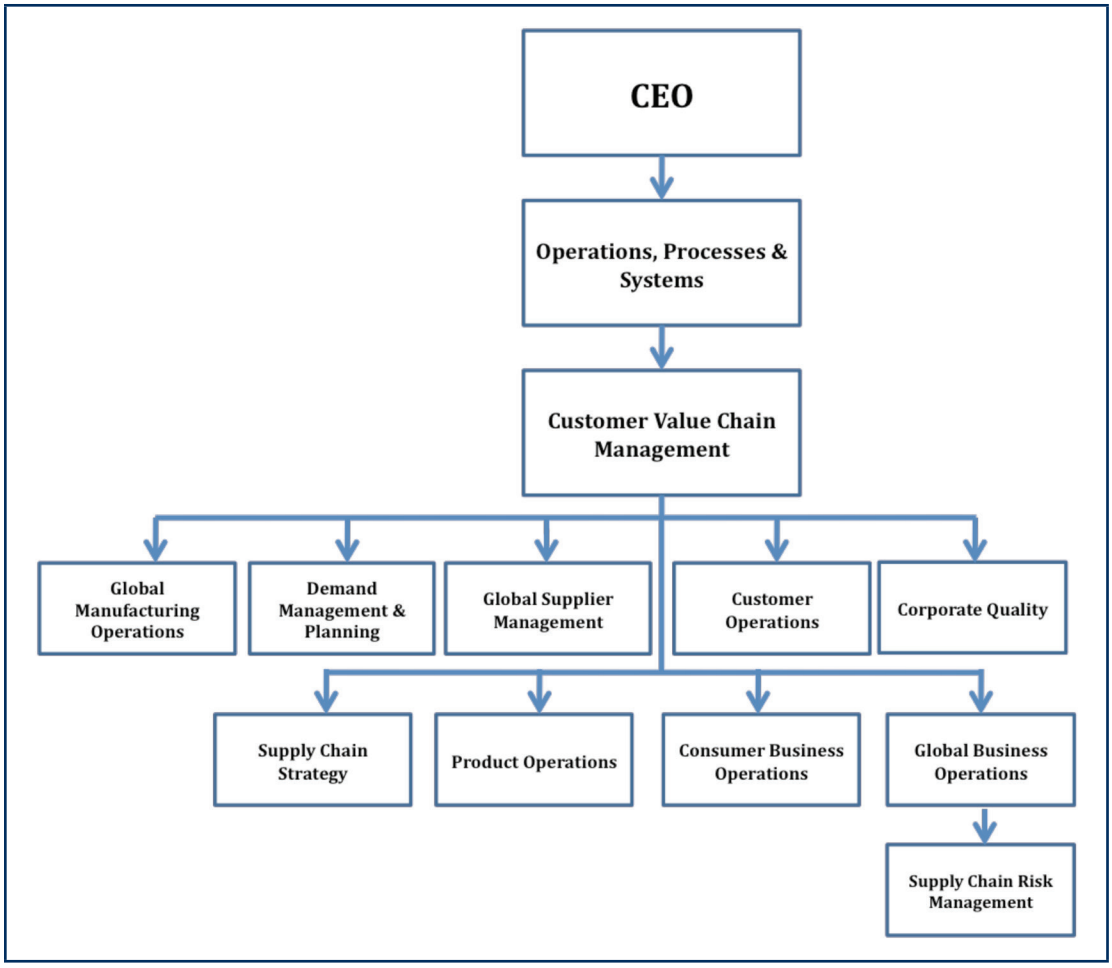
Cisco's Supply Chain Footprint in China and Taiwan



Source: Unpublished Cisco Systems Inc. internal document, 2009.

Exhibit 2

Cisco Organization Chart



Source: Unpublished Cisco Systems Inc. internal document, 2009.

Exhibit 3

Cisco's Financials

Consolidated Statements of Operations
(in millions, except per-share amounts)

Years Ended	July 25, 2009	July 26, 2008	July 28, 2007
NET SALES:			
Product	$ 29,131	$ 33,099	$ 29,462
Service	6,986	6,441	5,460
Total net sales	36,117	39,540	34,922
COST OF SALES:			
Product	10,481	11,660	10,567
Service	2,542	2,534	2,096
Total cost of sales	13,023	14,194	12,663
GROSS MARGIN	23,094	25,346	22,259
OPERATING EXPENSES:			
Research and development	5,208	5,325	4,598
Sales and marketing	8,403	8,690	7,401
General and administrative	1,565	1,387	1,151
Amortization of purchased intangible assets	533	499	407
In-process research and development	63	3	81
Total operating expenses	15,772	15,904	13,638
OPERATING INCOME	7,322	9,442	8,621
Interest income (expense), net	499	824	715
Other income (loss), net	(128)	(11)	125
Interest and other income, net	371	813	840
INCOME BEFORE PROVISION FOR INCOME TAXES	7,693	10,255	9,461
Provision for income taxes	1,559	2,203	2,128
NET INCOME	$ 6,134	$ 8,052	$ 7,333
Net income per share—basic	$ 1.05	$ 1.35	$ 1.21
Net income per share—diluted	$ 1.05	$ 1.31	$ 1.17
Shares used in per-share calculation—basic	5,828	5,986	6,055
Shares used in per-share calculation—diluted	5,857	6,163	6,265

Source: Cisco Systems Inc., 2009 Annual Report.

