Pandemic readiness in the US financial services sector: When failure is not an option

Annie Searle

Received: 7th March, 2008

Enterprise Risk Services, Washington Mutual, 1301 Second Avenue, WMC0601,
Seattle, WA 98101, USA
Tel: +1 206 500 2250; E-mail: annie.searle@wamu.net

Annie Searle *is Senior Vice President and Divisional Executive for Enterprise Risk Services. Her portfolio of responsibilities includes business continuity and technology risk management for the entire company, as well as regulatory and audit assurance for its technology group. She is the chair of Washington Mutual's crisis management team, a member of the company's public policy management committee, and executive sponsor of its technology innovation programme. Nationally, Annie represents the company as a member of the BITS Advisory Council for the Financial Services Roundtable, based in Washington DC. She chaired the 'Pandemic Readiness: Interweaving the Plans' panel for the Fall 2007 Critical Infrastructure Protection Congress, which included the heads of five critical sectors as well as the Department of Homeland Security. She is a member of the Pacific Northwest Regional Disaster Resilience Advisory Council, and co-chair of the Pacific Northwest Regional Recovery Coalition for Financial Services. She was a member of the project planning team and design working group for the US Treasury Department's three-week pandemic exercise in autumn 2007.*

Abstract

This paper provides an update to 'Pandemic flu planning in the US financial services sector', a paper published in Volume 1, Number 3, of Journal of Business Continuity and Emergency Planning. *In the present paper, the author examines the state of pandemic readiness one year later, referencing four new publications available for planning in the USA. The paper focuses on key observations and lessons learned from the US Department of Treasury's autumn 2007 exercise, which was conducted among 2,775 financial services institutions. The paper then briefly discusses the pandemic guidance issued by the Federal Financial Institutions Examination Council in December 2007.*

Keywords: pandemic, avian flu, financial sector planning, US Treasury Department, US Department of Homeland Security

As strategic continuity planners, it is still possible to buy time on the pandemic challenge while the existing imperfect plans are refined. This can either be done now, using data that have become available in the last year, or on the fly when a pandemic strikes. In a significant Harvard Health report published last year, Max Bazerman defined the blind spots that continue to exist in pandemic planning, around what he called 'predictable surprises' — 'known problems whose predictability is supported by extensive data'.[1]

Journal of Business Continuity & Emergency Planning
Vol. 2 No. 4, pp. 357–364
© Henry Stewart Publications,
1749-9216

The historic examples he uses are the number of studies that anticipated the breach of New Orleans' levees and the intelligence that was in hand before the September 11th attacks. Examples of future predictable surprises would include climate change and over-harvested fisheries. Bazerman goes on to identify cognitive, organisational and political barriers that keep people from acting in advance on future predictable surprises, such as pandemics.

Bazerman's excellent study is important because it is still a challenge to discuss pandemic planning across public and private sectors with clarity. There are still blind spots. Pandemic is coming, but it is not possible to say precisely when. Bazerman suggests that people are not good at investing today for an unclear future benefit. Thus, part of the challenge is to find ways to make the urgency of the planning clearer, especially when other issues affecting the banking and financial sector seem significantly more important right now.

Were it possible to disable 40 per cent of the nation's critical infrastructure for a day and run a single live nationwide test, everyone would understand why a pandemic represents a crisis of unparalleled magnitude. Indeed, it is worth looking at other wake-up calls that can be issued this year so that there is not a single place in the country that does not take the risk of a pandemic seriously. In the meantime, continuity professionals will continue to elevate the importance of planning. Here, thanks are especially due to those whose work has led to the release of the new Federal Financial Institutions Examination Council (FFIEC) guidance on pandemic influenza.

Although planning in the financial sector is considered by many to be more advanced than other critical components managed by the private sector, the three-week Treasury Department test conducted last autumn (2007) indicates that there is still a great deal to do — agreements to be forged and unusual solutions to be developed to handle dangers and opportunities that can be anticipated.

In the past year, however, progress has been made in the pandemic arena, in particular with the issuance of four key documents: the 2007 National Infrastructure Protection Plan; the Department of Homeland Security (DHS) Pandemic Influenza Plan One-Year Summary; the After Action Report of the Treasury Department's 2007 Pandemic Flu Exercise; and the FFIEC Pandemic Influenza Guidance. The paper will review the first two documents briefly, before examining the latter two in more detail.

The first document, the 2007 National Infrastructure Protection Plan, contains a risk management framework that includes an international component as well as a banking and finance sector description and dependencies declaration.[2] The 2007 DHS Pandemic Influenza Implementation Plan One-Year Summary,[3] meanwhile, supplements its 2006 guide to critical infrastructure/key resource planning for a pandemic.[4] A close reading of these two framing documents is highly recommended.

