



Quick answers. Proven products. Reliable experts.
All to help meet your clients' commercial insurance needs.

- Commercial Auto
- Liability
- Workers Compensation
- Group Benefits
- Property

SEE MORE >

Pandemic Threat Makes Contingency Planning Critical For Enterprise Risks

Flu outbreak, other disasters could disrupt most important asset—employees

By **JAMES M. MYERS**
 Published 8/31/2009

[Email Share](#) [Print This Article](#) [Normal Text](#) [Large Text](#)

With the threat of a global flu pandemic looming large, risk managers must take steps to maintain timely access to key enterprisewide data and resources during such a crisis so that a disruption does not devastate revenue streams, undermine client accounts or prevent government mandates from being met, all while protecting their most valuable assets—their employees.

Developing an effective and efficient contingency plan ensures informational resources are available prior, during and following an enterprise interruption event.

There are four key components to business contingency planning:

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



A comprehensive contingency plan must take into account employees or suppliers becoming ill themselves during a pandemic, or having to stay home to care for sick relatives.

From a contingency planning perspective, a DRP ensures the protection of data back-ups and safe storage of duplicate information (data and paper) so enterprise-critical information cannot be lost or damaged from an interruption event.

The DRP supports the technical aspects of the information technology 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 enterprisewide 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, workplace violence, electronic security breaches, civil disorder, theft.
- Technical—power failure, hardware or software failure, software virus.

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 know 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.

As a result, 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 risk managers default to saying "our employees will work from home." This creates a false sense of security that has multiple pitfalls. These pitfalls are:

- An increase in IT security risks if remote connectivity has not been tested and validated for secure transmission of sensitive content.
- A rise in capital expenditures within IT to support the increase of remote workers.
- Current Virtual Private Network (VPN) and/or remote connectivity company policies do not support all functions.
- A spiked increase in bandwidth demand on Internet infrastructure creates bottlenecks to effectively transmitting and receiving data.
- During normal working hours, employees' time and energy are spent on family medical issues while their job functions take a back seat.
- Many employee 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 widespread flu incident should be a component of every contingency plan—regardless of size and complexity.

A vast number of enterprise risk 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 enterprise 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 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 president and CEO of Contingency Now, with corporate offices in Los Angeles, Calif. He may be contacted at 818-510-4939.

Quick answers and proven products to help meet your clients' business insurance needs.



SEE MORE >

Download FREE Webcast



where information lives™

Learn how you can cut costs, streamline, & automate your P&C claims process.

MOST READ ARTICLES

- Zurich Net Income Drops 53% As Recession Takes Toll
- New Orleans Levee Boards Settle Breach Case For \$20 Million
- New Health Care Draft Would Omit Public Plan Provider
- CEOs Form Global Reinsurance Trade Group
- Auto Insurers Should Be Investigated, Says Conn. AG



Quick answers. Proven products. Reliable experts.
All to help meet your clients' commercial insurance needs.

- Commercial Auto
- Property
- Group Benefits
- Workers Compensation
- Liability

SEE MORE >

RELATED ARTICLES

- SICO Did Not Breach Trust With AIG
- AIG, Greenberg Agree To Arbitration
- Predictive Models Won't Replace People, But Can Help With Underwriting, Claims
- Sam's Blog: Obama Should Set Trigger For Public Option!
- Zurich Says Insurers Must Step-Up On Climate Change
- Caroline's Blog: Rumor Mill Links Bill White To U.S.V.I.
- RIMS Exec Calls For National Comp Law To Reduce Litigation, Standardize Benefits
- Sheffield Ready To Run For Commissioner Post In Georgia