‘Swine Flu’: Lessons in Pandemic Preparedness From the Financial Industry

Gartner RAS Core Research Note G00167922, Richard J. De Lotto, Ken McGee, Roberta J. Witty, 1 May 2009, RA3 04162010

A true pandemic will significantly disrupt an enterprise’s business operations worldwide, because of extremely high absentee rates, and because few enterprises have adequate pandemic preparedness plans in place. Business continuity management and disaster recovery professionals and many other stakeholders — especially IT managers — must plan, test and add capacity to ensure the sustainability of operations under extremely difficult circumstances.

Key Findings

- A pandemic is worldwide in scope and of indefinite duration, and may cause staff absenteeism exceeding 40% for extended periods. (The current influenza outbreak, although extremely serious, is not yet a pandemic and may not become one.) Enterprises with global presence, partners, suppliers or service providers will likely be more dramatically affected than purely “national” enterprises.

- Many enterprises’ operational continuity during a pandemic will depend almost entirely on the sustainability of their IT functions — particularly, enterprises able to do so will shift largely to a work-at-home model and move workload to outsourcers or partners in less-affected areas.

- Communications and other essential services will likely be seriously disrupted during a pandemic. Significant travel restrictions are likely to be imposed prior to the declaration of an epidemic, and they will become almost universal in the case of a pandemic.

Recommendations

- Immediately download and examine the U.S. Federal Financial Institutions Examination Council after-action report on its recent pandemic-response-planning exercise, and disseminate relevant findings across the enterprise to raise awareness of the urgency of pandemic response planning.

- Identify existing and projected critical skill shortages, and initiate necessary personnel cross-training, testing and certification. (For most enterprises, this will be the most disruptive and time-consuming area of remediation.)

- Determine which business operations are sustainable, and at what level, and the likely durations of downtime for normal business operations with extraordinarily high IT personnel absentee rates. Test for various combinations of leaders and skilled personnel.

Gartner

- Testing should start immediately to isolate and remediate problem areas. Testing should be rigorous, inventive, ongoing and documented.

ANALYSIS

1.0 The Potential Impact of a Severe Disease Outbreak

The international outbreak of H1N1 influenza, commonly known as "swine flu," continues to spread. The disease is currently having its greatest impact in Mexico, where more than 100 H1N1 influenza deaths have been reported — though far fewer have been confirmed. Smaller outbreaks, with some fatalities, have occurred in Brazil, Canada, France, Israel, New Zealand, Spain, the United States and elsewhere. On 28 April 2009, the World Health Organization (WHO) raised the threat level for the outbreak to the second-highest level, Phase 5, which indicates that person-to-person transmission of the H1N1 virus is occurring at the national level (see Note 1). This means that the outbreak does not yet represent a pandemic — Phase 6 on the WHO rankings — which requires the cross-regional spread of a serious illness that is easily transmitted from person to person and for which there is little natural immunity. At the time of this writing, there is no clear indication that the H1N1 outbreak will reach that level. This strain of influenza appears to be treatable with common antivirus medications, and person-to-person transmission can be significantly inhibited by precautions as simple as careful personal hygiene, including regular hand washing.
For up-to-dateinformation on the outbreak, see http://news.bbc.co.uk/2/hi/europe/8027043.stm.

Note 1 H1N1 Influenza

WHO has chosen to avoid using the term "swine flu." Although H1N1 influenza appears to have originated in pigs, it is spread largely by human-to-human transmission.

Nonetheless, the spread of H1N1 influenza is already having a significant adverse impact on enterprises' business operations. A recent decline in the market price of oil, for example, has been attributed to fears of a disease-driven economic decline — adding to the worldwide downturn already in progress — and health authorities in some areas, including the European Union, have issued travel warnings for Mexico and the United States. Influenza-related disruptions will likely continue and increase, even if this remains a "simple" outbreak and does not reach epidemic or pandemic proportions. Forward-thinking enterprise decision makers — including senior executives, line-of-business managers, business continuity management (BCM) and disaster recovery (DR) professionals, risk managers, IT managers, and other stakeholders — will treat this outbreak as a very serious threat to their ongoing operations.

Enterprises should, at a minimum, view this event as a test case for a true catastrophic worldwide pandemic. Pandemics — for example, the devastating 1918 influenza outbreak, the most serious pandemic in modern times — are extremely rare, but epidemiologists and other healthcare providers widely regard at least occasional pandemic outbreaks as virtually inevitable. For this reason, enterprises need well-developed, well-implemented and well-tested plans in place to deal with the human and operational disruptions that will inevitably result from a pandemic or even from a less-serious outbreak of disease.