Further enhancing these plans are the results of the national pandemic exercise conducted over a three-week period last autumn. Modelled on the 2006 British pandemic test and led by the US Treasury Department through the Financial Banking Information Infrastructure Committee (FBIIC), the Financial Services Sector Coordinating Council (FSSCC), and the Securities Industry and Financial Markets Association, the exercise was designed to enhance the understanding of systemic risks to the sector; provide an opportunity for 2,775 firms to test their pandemic plans; and examine how the effect of a pandemic flu on other critical infrastructures will affect the financial services sector.[5] More than 100 delegates from public and private financial service groups worked together, largely by conference call, to develop the exercise. Here it is worth briefly touching upon some of the data collected from respondents, before moving on to post-scenario recommendations:

- nearly 64 per cent indicated that they have a pandemic plan;
- only 42 per cent indicated that they have pandemic HR policies;
- over 56 per cent indicated that they now evaluate their pandemic plans as 'moderately effective';
- over 96 per cent stated that the exercise allowed organisations to identify critical dependencies, gaps and seams that warrant additional attention;
- almost 99 per cent indicated the exercise was useful in assessing pandemic business planning needs.

It should really come as no surprise that, until the planning committee designed and executed this type of test, and until the after-action report was published, companies would not formally state that there was room for improvement in their plans. Nor is it a surprise that the financial sector is extremely dependent upon other critical infrastructure sectors such as telecommunications, energy, transportation and information technology. Of course, this has always been known in principle, but with no set benchmarks for best practices, firms were working in relative isolation or with regional public partners to develop higher levels of maturity into their respective plans. Released in January 2008, the Treasury Department's report from the exercise is an excellent summary with recommendations, many of them involving work already in progress to varying degrees. Here, the paper will discuss six of the recommendations and observations that seem to offer the most compelling impetus forward for everyone.

> 'As the financial services sector works to improve its planning activities, organizations may wish to consider participating in regional partnerships … Such partnerships also create avenues for coordination with local, State and Federal government agencies.'[6]

The regulators have worked with the Treasury to recommend the creation of what are now 21 regional financial sector coalitions.[7] Each of the coalitions is organised somewhat differently and has individualised objectives that differ based on the maturity of the alliance, but they all are based upon information sharing and analysis. The most sophisticated model is that of the earliest coalition to be formed — Chicago First — which is an aggregation of local banking and insurance companies as well as national banks that have a presence in Chicago. In Chicago, membership dues are collected and a representative of the group sits in the City of Chicago's Emergency Operations Center, tying public and private interests together irrevocably. This type of consortium has proven it can work on issues like mutual aid when the LaSalle Bank fire occurred. In other cities, like Tampa and San Francisco, regional coalitions have conducted pandemic tabletop exercises and shared lessons learned. The next step in the evolution of such sector-specific coalitions is to engage in additional public–private interdependency tests. This is the quickest way to determine the effectiveness of a strategy that is untested for a region — elsewhere known as 'a plan in principle'.

One would hope that other government departments would use the Treasury as an example of how to foster the creation of the regional sector-specific coalitions and then ask the DHS to call for testing of interdependencies by region. In the Pacific Northwest, there is actually both a Treasury-recommended financial coalition as well as a regional public–private partnership devoted to testing interdependencies. Furthermore, a vote has been taken on whether or not the Treasury coalition should also be designated the Washington State DHS sector-specific organisation.

> 'The exercise did not investigate the willingness of employees to come to work in the context of the dangers — both real and perceived — posed by a pandemic.'[8]

It is not really possible to turn customer-facing jobs into remote tasks. While some institutions can rely upon delivery channels such as online banking, drive-through facilities or ATMs, employees or third-party providers are still needed to move the cash, tweak the servers, or sit in the drive-through window. It is still important to understand just what kinds of assurance institutions can provide to those who need and wish to come to work. Most organisations do not have in-house facilities in their data centres or high-occupancy buildings that could easily convert to housing for extended periods of time. Such organisations would be dependent upon local hotels, which will be equally disadvantaged by the pandemic. One of the questions being examined in Washington State is how to balance the needs of critical sector institutions to keep operating against the risk to service organisations which might have to find alternative ways to serve in an emergency. One can recall Manhattan hotels opening their doors to emergency workers during September 11th and providing food and supplies as well as shelter. While the impact of September 11th was harsh and sustained for over 30 days, the impact of a pandemic is estimated to be three times that of September 11th in terms of duration — and not isolated to a single city.

Thus, the question of what firms owe their employees and how they can be both educated and encouraged to work if they are healthy and able to be away from their families is still very much a work in progress.

> 'Financial institutions may wish to consider adding disaster preparedness education programs to their overall business continuity strategy if they do not currently exist.'[9]

Because of Occupational Safety and Health Administration requirements, most institutions have in place some sort of formal programme to educate their employees on evacuation of their building during an emergency. Many financial sector institutions run stories on their intranet sites for disaster preparedness month or set pointers to a public health site during influenza season. It is apparent that measures need to go much further. Part of the strategy at Washington Mutual has been to identify the interlinked components of a unified disaster response plan, and to try to operationalise it for single points of contact and confirmation during an event.

