Cisco Supply Chain Business Continuity

**How does Cisco mitigate supply chain risk?**

- Cisco continually monitors our supply chain for issues that may impact our operations, working closely with our suppliers to assess and minimize any potential effect.
- By continually optimizing our supply chain, we are able to quickly respond to changing market dynamics, minimizing impacts to our business and disruptions to our customers.
- Cisco has well-established processes to coordinate our efforts during outbreaks like COVID-19, including our Global Business Resiliency (GBR) and Supply Chain Incident Management (SCIM) Processes. For information, please see our Business Resiliency program.

**Where does Cisco manufacture its products?**

- Cisco has a global, distributed and agile supply chain. Our global network includes manufacturing facilities and partners located in countries around the world.
- You can learn more about Cisco’s supply chain footprint, and responsible sourcing and manufacturing in the 2019 Corporate Social Responsibility Report.

Cisco Supply Chain Response to COVID-19 Coronavirus

**How is Cisco addressing the supply chain impact by the COVID-19 Coronavirus outbreak?**

- Cisco has activated our pandemic response plan. Our global response is being coordinated by a dedicated Incident Management Team with 24/7 coverage, reporting to our Executive Leadership Team. The team is monitoring the situation closely and providing direction and guidance based on advice from our corporate medical director, from recognized international health bodies, together with official guidance from government, municipal and local authorities.
- In situations like these, Cisco moves quickly to take action to minimize potential risk this may have for Cisco employees, customers and business.
- Cisco’s technology plays an essential role in enabling critical infrastructure such as healthcare, public services, education, service providers, and regulated financial services during the COVID-19 pandemic. As the situation continues to evolve, we will prioritize our resources to support impacted people globally. We are regularly monitoring the needs of those at the front line of the global response and will continue to make adjustments as necessary.

**Are there any manufacturing or logistics impacts due to the pandemic?**

- There are currently no manufacturing sites closed in Cisco’s supply chain. In certain countries, restrictions have been imposed on businesses, however Cisco along with our partner manufacturers have been granted exceptions for certain critical business work which have allowed us to continue to operate with available capacity.
- Cisco imports goods from around the world through a wide variety of ports of entry. Our logistics team is responsible for managing constraints at specific points of entry. At present, we are not experiencing significant delays in moving goods domestically or internationally.

**Are Cisco Failure Analysis (FA) operations impacted during the COVID-19 pandemic?**

- Cisco has a global, distributed and agile supply chain. Our global network includes manufacturing facilities and partners located in countries around the world.
There are government-imposed restrictions in some countries however Cisco has been granted 'critical manufacturing' exceptions to stay open with available capacity in most jurisdictions.

We are leveraging the available capacity to process your cases and, in some instances, re-route them to alternate FA sites. This mitigation strategy may result in longer response times than normal.

Please contact your existing Cisco TAC or Account team with any questions.

How does Cisco prioritize/allocate the available supply for fulfillment?

- Under normal operating circumstances, Cisco would be making sure we can support all our customers’ needs. Given the current environment, we are prioritizing critical infrastructure such as healthcare, public services, education, service providers, and regulated financial services.

How is Cisco protecting factory workers’ rights during the Covid-19 outbreak?

- The health and safety of workers is a top priority, and we require our partners to follow all applicable government regulations and the Responsible Business Alliance (RBA) Code of Conduct.
- Cisco has been communicating with suppliers to ensure they are maintaining focus on workers’ human rights in conformance with the RBA Code of Conduct during the COVID-19 outbreak. We reiterated our expectations for health and safety, management of working hours, and payment of wages which could be impacted by the outbreak.
- We are surveying suppliers to assess their management of these issues and following up with any suppliers whose responses indicate risk.

Impact of COVID-19 Coronavirus on Cisco Service Availability

Have Cisco’s Global Service Logistics and Operations services been impacted by COVID-19 (including technical support, availability and mitigation measures)?

- Cisco’s Global Service Logistics and Operations services are operating normally, within the framework of country or regional specific movement constraints. In areas where official restrictions are in place, this may delay or prevent a field engineer from physically accessing a customer or partner site and/or replacement parts from being delivered.
- Our Customer Experience organization maintains a global network of 24-hour Technical Assistance Centers (TACs) and will assist customers in identifying alternative solutions alongside providing remote support to sites that do not permit physical access. As documented in the service contract, appropriate remote access capabilities are required in order for this to be achieved.
- We will continue to observe all official advice and directions on restricting the spread of the infection and will keep customers informed where there is an impact on our service delivery.

How is Cisco addressing greater demand for WebEx services due to the increase in customers working from home?

- Our top priority is helping users collaborate and connect using WebEx. During this extraordinary time, when most people are moving to work remotely, we are seeing an unprecedented increase in WebEx usage from our enterprise customers. This may cause some occasional service degradation issues, but we are continuously monitoring all services and are working 24/7 to proactively provide the high-quality service that our customers expect. We sincerely appreciate the patience and understanding of our customers and partners.
- Please use the WebEx status portal as a resource to get the latest updates, http://status.webex.com/.