Exhibit 4

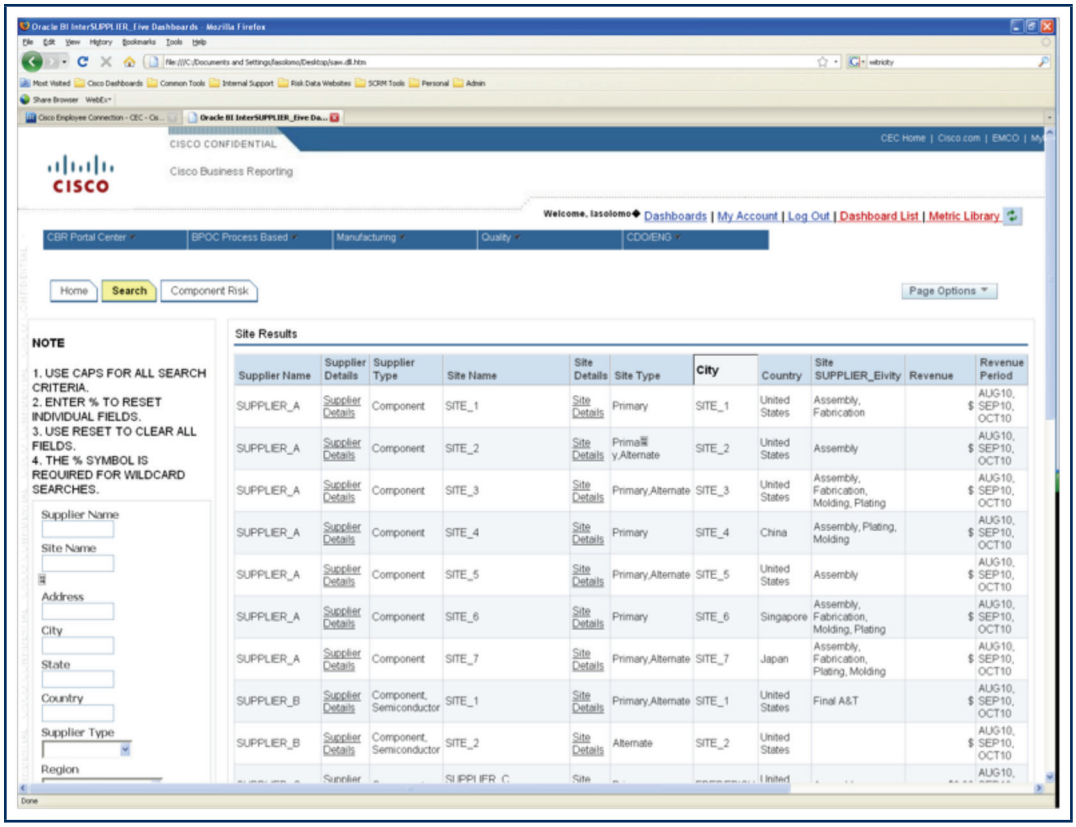
Global Business Operations Capabilities

Source: Unpublished Cisco Systems Inc. internal document, 2009.

Exhibit 5

Cisco's BCP Dashboard

Note: Below indicates general fields available on Cisco's value chain crisis dashboard. All supplier data, including any supplier or other site locations, have been removed.

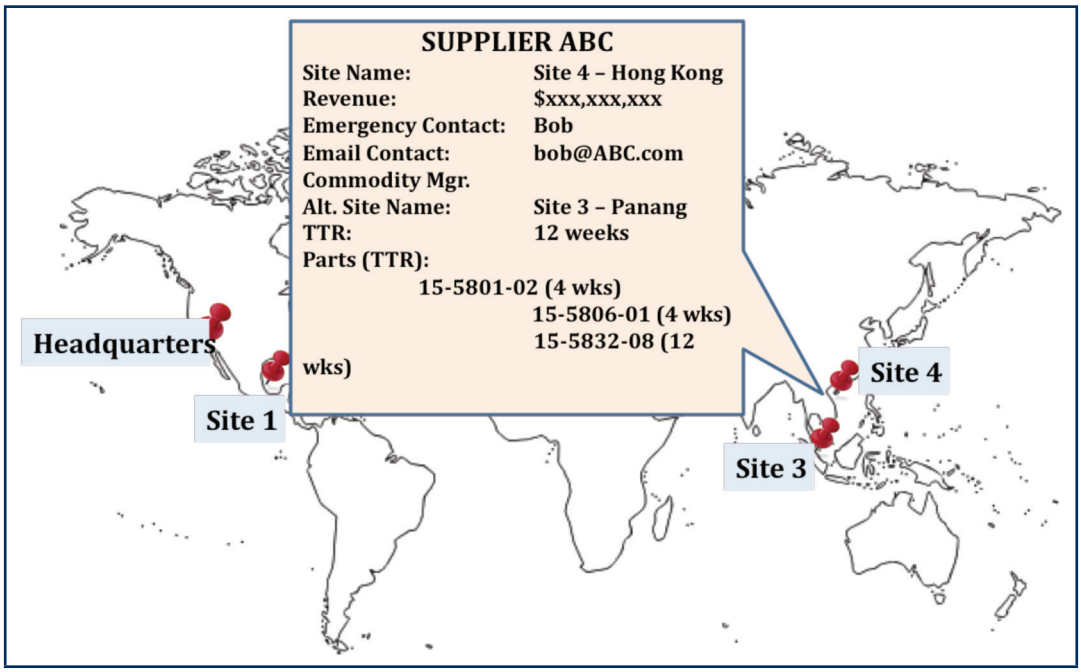


Source: McMorrow, Joe. Unpublished Cisco Systems Inc. internal document, 3 Aug. 2008.

Exhibit 6

Supply Chain Mapping Capability

Note: Example is illustrative only, and not a reference to an actual Cisco supplier.



Source: Unpublished Cisco Systems Inc. internal document, 2009.

Exhibit 7

Sample Monitoring Alert

From: Global Monitoring Service

Sent: Wednesday, April 29, 2009 12:16 PM

Subject: Suspending of Government Activities

Mexico to suspend federal government activities from May 1–5 due to H1N1 swine flu

Relevant Area: Mexico

Incident Location: Nationwide, Mexico

Incident: Health

Incident Type: Health

Severity: Severe

When this Happened: 04/29/2009 03:16 PM EDT (04/29/2009 12:16 PM PDT)

Description:

Mexico will suspend federal government activities from May 1–5 due to the H1N1 swine flu. Mexico's Health Minister asks for all non-essential parts of the economy to shut down during the mentioned five days.