2.0 Lessons Learned From the Financial Services Industry

The experience of the financial services industry — the only industry sector known to have undertaken serious pandemic response planning — can be instructive for enterprises in all industries and across all regions. In the United States, for example, the Federal Financial Institutions Examination Council (FFIEC) requires financial institutions under its jurisdiction to have a tested response plan in place to minimize the operational impact of a potential pandemic (see "FFIEC Releases Guidance on Pandemic Planning"). In December 2007, the FFIEC released expanded pandemic-response-planning guidance, based on the results of the Financial and Banking Information Infrastructure Committee (FBIIC)/Financial Services Sector Coordinating Council (FSSCC) Pandemic Flu Exercise of 2007, which was conducted by the U.S. Treasury.

This exercise received little attention in the media, including the specialized financial services and IT-oriented press. This was both surprising and disappointing, because the exercise clearly showed that most of the participating financial institutions determined that their BCM/DR pandemic response plans were ineffective and contained critical gaps (only 12% ranked their plans as "highly effective"). Gartner believes this exercise represents the only large-scale testing of business pandemic plans ever conducted, and enterprise stakeholders, regardless of industry or location, should study and disseminate the FFIEC's after-action report (available for download at www.fspanfluexercise.com) and determine how the findings can be applied to their own specific cases. The FFIEC's guidance extends well beyond previous directives, explicitly citing the critical role that IT staff must play to ensure continued operations in the face of massive, prolonged staff shortages. The after-action report should be of intense interest to IT managers everywhere.

2.1 Pandemic Impact Projections

The societal costs of a true influenza pandemic will be high. The U.S. Congressional Budget Office's 2005 estimate of the effects of a pandemic of the avian influenza virus H5N1 (the so-called "bird flu") projected 90 million cases of infection and 2 million deaths in the United States alone. (The actual impacts of different disease

outbreaks vary widely, and the severity of the H1N1 influenza strains remains unclear at the time of this writing.) Gartner's pandemic planning assumptions are based on the FBIIC/FSSCC exercise, as well as the lessons learned from the devastating 1918 pandemic and other severe disease outbreaks and Gartner's extensive body of BCM/DR research. We project:

- Moderate-to-severe business disruptions for more than 70% of enterprises
- A minimum of 40% absenteeism for as long as eight weeks during peak outbreaks — particularly for personnel in households with children (which have a projected infection rate of 20% for adults and 40% for children), which may be repeated during multiple waves of infection
- The possibility of absentee rates close to 100% in some organizations, caused by factors including:
  - School and day-care center closings, which require parents to stay home with their children
  - The demands on personnel who are responsible for caring for family members and others at greatest risk from disease, including infants, the elderly, pregnant women and individuals with chronic medical conditions
  - Call-ups for volunteers with existing military reserve, law enforcement, paramedic or other emergency duties
  - Significant disruptions in the operations of business partners, suppliers, service providers and other stakeholders, which will further adversely affect enterprises' own operations

The FBIIC/FSSCC exercise revealed that, despite previous guidance, more than a third of the participating financial institutions had made no special BCM/DR plans for pandemic conditions. These enterprises apparently did not view the risk to their institutions as high enough to warrant action or to be singled out as requiring special event response and contingency strategies. Disturbingly, the exercise revealed that the vast majority found their pandemic-related plans to be no better than "moderately effective" at maintaining normal operations.

2.2 The FBIIC/FSSCC Exercise

The 2,775 participants in the FBIIC/FSSCC pandemic response plan exercise were drawn from financial institutions operating across the United States:

- 62% came from banks or credit unions, 23% from securities firms, and 11% from insurance companies.
- The selection of participants was biased toward smaller institutions, with 85% of the participants working for firms with 1,000 or fewer employees and annual revenue of $500 million or less.
- Only 64% had BCM/DR pandemic response plans in place. Of these, 56% of them thought the exercise revealed their plans to be moderately effective, and 32% found their plans minimally effective or not at all effective.
- 97% of participants found that the exercise revealed critical dependencies, gaps or flaws that merited additional attention, and 91% planned additional all-hazard plan refinement based on the lessons learned during the exercise.
- Only 42% had HR policies or plans designed to address their organizational needs during a pandemic.

The FBIIC/FSSCC exercise and the FFIEC after-action report focus on U.S. financial institutions, but enterprises of all types, in all industries and across all regions can draw valuable lessons from them. The most urgent is that most enterprises' BCM/DR plans for pandemics have clearly proved to be insufficient and require immediate upgrades. A pandemic will differ from a "normal" disaster in many important ways: A pandemic will be at least regional in scope, and most likely global; it will be of indefinite duration; and it will likely drive absenteeism above 40% for extended periods. Existing BCM/DR plans, which are normally based on the assumption of limited access to specific locations or systems for short periods of time, are unlikely to provide adequate protection. This will not be the case during a pandemic.