Customer and Partner Order Inquiries

Are there any near-term impacts to Cisco production and delivery schedules?

- Cisco is leveraging its global network and working aggressively to re-route orders, expedite alternative component supply, and bring up additional manufacturing capability.
- Cisco has taken a wide range of measures to mitigate the impact of the COVID-19 on customers by:
  - Identifying alternate manufacturing sites to move production
Creating new capacity in new locations
Collaboration with sub-tier suppliers to optimize production capacity

Lead-times were extended on products directly or indirectly affected by this disruption. Our ordering tools, Cisco Commerce Workspace (CCW), is updated with current information.

**Which products/product families are affected by this situation?**
- The lead-times for product/product families affected by this situation, both direct and indirect, are reflected in our ordering tool, Cisco Commerce Workspace (CCW).

**Can Cisco fulfill my order from a different fulfillment site?**
- Cisco is pursuing opportunities to leverage our global supply chain network and minimize the impact on our customers and the business.
- We are aggressively taking action to re reroute orders, expedite alternative component supply, and add manufacturing capabilities in other regions.

**What should customers do if their site/facility is closed and unable to accept delivery of a Cisco order?**
- We understand that COVID-19 has resulted in customer facility closures with little or no advance warning. Please contact your Customer and Partner Services' Regional Operations point of contact to update them on your closed facilities or ones with the potential for closure.

**What is Cisco's refused delivery policy?**
- If a carrier tries to deliver a shipment and it is refused, it will be routed back to Cisco’s Return Center. Some carriers may hold the shipment for 3-5 days before sending back to Cisco. Once the product is received at the Cisco Returns Center, the Customer and Partner Services team will be notified and they will contact the customer directly to determine if shipment should be held, reshipped or if an RMA is to be requested.

**What is the impact and mitigation strategy for Return to Stock (RTS)?**
- RTS shipments will be held awaiting reshipment to the Customer at Cisco cost. If a customer does not want the product re-shippered, they will need to request a RMA via the CCW Returns Tool per the standard process.

**Is it safe to receive a product and packaging shipped during the COVID-19 pandemic?**
- The World Health Organization has confirmed it is safe to handle packages, but if you think a surface may be infected, clean it with simple disinfectant to kill the virus and protect yourself and others. Clean your hands with an alcohol-based hand rub or wash them with soap and water. Avoid touching your eyes, mouth, or nose.
- For your reference, review the latest information on disinfectants from the United States Environmental Protection Agency (EPA), [https://www.epa.gov/coronavirus](https://www.epa.gov/coronavirus)
- Regardless of the current outbreak, it is good hygiene practice for us all to wash our hands thoroughly after handling packages.

**Does Cisco have recommendations for disinfecting a Cisco product?**
- The United States Environmental Protection Agency (EPA), [https://www.epa.gov/coronavirus](https://www.epa.gov/coronavirus), has a current list of COVID-19 disinfectants. In addition, Cisco’s supply chain technologists are testing various disinfecting protocols for Cisco products. The following guidelines are available for your consideration:
  - Network equipment enclosures
    - IPA-based cleaners are safe for plastic resins of PC/ABS materials and powder painted surfaces when used for wiping but not for prolonged exposure (e.g. Spor-Klenz, Sanitary wipes: Clorox, Lysol, Dispatch).
    - Ammonia-based cleaners (e.g. Formula 409, Windex) are not recommended for cleaning plastic surfaces and powder painted surfaces due potential of surface cracking.
  - Collaboration, Webex devices & IP Phones
- IPA-based cleaners plasticizers, bleach, and peroxides should NOT be used for rubber (thermoplastic elastomer/urethane) gaskets and overmolds. Use on these materials will lead to potential degradation.

- Interconnects
  - In general, the cables and connectors are able to withstand brief exposure to disinfectant solutions when applied by spray or wipes; excessive soaking can be harmful and damaging.
  - Cables and interconnect components are resistant to isopropyl alcohol based-cleaning solutions.
  - PA66 or Nylon is susceptible to hydrogen peroxide damage (a component of Spor-Klenz) in concentrations of 10% or higher.
  - Sodium hypochlorite or bleach products can be harmful to LCP resins if above 12.5% concentration.

Will my warranty be invalidated if I use a cleaning agent to disinfect a Cisco product?
Cisco Business

How is Cisco protecting its workforce from exposure to COVID-19?

- As of Monday, March 16th, our offices globally moved to a mandatory work from home policy for the safety of our employees and in alignment with the guidance of medical professionals. All Cisco employees are working from home, using Cisco technology to continue to deliver on customer projects and stay connected.
- Any changes to this policy will be in accordance with official guidelines.
- We have put in place strong additional measures to help protect our employees, including the suspension of global business travel and the cancellation of our participation in a number of events globally, with key significant Cisco events switched to virtual.