Information Quality: Media

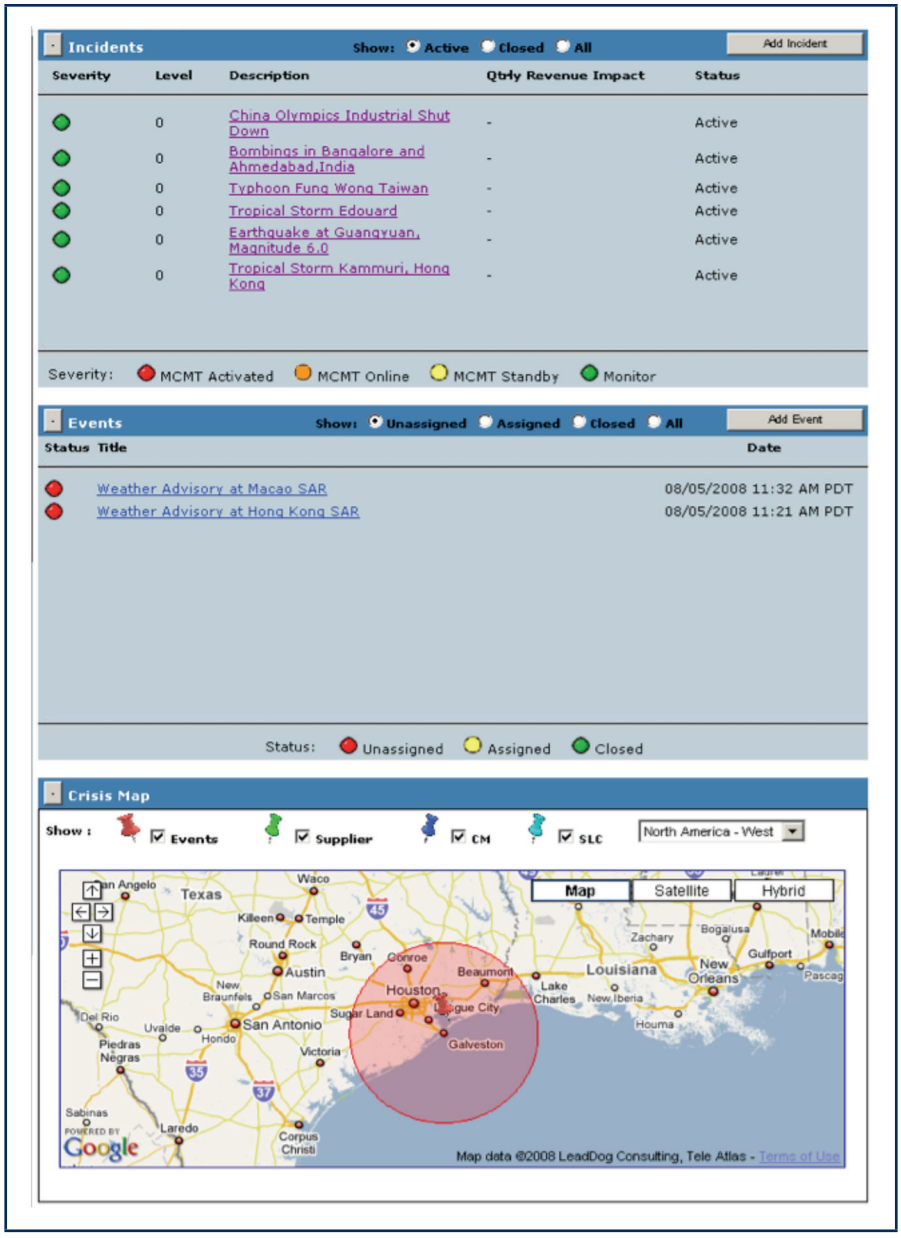
Source: Media

Source: Unpublished Cisco Systems Inc. internal document, 2009.

Exhibit 8

Crisis Dashboard

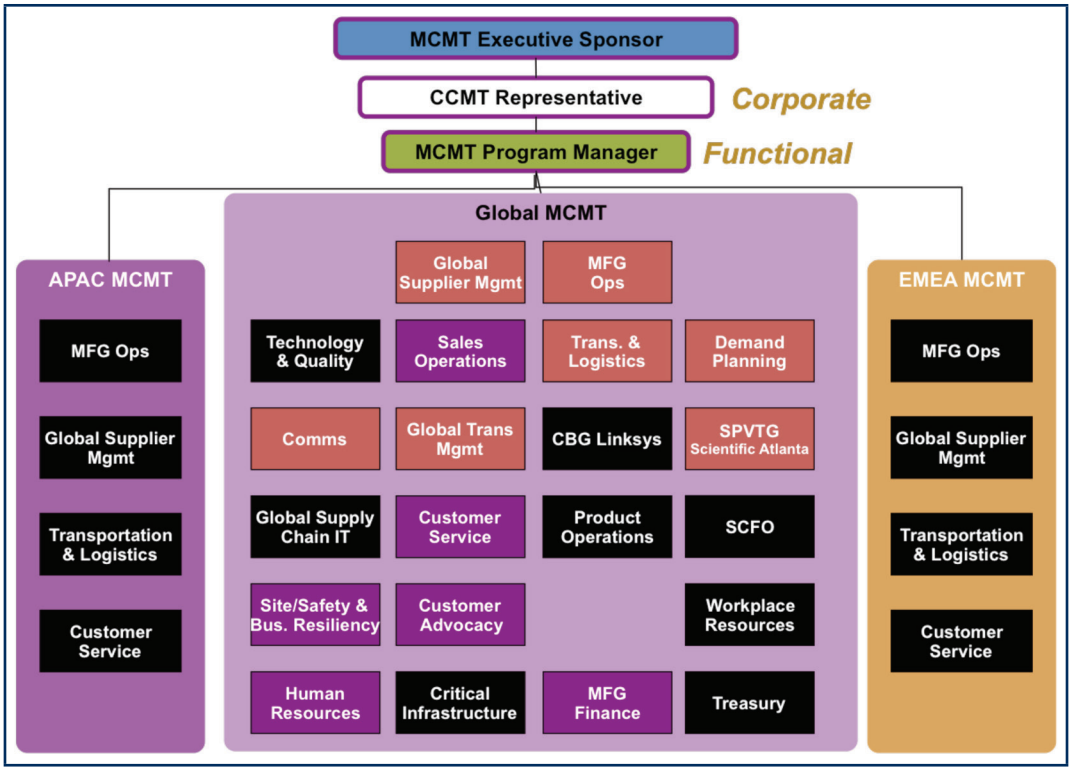
Note: Below indicates general fields available on Cisco's value chain crisis dashboard. All supplier data, including any supplier or other site locations, have been removed.



Source: McMorrow, Joe. Unpublished Cisco Systems Inc. internal document, 3 Aug. 2008.