A further problem is the fact that risk-assessment-based planning is complicated by the lack of contemporary examples from which to draw best practices or examples of poor practices. Previous expectations, even of regional disasters, have been based on the premise that there will be secure areas from which to regroup and recover business operations. This is not expected to be the case for pandemics. Even the best-case scenarios strain managerial willingness to accept the "unknowability" of actual risk, potential speed of onset, extensive problem set and lack of clear solutions. Testing of BCM/DR plans should include the ability to close and reopen smoothly if staff shortages temporarily rise above sustainable rates, or if situations warrant that the entire staff be replaced.

3.0 Personnel and IT — The Critical Failure Point

The success, and indeed the ongoing viability, of enterprises during a pandemic will require that they enable their personnel — the key failure point in a period of sustained high absenteeism — to continue working under what are likely to be extremely difficult circumstances. This will in turn require that their IT functions remain in operation during pandemics, which makes business continuity an immediate and urgent concern for CIOs and their planning teams. The FBIIC/FSSCC exercise helped to confirm that most enterprises plan to meet their business and regulatory obligations during a pandemic by using IT assets to reduce as much as possible the need for face-to-face interactions between personnel, partners, customers and other stakeholders. Anticipated methods included:

- Establishing work-at-home capabilities (54%)
- Dividing business units into parallel teams and distributing large parts of the workforce geographically (41%)

- Shedding workload to outsourcers or reciprocally partnered organizations in less-affected areas (26%)

All of these methods will require extensive (and expensive) planning, training, testing and coordination well before the first cases are reported. Enterprises preparing for these methods should:

- **Check BCM/DR plans for irrationally optimistic personnel assumptions.** The FBIIC/FSSCC exercise did not address several critical problems, including:
  - **Caregiver and staff "burnout."** The exercise stopped at the "first wave" of the simulated pandemic, even though the prevailing guidance is for several sequential waves. Physical resources, such as antivirus medications and personal protective equipment, have generally been purchased only in amounts sufficient for the first wave.
  - **Unrealistic assumptions of personnel capabilities.** Some of the large institutions participating in the FBIIC/FSSCC exercise believed that they would be able to cope by shifting part of their operations overseas. Gartner's view is that this belief results either from an unrealistic assumption of heroic efforts by both domestic and overseas personnel and infrastructure providers, or from a failure to grasp the global nature and impact of pandemics. In most cases, enterprises' partners, suppliers and service providers overseas will be preparing for, experiencing or trying to recover their operations at the same time as the enterprises themselves.
  - **Lack of realistic estimates of personnel to come to work under pandemic conditions.** No one has found a method to reliably estimate or test the willingness of employees in any industry to come to work under profoundly unusual circumstances. Wartime models will not necessarily apply.
- **Test the enterprise's ability to operate for long periods with reduced IT personnel.** The first step in this process is to establish realistic service-level expectations with IT personnel absentee rates of 10%. Test the actual depth of cross-training, succession planning and backup staffing strategies to determine whether the established backup team can actually do what needs to be done. A simple review of existing delegation and backup assignments will not be enough to ensure service levels in the face of the emerging threat. Only actual, periodic hands-on performance of delegated duties will reveal whether individuals have the necessary skills or require retraining. Managers will need to check at least quarterly to ensure that personnel designated as backups are in fact available and have not had life changes that preclude their participation. This will place tremendous stress on IT staff to have all system documentation updated and current enough to be used as an instruction handbook by less than optimally skilled replacements. Cross-trained staff must keep all licenses and certification up to date.
- **Test the command, control and communications system.** Communication with mission-critical personnel and their surrogates will be another critical potential failure point. It is essential that personnel be located, inventoried and communicated with under extremely adverse conditions. Most enterprises will already have some form of emergency contract protocol for "normal" emergencies. However, many personnel are likely to be dislocated by the pandemic, due to families' convening at points unknown to the enterprise or due to being "frozen in place" by quarantine restrictions. For this reason, enterprises should consider issuing standard long-life mobile telephones with messaging capabilities to business-critical personnel, and make carrying these devices a condition of employment. Some personnel may also need backup satellite communications capabilities. Support and communications services for senior managers and key staff will be critical.

It is very likely that the first major government response to a pandemic that significantly impacts enterprises will be to shut down the air and ground transport systems, potentially stranding key operating and managerial staff for indefinite periods. The next major impact will be the overloading of telecommunications services, including Internet services, which prevents easy communication.

