SUNGARD

# NINE STEPS TO PREPARE YOUR BUSINESS FOR A PANDEMIC

Ask the Experts

## 1 CONSIDER THE IMPACT OF MISSING PEOPLE WITHIN YOUR ORGANIZATION

Now is the time to review and update your group's role in your organization's pandemic response plans to address workforce absenteeism. If these plans do not exist, then response plans that consider a significant absence of an organization's workforce or inability to work at your primary location can be leveraged or should be developed. Technology staff members often provide coverage around the clock, which may be difficult as a pandemic impacts particular geographies and impacts local support resources – or central services and systems. Guidance has been provided to plan for 40 percent of your staff to be absent. Given this, ask yourself – do you have the cross-training, documentation, tools, and support to continue working with a significantly lower level of expertise? Consider whether it may be an option to share support roles from two or more geographic areas, to minimize impact on the potentially hardest-hit locale.

## 2 REVISIT AND REASSIGN RESPONSIBILITIES

If your workforce or organization has been restructured recently, it is possible that those responsible for action in the face of a pandemic may not be fully trained in their role. Consider single points of failure among your staff from a knowledge perspective, and take action to identify alternate staff and to provide some level of cross-training.

## 3 CONSIDER THE IMPACT OF MISSING PEOPLE OUTSIDE YOUR ORGANIZATION

Technology operations depend on many maintenance and support contracts that are outside your company or organization. These partners may potentially experience the same severe absenteeism as your company should a pandemic develop. Review each of these support relationships, and ask those partners and vendors to share how they intend to meet support requirements. If you are not satisfied, consider multiple vendors to diversify your risk, and develop those relationships now.

## 4 CONSIDER THE REQUIREMENTS AND PRIORITIES OF YOUR INTERNAL CUSTOMERS

Business operations at specific operating sites and even throughout the company may be revised and altered, based upon the local impacts of the pandemic. Departments may close, and other departments adjust their priorities to match their specific business needs. It's important to align resources to meet vital operations, and ensure that basic business operations can continue. This may be required even if the central or supporting IT organizations are not directly impacted by the pandemic situation.

## 5 CONSIDER THE IMPACTS OF MORE PEOPLE WORKING FROM HOME

Today your remote worker infrastructure may be focused on the occasional user or traveler; however, in a pandemic situation more people may opt to – or be required to – work from home. Assess your infrastructure for providing that support, focusing not only on technologies but also support services. Home workers will still need application support, login and password support, and hardware support. Also, if your company is not used to a significant number of people working from home you'll have an increase in learning and awareness needs – how do I use remote access? Why can't I get to X system?

## 6 PREPARE FOR LIGHTS OUT

A pandemic event is unlike any technology disaster. Systems will continue running, although there may be a degradation of performance over time as maintenance and infrastructure weaknesses develop without the benefit of the ongoing planned and unplanned preventive maintenance and activities on an on-site support staff. If you have planned maintenance activities – get them scheduled now. Ensure system documentation is up to date and readily accessible by support staff working in a remote location. Encourage cross-training. And take advantage of weaknesses already identified from past exercises and ensure they are corrected, putting you in the most resilient position possible.

## 7 UNDERSTAND YOUR VULNERABILITIES

The key to planning is understanding your vulnerabilities and then mitigating them – either by eliminating or minimizing the chance they can occur, or minimizing the impact when they do occur. Ask yourself - How will you provide remote support? How will you do preventive maintenance – particularly hardware maintenance? What expertise is limited within your organization and how would you deal with that loss under these circumstances? What systems require special "care and feeding" because of their hardware or software instability? How will you handle call volumes? Focus on solutions that can be implemented quickly and provide the greatest benefit against the pandemic threat.

## 8 WHAT SHOULD I DO NOW – TODAY?

General business preparedness for a pandemic should be covered by each business unit. For technology teams, it becomes an interesting exercise to ask how you would handle a technology failure, or a typical disaster, while your staff numbers are compromised. Can you handle hurricane season and a pandemic simultaneously? What limitations in people, process, or technology would be exposed if your organization needs to respond to a "typical" disaster while operating without 40 percent of your staff?

## 9 WHAT IF I HAVE NO PANDEMIC PLAN?

The pre-pandemic phase is a little bit like a hurricane – you still have some time to prepare, but there is a sense of urgency as the WHO levels are increased. Determine first who within your organization will make critical decisions in the face of a pandemic impacting your operations, and work with any corporate pandemic leaders or crisis management structure. Then understand your vulnerabilities looking at systems and data to some extent – but particularly at process and people.

**About SunGard Availability Services**

SunGard Availability Services provides disaster recovery, managed IT, information availability consulting services and business continuity management software to over 9,000 customers globally.

SunGard Availability Services | 680 East Swedesford Road | Wayne, PA 19087 | 800-468-7483 | www.sungardas.com