Exhibit 9

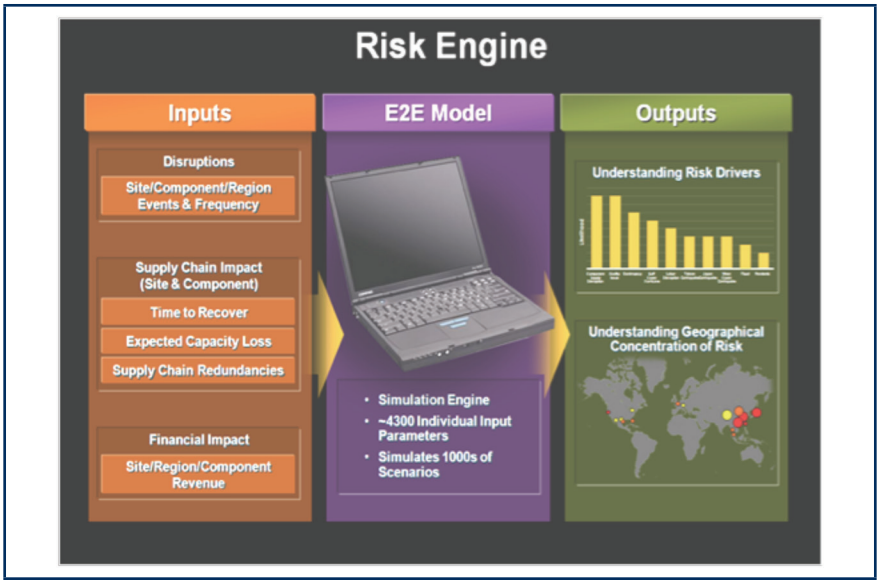
Manufacturing Crisis Management Team Organizational Structure



Source: McMorrow, Joe. Cisco Systems Inc. unpublished document, 2009.

Exhibit 10

Cisco's Risk Engine



Types of disruptions modeled in the risk engine:

- Fire
- Earthquake
- Wind
- Tropical storm
- Flooding
- Labor strike
- Political unrest
- Pandemic

Source: Unpublished Cisco Systems Inc internal document, 2009.

Exhibit 11

Product Resiliency Scorecard

Overall Product Resiliency Score (Out of 10) **7.71**
FY09 Goal (Out of 10) 7.30

Component Resiliency Score — Weight: 30% — (Out of 3) 1.61

	Weight	Current	Score (0-10)	Weighted Score Possible	Weighted Score	Action (Owner)	RYG
% of Single Sourced Risk Rated 1A	30%	38%	2.48	3.00	0.74	37 Parts to 2nd Source (GSM/SCRM)	
Average TTR for Single/Sole Sourced Parts	25%	14.25	6.06	2.50	1.51	47 Parts with TTR>12 wks (GSM/SCRM)	
% Single/Sole Sourced Parts on BOM	15%	15%	7.03	1.50	1.06	109 SS Parts to 2nd Source (GSM/SCRM)	
Number of Risk Rated X CPNs	10%	3	4.00	1.00	0.40	6 Risk Rated X parts to be 2nd Sourced	
% of Risk Rated 1-B,C,D,E,F (Single Source)	10%	15%	7.06	1.00	0.71	16 Parts (Mfg Ops, GSM)	
% of SS Parts without BCP Part Site Coverage	10%	6%	9.45	1.00	0.94	8 parts need Part Site Mapping (SCRM)	
# of PNRs with Single Source (Multi-Source Strategy)	0%		10.00	0.00	0.00		
Standard Power (Y/N)	0%		0.00	0.00	0.00		
Standard Chassis (Y/N)	0%		0.00	0.00	0.00		
		Sum of Score	46.08	10.00	5.36		

Supplier Resiliency Score — Weight: 20% — (Out of 2) 1.80

	Weight	Current	Score (0-10)	Weighted Score Possible	Weighted Score	Action (Owner)	RYG
SS Suppliers with Weak Financial Scores (Mitigate Y/N)	40%	N	10.00	4.00	4.00	1 Red Suppliers (GSM/SCRM)	
# of SS Suppliers with Weak Financial Scores (Monitor)	35%	2	8.00	3.50	2.80	2 Monitor Supplier (Finance)	
% of SS Components with Non-PSL Suppliers	25%	3%	8.90	2.50	2.22	7 Non-PSL Suppliers to 2nd Source (GSM)	
% of Suppliers with Non-Compliant BCP	0%		0.00	0.00	0.00		
# of New Suppliers (New to Cisco)	0%		0.00	0.00	0.00		
		Sum of Score	26.90	10.00	9.02		

Manufacturing Resiliency Score — Weight: 30% — (Out of 3) 2.77

	Weight	Current	Score (0-10)	Weighted Score Possible	Weighted Score	Action (Owner)	RYG
Manufacturing TTR	50%	8.00	8.46	5.00	4.23	Validate FOC & FDO 8 wk TTR plans	
Qualified Alternate PCBA Site (Y/N)	20%	Y	10.00	2.00	2.00	Alt. Site Qual for FOC, FDO (SCRM, Mfg	
Dual Build PCBA Site (Y/N)	20%	Y	10.00	2.00	2.00		
Dual Build FA&T Site (Y/N)	10%	Y	10.00	1.00	1.00		
		Sum of Score	38.46	10.00	9.23		

Test Resiliency Score — Weight: 20% — (Out of 2) 1.52

	Weight	Current	Score (0-10)	Weighted Score Possible	Weighted Score	Action (Owner)	RYG
Test Equipment TTR	90%	8.00	8.46	9.00	7.62	Mitigate BST, RDT/ORT (SCRM, ISM, Mfg	
PSL Test Equipment (Y/N)	10%	N	0.00	1.00	0.00	Create PSL (ISM)	
Standard Test Equipment (Y/N)	0%		10.00	0.00	0.00		
		Sum of Score	8.46	10.00	7.62		

Source: Unpublished Cisco Systems, Inc., internal document, 2009.

