

Pandemic Planning and Business Resilience

In today's constantly changing and competitive business environment, access to your enterprise's information resources, data and personnel are more critical than ever before. Regardless of enterprise size and type, not having timely access to key enterprise wide data, information, and human resources can be devastating to existing revenue streams, maintaining current client accounts, or supporting governmental mandates. Developing an effective and efficient enterprise-wide contingency plan ensures informational resources are available prior, during and following an enterprise interruption event. There are four (4) key components to business contingency planning:

1. Business Impact Analysis & Assessment (BIA)
2. Disaster Recovery Plan (DRP)
3. Business Continuity Plan (BCP-Private, COOP-Public)
4. Exercise & Maintenance (Test)

From a contingency planning perspective, a DRP ensures the protection of data back-ups and safe storage of duplicate information (data and paper) so that enterprise-critical information cannot be lost or damaged from an interruption event. The DRP supports the technical aspects of the Information Technology ("IT") department. Equally important, a BCP and/or Continuity of Operations Plan ("COOP") ensures the continuous availability of critical business processes and procedures. A BCP/COOP is the operational glue that keeps the doors to an enterprise functionally open during unplanned natural, human, or technical events upon the enterprise.

Incidents inside and against enterprises occur on a daily basis. Many of these incidents turn into enterprise-wide disasters. Disasters are created due to a lack of contingency planning to effectively manage an incident. Disasters are borne from three different areas: natural, human and technical. Examples are:

- Natural-- floods, tornados, earthquakes, pandemics, severe storms (rain/ice/snow)
- Human-- terrorist activity, work place violence, electronic security breaches, civil disorder, theft
- Technical-- power failure, hardware or software failure, software virus

Pandemic Fears Affect Contingency Planning

For many years business owners and enterprise managers have been discussing and planning for technical failures within IT. System based failures and/or loss of critical data stores have achieved extensive notoriety across the enterprise. However, very recently all levels of government have been warning the general public of possible out of control flu strains that could create a pandemic situation. Two real life examples of flu strains are Avian Flu (H5N1) and Swine Flu (H1N1).

Various flu strains have negatively affected human society for hundreds of years – both physically and mentally.

Today's business environment has significantly changed since the last widely known pandemic. Gone are the days for a flu strain to travel the world in weeks or months. In today's mobile environment flu strains can travel from country to country within a few short hours. It's a "1 to N" relationship between humans and now countries that allow the flu strain to pass from human to human without physical boundaries. Fears of a new pandemic have become a reality for many business owners and their employees.

The number one most valuable asset to an enterprise is the employee. The number one most expensive asset to an enterprise is the employee. Hence, without employees there is no business. The business and its employees can be directly or indirectly affected by a pandemic incident. Consider this short list of indirect dependencies upon the business when developing the pandemic response component of your contingency plan:

- Employees becoming ill while on business travel
- An employee has a child or children whose school is closed
- An employee's direct family member becomes ill and requires immediate care
- The physical premise of key suppliers to the business are placed under quarantine
- Public transportation systems are temporarily closed

When family members become ill someone must help with managing their illness. Schools close, transportation systems are interrupted – it's a top/down pyramid affect that directly impacts the ability of the business to generate, maintain and manage revenue. Many enterprise managers default to saying "our employees will work from home". This creates a false sense of security that has multiple pitfalls. These pitfalls are:

1. An increase in IT security risks if remote connectivity has not been tested and validated for secure transmission of sensitive content.
2. Increase in capital expenditures (HW and SW) within IT to support the increase of remote workers.
3. Current Virtual Private Network (VPN) and/or remote connectivity company policies do not support all functions.
4. A spiked increase in bandwidth demand on internet infrastructure creates bottlenecks to effectively transmitting and receiving data.
5. During normal working hours, employees' time and energy are spent on family medical issues while their job functions take a back seat.
6. Many employee's functions are heavily paper based and do not support a remote work environment.

To circumvent these pitfalls, contingency planning is a must for any size enterprise. Planning for a wide spread flu incident should be a component of every contingency plan – regardless of size and complexity.

Contingency Planning Is Key to Resilience

A vast number of enterprise managers, owners and executives today are either minimally prepared, have not reviewed their current action plan for four to five years, are too busy to develop a plan, are short on human resources, or simply don't know how or where to begin. The need for contingency planning and support will continue to intensify as private and public enterprises' needs become more demanding. New and emerging technologies, government regulation, customer and employee demands will further drive this need. Human, natural and technical incidents consistently loom on the horizon of every business enterprise. The need for validating key business continuity processes, policies and procedures across the enterprise is increasing and will continue to remain on the corporate score card. A business resilient enterprise is one that invests in the technical and business process components of contingency planning. Compared to the alternative, investing in contingency planning is a financially sound and time efficient choice.

James M. Myers is the President & CEO of Contingency Now with corporate offices in Los Angeles, California. Contingency Now can be contacted at 310-686-9094.