- **Establish a clear chain of command.** An enterprise's succession plan is normally a closely held secret, but a pandemic will require a clearly defined and firmly established chain of command. Senior executives, line-of-business managers and other key personnel may be incapacitated or isolated by quarantine restrictions for more than a predetermined period. The IT organization will need to establish and test methods for preprovisioning, authenticating and remotely enabling backup staff with the requisite tools, access and permissions and doing so in a highly secure manner.
- **Ensure that all critical personnel can be reached in an emergency.** Key personnel must be aware that they need to be "reachable" on a multichannel basis in case of emergency; they must be available to be on call; and they must be equipped to do so. The FBIIC/FSSCC exercise found that most BCM/DR plans did not adequately factor in the need for child care and elder care, and Gartner believes the staff availability projections for lesser disruptions have probably been overestimated as well.

4.0 The IT Organization's Role in Pandemic Preparedness

Gartner has identified three critical areas in which enterprise IT organizations must contribute to pandemic response plans and preparations. This is to meet regulatory requirements as well as to ensure continuity of business operations.

4.1 Documentation

Requirement: Prepare a documented strategy that is scaled to the stages of a pandemic outbreak. Covered institutions are expected to draw and test plans suitable for maintaining their IT operations and, therefore, institutional operations for varying scenarios at each of the seven U.S. federal government response stages (see Table 1).

Table 1. Response Stages and Gartner Recommendations

WHO Pandemic Phases	U.S. Federal Response Stage	Defining Characteristics	Gartner Recommendations
Phase 4 Phase 5	Stage 2	Confirmed human outbreak overseas	• Institute mandatory hygiene training for all personnel. • Limit foreign travel. • Test work-from-home plans by personnel rotation. • Physically check shelter-in-place supplies. • Confirm facilities access and security coverage during emergency situations. • Ensure that management backups and surrogates have passwords and provisioning necessary to assume responsibility if needed. • Test the emergency communications system. • Test the crisis communications plan. • Obtain up-to-date copies or documentation of work being performed offshore. • Implement contingency plans for anticipated supply chain disruptions. • Communicate enterprise policies on time off, use of vacation, sick leave and other issues during a pandemic. • Provide emergency payroll advances for purchases of personal preparedness supplies.
Phase 6	Stage 3	Widespread human outbreaks at multiple locations overseas	• Limit domestic travel. • Instruct traveling staff to return to country of domicile, if possible. • Perform actual live testing of all pandemic precautions, regardless of disruptions to operations. Conduct remediation as needed, without regard to personal or organizational sensitivities. • Initiate daily check-in procedures.
Phase 6	Stage 4	First human case in North America	• Activate all pandemic plans. • Prepare for a freeze in mass transit (including airlines and railways).
Phase 6	Stage 5	Spread throughout a specific country	• Implement contingency plans for widespread supply shortages and restrictions on the use of critical infrastructure. • Maintain overall situational awareness.
Phase 6	Stage 6	Recovery and preparation for subsequent waves	• Begin recovery and resupply to prepare for subsequent waves of infection.

Source: Gartner (May 2009)

Plans should be documented with enough detail to enable proper execution by new managers or backup personnel. Plans should be readily available to current and backup managers if normal access to systems and facilities is curtailed.

Requirement: Have a comprehensive framework in place to ensure the continuity of critical operations. Critical business processes and capabilities should be clearly identified, along with criteria as to when it is appropriate to temporarily abandon less-critical functionality. Some details may necessarily be kept confidential to the company and have only limited distribution.

4.2 Response: Test, Test and Retest

Requirement: Institute a testing program for pandemic preparations. Testing should begin immediately, to isolate and remediate problem areas. Testing should be rigorous, inventive, ongoing and documented. Every aspect of IT operations should be stress-tested for the pandemic environment, but these areas — shown by the FBIIC/FSSCC exercise or previous events to be of special concern — should be given particular attention:

- **Test preventive programs.** Most preventive measures will be taken by the enterprise's central BCM/DR team, but the IT organization should also have such measures in place — for example, to reduce the risk of intrapersonnel infection. These precautions may include providing infection control supplies (for example, hand cleansers, tissues and receptacles for their disposal) in all IT locations, with backup stock to cover possible supply line disruptions. Heating, ventilation and air-conditioning systems should be well-maintained to ensure smooth operation and to reduce the spread of airborne infections.