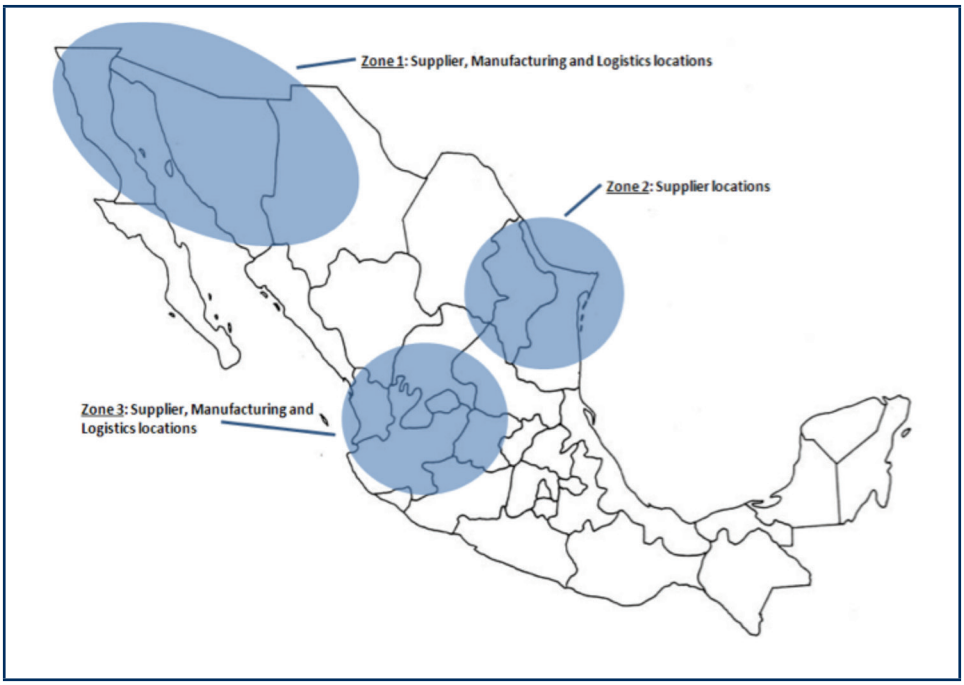
Exhibit 12

Supply Chain Risk Leadership Council

Source: Supply Chain Risk Leadership Council, Cisco Systems, Inc., internal document, 2009.

Exhibit 13

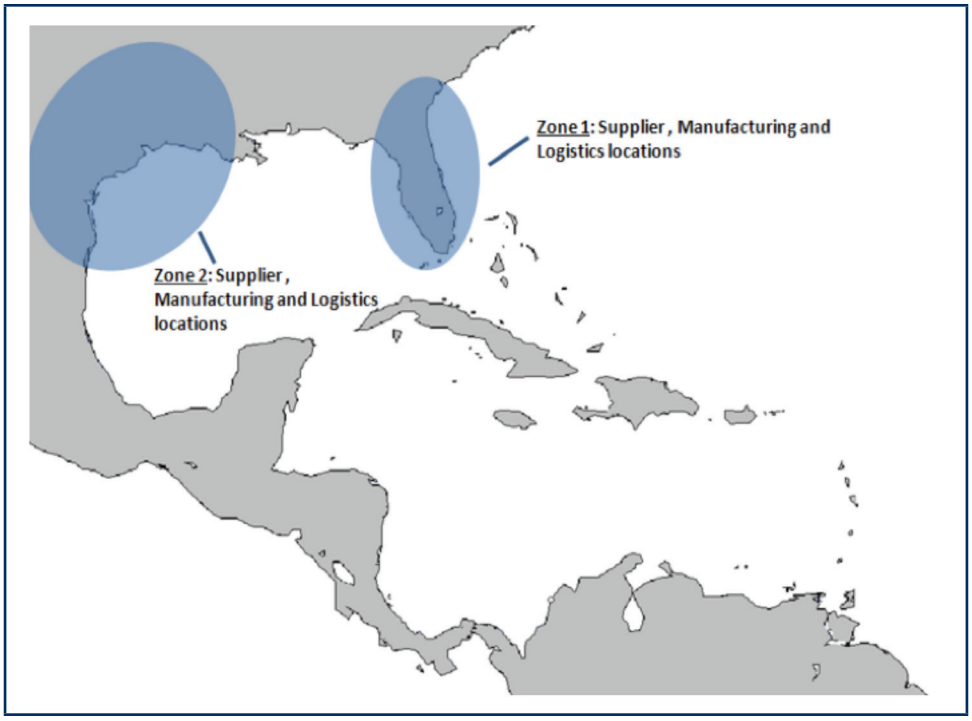
Cisco's Supply Chain in Mexico



Source: Unpublished Cisco Systems Inc. internal document, 2009.

Exhibit 14

Cisco's Supply Chain in the US Gulf Hurricane Region

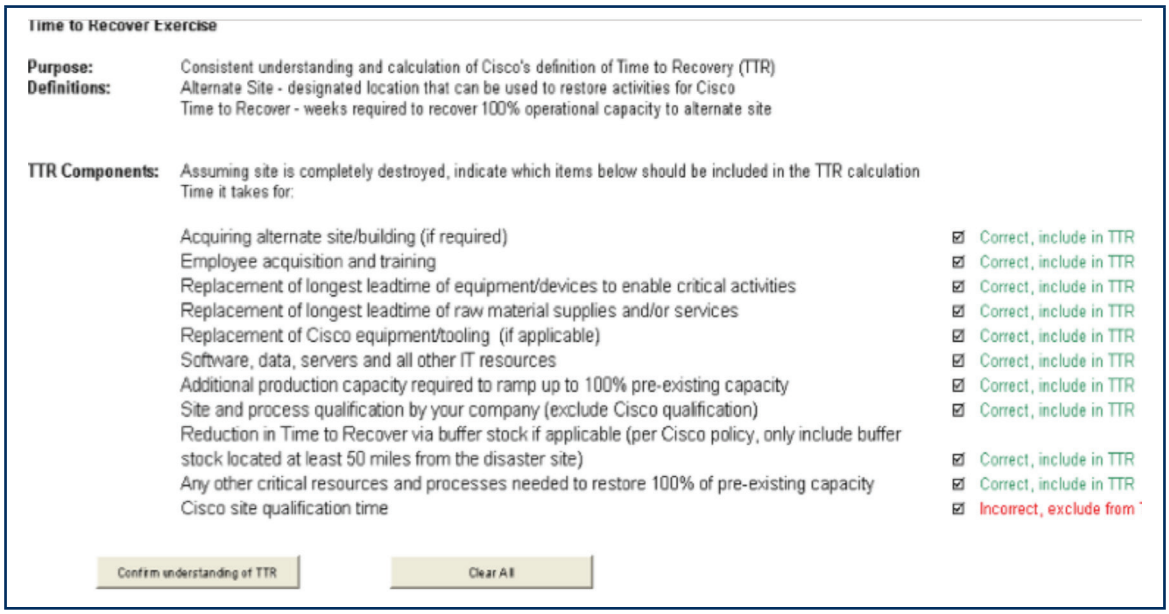


Source: Unpublished Cisco Systems Inc. internal document, 2009.

