Symantec Enterprise Resiliency Organization

Program Summary

May 20, 2016

Strategy Statement

- Symantec's Enterprise Resiliency Program is a key component of our business model. A comprehensive set of Business Continuity Management Plans document the critical staff resources, procedures, processes, and infrastructure required to continue to support our customer operations in the event of a disruption to Symantec operations.

- The principal focus of the ERO Program is to identify actual and potential risks to business function resilience; mitigate those risks by ensuring respective business functions design, document and exercise business continuity strategies, then facilitate the execution of those strategies if there is a disruption to critical Symantec functions, while maintaining our ability to deliver services to our customers. This is accomplished through a geographically flexible model, where several global locations provide coverage and backup for primary locations to enable continuity and immediate response to our customer's critical support requirements.

- The Symantec ERO lifecycle addresses awareness and training, assessment, strategy development, planning, exercising/incident response and continuous improvement.

Implementation Details

Symantec's Business Continuity Program is active at several response and recovery levels:

- A framework of Global, Regional, and Site Level Incident Management Teams composed of executive, strategic, and tactical team members, who are trained utilizing Incident Command System (ICS) methodology to respond to, and effectively manage, worldwide incidents.
- Immediate, concurrent emergency communications capability, multiple hard communications mechanisms, and ICS soft communications protocols.
- A global Business Impact Analysis study is conducted to identify critical business processes recovery time and point objectives to support Symantec's continued operations and our continued client operations.
- Business Continuity and Disaster Recovery strategies have been created and implemented to support Symantec's critical RTOs and RPOs to provide continued client support and maintain the revenue stream.
- An ISO 22301 compliant business continuity plan framework is provided all Symantec response and recovery teams worldwide to build and maintain current business continuity and disaster recovery plans.
- Symantec has tested continuity capability for all critical business processes including technical support services, business critical services, licensing, security response and managed security services, and software as a service and vendor fulfilment, in the event that facilities, business processes, their technology support, or staff, are unavailable, so that we can continue to maintain the services and products used by clients.
- Critical third party service provider's business continuity capabilities are reviewed for compliance in alignment with their criticality to the owning Symantec business unit.

©2016 Symantec – All rights reserved