- **Test the availability of critical service providers.** The FFIEC guidance and other U.S. sources anticipate that the first pandemic outbreak will be outside the U.S., and most likely in Asia. All the ambiguities and risks associated with pandemics in the U.S. are exacerbated at locations in the developing world, where all resources, including those devoted to infrastructure and public health, are less widely available. Test suppliers' and service providers' provisions, and back up their capabilities with local companies if necessary. Local power, environmental services and telecommunications providers will face the same problems enterprises do in maintaining critical personnel and functionality levels. Collect and evaluate their planned service levels for pandemics, and determine where your operations rate on critical-user scales. A lack of pandemic response plans should be a severe warning sign.

- **Test infrastructure and facilities.** Business continuity managers should immediately determine the answers to the following questions:

  - How resilient is the local civil infrastructure in your areas of operations? Are the same trauma, fire and police services available, with the same response times, as when you last updated your plans? It is important to remember that utility companies and other providers will have the same problems you do, and it will almost certainly take longer to restore electricity, water and other essential services during a pandemic than during a "normal" outage.

  - What priority will be assigned by utilities, police, fire and rescue to safeguarding enterprise resources during a pandemic?

  - Will the physical security of your sites — and the safety of your staff and customers — be reduced by reduced police presence, increased emergency response times or longer trips to trauma facilities? Will there be an impact on your site insurance?

- **Test the enterprise's ability to provision, operate and support work-at-home staff and remote workplaces.** This will be a far-reaching effort and may involve substantial reprovisioning, including:

  - Providing personnel with the necessary hardware or software tools for secure remote access — either in advance or when needed — including sourcing by alternative suppliers and channels. These tools may include Secure Sockets Layer virtual private network software and risk-appropriate authentication methods.

  - Promptly updating entitlements to allow personnel to provide backup for absent colleagues in addition to their normal responsibilities, paying close attention to segregation-of-duty conflicts (which may be unavoidable in extreme circumstances but will require detective controls).

- Regional telecommunications infrastructure will be strained, perhaps to the breaking point, during a pandemic. Ensure that key personnel and their backups have access to reliable and high-speed Internet service, Short Message Service (SMS), mobile telephones and multiple landlines. Plan for multiple long-term service outages. Testing can be anecdotal — if it is properly documented — for regions with bad seasonal weather conditions. Any weather condition severe enough to close schools can severely reduce personnel availability and strain the local and regional communications resources necessary for a work-at-home infrastructure.

- **Ensure that customer privacy can be maintained in a remote workplace.** Adopt full encryption for sensitive data. Automatically disable visual access to unattended computers with "passworded" screen savers or automated lockouts, so that unauthorized users (for example, family members or roommates) cannot see confidential consumer data simply by walking past the monitor. Consider augmenting or replacing passwords with higher-assurance authentication methods. Provide remote workers with the tools that are normally used to keep sensitive hard-copy data secure, including limited-access areas, secure file cabinets and paper shredders.

- **Test the reliability and surge capacity of online customer service and support.** The online and telephone channels will likely emerge as the key conduits for service and support during a pandemic. A communication plan and technology must be tested and in place to keep customers aware of what services are available and where, and to direct customers to available alternative facilities or channels for critical products and services.

- **Test the ability to staff critical staffing-intensive operations.** Any enterprise with critical, labor-intensive operations needs to prepare for high and possibly prolonged absenteeism. IT data center print and mail operations, for example, are labor-intensive and highly dependent on outside suppliers and service providers to operate printers, run inserters, manually stuff envelopes and move materials. Whether prepared in-house or externally, the transaction documents (bills, checks, policies and regulatory documents) they produce are the lifeblood of the enterprise.

4.3 Response: Increase Oversight

Requirement: Have an oversight program to ensure that the plan is reviewed and updated. Gartner has noted that expenditures for pandemic response are high and highly politicized. IT managers should expect to face pressure to adjust risk estimates — and associated spending requests — downward in times of economic stress.

BCM/DR plans need constant updating to deal with changes in normal daily operations. Pandemic plans, due to the highly abnormal nature of the risk, will be even more difficult to keep current. Plans should be formally reviewed at least quarterly and at each change in the World Health Organization pandemic phase or the U.S. federal government response stages. U.S. guidance indicates that pandemic planning is a specific board-of-directors-level responsibility. Plans must be reported to the board and senior managers for review and approval at least annually.

Additional research contribution and review: Ant Allan, Pete Basiliere, David Furlonger and Mary Knox.

Acronym Key and Glossary Terms

BCM	business continuity management
DR	disaster recovery
FBIIC	Financial and Banking Information Infrastructure Committee (U.S.)
FFIEC	Federal Financial Institutions Examination Council (U.S.)
FSSCC	Financial Services Sector Coordinating Council (U.S.)
SMS	Short Message Service
WHO	World Health Organization