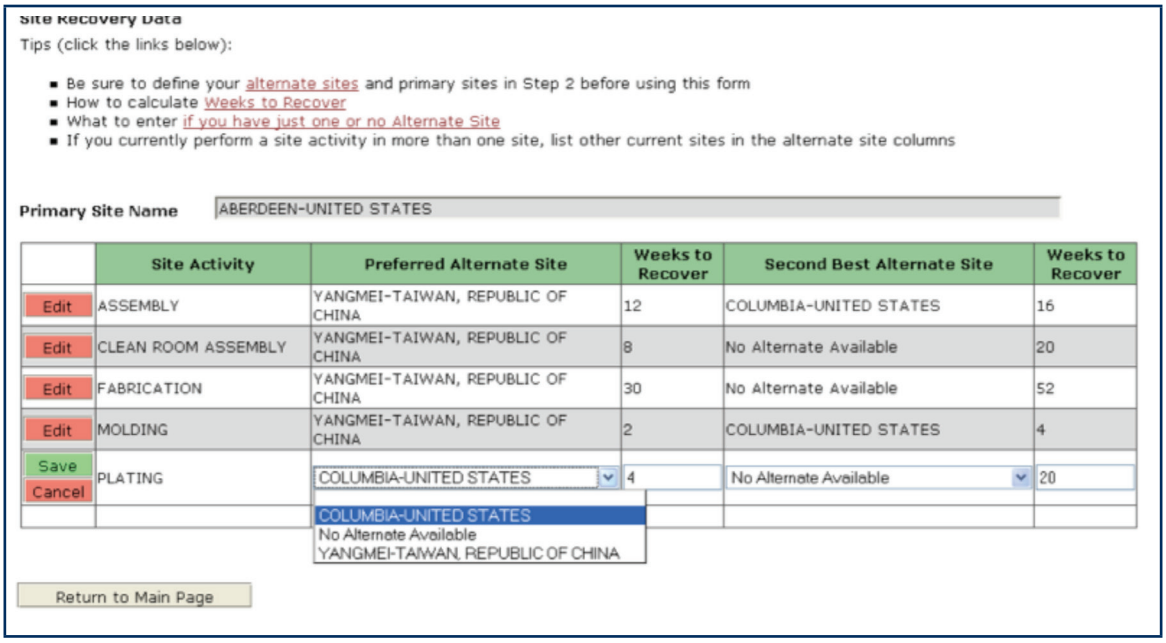
Appendices

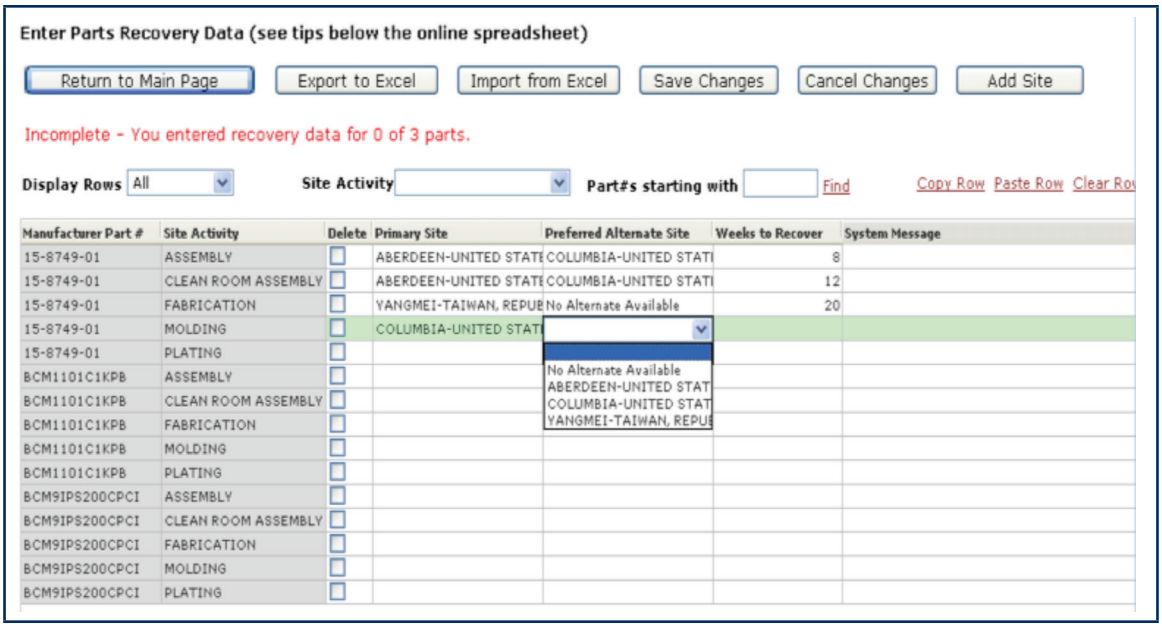
Appendix 1
Sample TTR Report

Section 1 – Supplier exercise to confirm understanding of TTR definition and elements to include in calculation before input of TTR for sites and parts:



Section 2 – Entering TTR Information for Sites and Parts





Enter Parts Recovery Data (see tips below the online spreadsheet)

Return to Main Page | Export to Excel | Import from Excel | Save Changes | Cancel Changes | Add Site

Incomplete - You entered recovery data for 0 of 3 parts.

Display Rows: All Site Activity: Part#s starting with: Find Copy Row Paste Row Clear Row

Manufacturer Part #	Site Activity	Delete	Primary Site	Preferred Alternate Site	Weeks to Recover	System Message
15-8749-01	ASSEMBLY	☐	ABERDEEN-UNITED STATE	COLUMBIA-UNITED STATI	8	
15-8749-01	CLEAN ROOM ASSEMBLY	☐	ABERDEEN-UNITED STATE	COLUMBIA-UNITED STATI	12	
15-8749-01	FABRICATION	☐	YANGMEI-TAIWAN, REPUB	No Alternate Available	20	
15-8749-01	MOLDING	☐	COLUMBIA-UNITED STAT			
15-8749-01	PLATING	☐				
BCM11O1C1KPB	ASSEMBLY	☐				
BCM11O1C1KPB	CLEAN ROOM ASSEMBLY	☐				
BCM11O1C1KPB	FABRICATION	☐				
BCM11O1C1KPB	MOLDING	☐				
BCM11O1C1KPB	PLATING	☐				
BCM9IPS200CPCI	ASSEMBLY	☐				
BCM9IPS200CPCI	CLEAN ROOM ASSEMBLY	☐				
BCM9IPS200CPCI	FABRICATION	☐				
BCM9IPS200CPCI	MOLDING	☐				
BCM9IPS200CPCI	PLATING	☐				

No Alternate Available
ABERDEEN-UNITED STAT
COLUMBIA-UNITED STAT
YANGMEI-TAIWAN, REPU

Appendix 2
Sample BCP Assessment Report

Business Continuity Assessment per Standards Set by CISCO

Supplier Company Name PEGATRON CORPORATION

Business Continuity Assessment Summary

Assessment Score 77 of 100

Overall Rating Yellow

Rating Meaning Partial BCM program

Rationale Some BCM fundamentals are in place. Planning gaps have been identified and plan improvements recommended.

Guidance

- **Gap importance:** Gaps are differences between your response and the Cisco standard. Red gaps require mitigation ("must haves"), Yellow gaps are for capabilities that are very important but not "must haves". Green gaps are recommended practices. All gaps affect your score.
- **Site Rating:** A site is rated Red with any Red gaps, Yellow with any Yellow gaps and Green otherwise.
- **Company Rating:** A company is rated Red if all sites are rated Red, Yellow if one site is rated Red and other sites are not rated Red, or Green if all sites are rated Green.
  - If your company rating is Red, remove your Red gaps from at least one site in order to achieve a Yellow company rating.
  - After that, work to remove Red gaps from all sites in order to achieve a Green company rating.

Site Summary

Site Name	Rating	Last Updated	Update By
MAINTEK SUZHOU PLANT5	Green	18-May-2009	vincent.h_chang@pegatroncorp.com
MAINTEK SUZHOU PLANT1	Green	18-May-2009	vincent.h_chang@pegatroncorp.com
ASKEY-WUJIANG	Green	18-May-2009	vincent.h_chang@pegatroncorp.com
PEGATRON- SHANGHAI SONGJIANG	Red	18-May-2009	vincent.h_chang@pegatroncorp.com

Business Continuity Gaps Summary

Site Name ASKEY-WUJIANG

37. Percent of components and materials from only one qualified source

Determine the percentage of this site's components and raw materials that have only one qualified source. Calculate the percentage as the total number of components with one qualified supplier divided by the total number of components.

47. Joint test with key suppliers or partners in the past 12 months

Participate in a disaster recovery or emergency response test with suppliers or partners each year.

Site Name MAINTEK SUZHOU PLANT1

37. Percent of components and materials from only one qualified source

Determine the percentage of this site's components and raw materials that have only one qualified source. Calculate the percentage as the total number of components with one qualified supplier divided by the total number of components.

Site Name MAINTEK SUZHOU PLANT5

37. Percent of components and materials from only one qualified source

Determine the percentage of this site's components and raw materials that have only one qualified source. Calculate the percentage as the total number of components with one qualified supplier divided by the total number of components.

Site Name PEGATRON- SHANGHAI SONGJIANG

6. Agreement with a site restoration contractor

Ensure that a contract is in place with a site restoration contractor in case of emergency events.

23. Hot work activities policy

Compliance date: 31-Dec-2009. Implement a written policy to manage hot work activities (bracing, grinding, welding, cutting using oxy-acetylene torch, etc.) that are either a part of the manufacturing processes or work done around the facility.

37. Percent of components and materials from only one qualified source

Determine the percentage of this site's components and raw materials that have only one qualified source. Calculate the percentage as the total number of components with one qualified supplier divided by the total number of components.

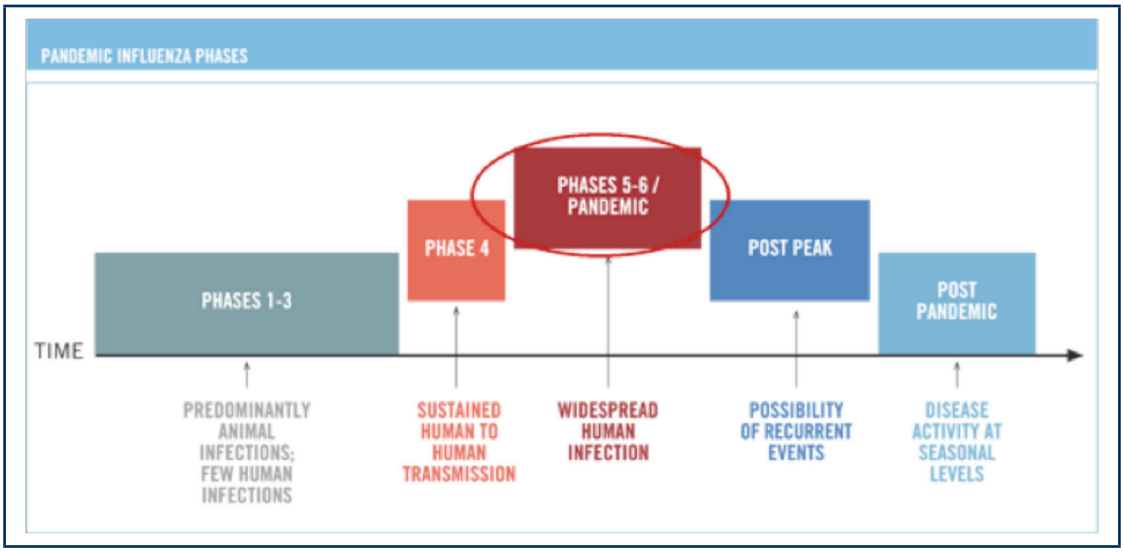
47. Joint test with key suppliers or partners in the past 12 months

Participate in a disaster recovery or emergency response test with suppliers or partners each year.

Appendix 3

World Health Organization's Phased Approach to Pandemic Alert System[28]

In a 2009 revision of the phase descriptions, WHO retained the use of a six-phased approach for easy incorporation of new recommendations and approaches into existing national preparedness and response plans. The grouping and description of pandemic phases were revised to make them easier to understand, more precise, and based upon observable phenomena. Phases 1–3 correlate with preparedness, including capacity development and response planning activities, while Phases 4–6 signal the need for response and mitigation efforts. Furthermore, periods after the first pandemic wave are elaborated to facilitate post-pandemic recovery activities.



In nature, influenza viruses circulate continuously among animals, especially birds. Even though such viruses might theoretically develop into pandemic viruses, in **Phase 1** no viruses circulating among animals have been reported to cause infections in humans.

In **Phase 2** an animal influenza virus circulating among domesticated or wild animals is known to have caused infection in humans, and is therefore considered a potential pandemic threat.

In **Phase 3**, an animal or human-animal influenza reassortant virus has caused sporadic cases or small clusters of disease in people, but has not resulted in human-to-human transmission sufficient to sustain community-level outbreaks. Limited human-to-human transmission may occur under some circumstances, for example, when there is close contact between an infected person and an unprotected caregiver. However, limited transmission under such restricted circumstances does not indicate that the virus has gained the level of transmissibility among humans necessary to cause a pandemic.

Phase 4 is characterized by verified human-to-human transmission of an animal or human-animal influenza reassortant virus able to cause "community-level outbreaks." The ability to cause sustained disease outbreaks in a community marks a significant upward shift in the risk for a pandemic. Any country that suspects or has verified such an event should urgently consult with WHO so that the situation can be jointly assessed and a decision made by the affected country if implementation of a rapid pandemic containment operation is warranted. Phase 4 indicates a significant increase in risk of a pandemic but does not necessarily mean that a pandemic is a forgone conclusion.

Phase 5 is characterized by human-to-human spread of the virus into at least two countries in one WHO region. While most countries will not be affected at this stage, the declaration of Phase 5 is a strong signal that a pandemic is imminent and that the time to finalize the organization, communication, and implementation of the planned mitigation measures is short.

Phase 6, the pandemic phase, is characterized by community level outbreaks in at least one other country in a different WHO region in addition to the criteria defined in Phase 5. Designation of this phase will indicate that a global pandemic is under way.

During the post-peak period, pandemic disease levels in most countries with adequate surveillance will have dropped below peak observed levels. The post-peak period signifies that pandemic activity appears to be decreasing; however, it is uncertain if additional waves will occur and countries will need to be prepared for a second wave.

Previous pandemics have been characterized by waves of activity spread over months. Once the level of disease activity drops, a critical communications task will be to balance this information with the possibility of another wave. Pandemic waves can be separated by months and an immediate "at-ease" signal may be premature.

In the post-pandemic period, influenza disease activity will have returned to levels normally seen for seasonal influenza. It is expected that the pandemic virus will behave as a seasonal influenza A virus. At this stage, it is important to maintain surveillance and update pandemic preparedness and response plans accordingly. An intensive phase of recovery and evaluation may be required.

Endnotes

[1] "Cisco Corporate Overview." Unpublished Cisco Systems Inc. internal document. 2006.

[2] Pellerin, Cheryl. "World Health Organization Declares Global Pandemic for H1N1 Flu." *America.gov*. 11 Jun. 2009. www.america.gov/st/scitech-english/2009/June/20090611140844lcnirellep0.1341364.html.

[3] *World Health Organization*. http://www.who.int/csr/don/2009_06_15/en/index.html . Accessed 23 Nov. 2010.

[4] Cisco. *2009 Annual Report*. http://www.cisco.com/web/about/ac49/ac20/ac19/ar2009/index.html.

[5] "Cisco Corporate Overview." Unpublished Cisco Systems Inc. internal document. 2006.

[6] Treece, J.B. "Just Too Much Single-Sourcing Spurs Toyota Purchasing Review." *Automotive News*. 3 Mar. 1997, p. 3.

[7] Latour, A. "Trial by Fire: A Blaze in Albuquerque Sets Off Major Crisis For Cell-Phone Giants – Nokia Handles Supply Shock With Aplomb as Ericsson of Sweden Gets Burned; Was Sisu the Difference?" *The Wall Street Journal*. 29 Apr. 2001, p. A1.

[8] Hendricks, K., and V. Singhal. "Association Between Supply Chain Glitches and Operating Performance." *Management Science*. 2005, 51(5), 695–711.

[9] "Geodynamics and Environment in East Asia International Conference & 6th Taiwan-France Earth Science Symposium." Université Paul Cézanne, Aix-en-Provence, France. 2010. Web. 3 Mar. 2011. <http://www.geea2010.org/GEEA2010_Abstracts.pdf>.

[10] Ahmad, Tariq, CISSP, technical consultant. "Business Continuity and Disaster Recovery Planning." Unpublished Cisco Systems Inc. document. NETSECLABS. 2009.

[11] Solomon, Lance, Jane Khoury, and Joe McMorrow. Cisco SCRM Team. Telephone interview by Ravi Anupindi. 17 Sep. 2009.

[12] Solomon et al.

[13] Solomon et al.

[14] Solomon et al.

[15] Solomon et al.

[16] Solomon et al.

[17] Solomon et al.

[18] McMorrow, Joe. Unpublished Cisco Systems Inc. document. 1 Aug. 2009.

[19] McMorrow, Joe. Unpublished Cisco Systems Inc. document. 3 Aug. 2008.

[20] McMorrow, 3 Aug. 2008.

[21] McMorrow, 3 Aug. 2008.

[22] McMorrow, 3 Aug. 2008.

[23] McMorrow, 3 Aug. 2008.

[24] Solomon, Lance, Jane Khoury, and Joe McMorrow. Cisco SCRM Team. Telephone interview by Ravi Anupindi. 17 Sep. 2009.

[25] Ahmad, Tariq, CISSP, technical consultant. "Business Continuity and Disaster Recovery Planning." Unpublished Cisco Systems Inc. document. NETSECLABS. 2009.

[26] McMorrow, Joe. Unpublished Cisco Systems Inc. document. 1 Aug. 2009.

[27] American Red Cross. "Flu Alert Now at Highest Level – Phase 6." *Redcross.org*. 11 Jun. 2009. http://www.redcross.org/portal/site/en/menuitem.1a019a978f421296e81ec89e43181aa0/?vgnextoid=dfd78423f59c1210VgnVCM10000089f0870aRCRD.

[28] *World Health Organization*. http://www.who.int/csr/disease/avian_influenza/phase/en/index.html.

Notes

Notes

Established at the University of Michigan in 1992, the **William Davidson Institute** (WDI) is an independent, non-profit research and educational organization focused on providing private-sector solutions in emerging markets. Through a unique structure that integrates research, field-based collaborations, education/training, publishing, and University of Michigan student opportunities, WDI creates long-term value for academic institutions, partner organizations, and donor agencies active in emerging markets. WDI also provides a forum for academics, policy makers, business leaders, and development experts to enhance their understanding of these economies. WDI is one of the few institutions of higher learning in the United States that is fully dedicated to understanding, testing, and implementing actionable, private-sector business models addressing the challenges and opportunities in emerging markets.