In developing a more comprehensive plan, an institution will want to pose a number of questions. Will all lines of business waive late fees, and over what period of time? Will small business programmes partner with the Federal Emergency Management Agency to keep small businesses afloat until their insurance cheques arrive? Will banks waive ATM charges, and will that be done in concert with all other financial institutions? Will institutions make charitable donations to the affected regions? Is there a pre-agreed announcement of what types of relief will be provided so that it can be quickly deployed as a sign in a branch or an ad in the newspaper? Will support be provided to customers and employees after disasters on a broader scale than the trauma counsellors, sensitivity training and childcare are deployed in other situations?

On the issue of employee education, Washington Mutual is looking at informal brown bag lunch presentations that tie disaster preparedness education topics to skills and understandings that are useful not only at work, but in connection with one's family disaster plan as well.

> 'Organizations may want to consider regular testing of the systems that will be used for telecommuting.'[10]

This seems essential to the identification of gaps, whether for a pandemic or one's regular business continuity programme. Some companies have asked their teams to work from home for a day to identify what they can or cannot do, or what they were unable to access from a remote location. This type of testing is likely to increase in frequency and horizontality in the next year. (It is worth noting that most who participated in the three-week national test did not telecommute for the test.)

> 'The financial services sector, in co-operation with federal authorities and communications service providers, may want to review existing authorities and emergency powers regarding the prioritization of network traffic to gain a better understanding of the capabilities, limitations, and availability of telecommunications and IT infrastructures during a pandemic.'[11]

As a regulator recently reminded, the internet is by architecture and design the free flow of unregulated traffic. Unfortunately, the unregulated nature of the internet could be the undoing of plans for coping during a pandemic. The social use of computers could render the plans useless if back office workers are unable to work from home. Thankfully, the Congressional House Financial Services and House Energy and Commerce Committees have asked the Government Accountability Office (GAO) to study the ability of 'the last mile' (to homes) to handle telecommuting in the event of a pandemic. It is hoped that the GAO report will include not only the analysis but a set of recommendations to prioritise traffic — even if it means shutting down other types of social traffic for prescribed periods each day.

> 'ATM availability often becomes a key customer concern in emergencies.'[12]

The 2006 National Infrastructure Advisory Council study extracted data from financial institutions designed to help better understand mutual dependencies, including the extent to which the same set of cash couriers are used. That remains a valid issue — perhaps more so now. Couriers will be equally disadvantaged by a pandemic, so one of the key questions is whether planning can take place to map pandemic routes in advance of the event. Identification of key facilities and which ATMs the bank will keep open during a pandemic would allow simplification of the routes and the volume for everyone. This is a key step forward in any single institution's pandemic strategy. Given sufficient time, it would be possible for financial institutions to collaborate to ensure that whole neighbourhoods are served by at least one, if not two, institutions. Rather than having the regulators decide for them, institutions should set the bar on what percentage of facilities they will keep open based upon what is reasonable given their scope and size.

> 'Participant responses indicate that there is potential value in the private sector opening a dialogue with the supervisory community to discuss identified concerns with regard to regulations.'[13]

It is difficult to know how to begin a discussion with the regulators on pandemic relief when it is not clear who has authority to draw up contingency plans for regulatory actions. This dialogue can be opened with the supervisory community on a company-by-company basis, to discuss concerns; or it is possible to work through organisations like the Financial Services Roundtable, the FSSCC or the FBIIC.

Discussion items here might include an extension of or waiver of regulatory reporting deadlines for Bank Securecy Act/Anti-Money Laundering (BSA/AML) and the USA PATRIOT Act, an extension of time to comply with consumer-related regulations, relaxation of branch closure/relocation notice requirements, easing of reserve and liquidity requirements, relief from prompt corrective action and capital rules, relief from Sarbanes-Oxley internal controls requirements, and relaxation of internal policies and procedures.

The Treasury Department's report, from which the foregoing recommendations and observations were drawn, is possibly the only report that examines, in detail, the key issues to consider around the threat of a pandemic. As said at the beginning of this paper, there is still time to get things right.

Supplementing the other three key 2007 documents referenced previously is the pandemic guidance released last December by the FFIEC. This recommends that a financial institution's business continuity plan provide for:

> '1) A preventative program … 2) A documented strategy … 3) A comprehensive framework of facilities, systems or procedures … 4) A testing program … and 5) An oversight program to ensure ongoing reviews and updates …'[14]

The FFIEC can be thanked for noting that a pandemic is a business-wide threat, not merely an IT threat, even though scrutiny of the programme will fall primarily within the IT component of examinations. The guidance references both the DHS pandemic guide and the national implementation plan mentioned earlier. There is also very close correlation between the FFIEC pandemic guidance and the after action report from the autumn 2007 test, as the regulators were involved in designing the test and certainly in reviewing the data from the test.

One of the more interesting sections of the guidance focuses on the identified risk of monitoring and testing components of a pandemic programme. Such a programme should include the following elements: clear roles and responsibilities; key planning assumptions; increased reliance upon online banking, telephone banking and call centres; and remote access and telecommuting capabilities.[15] The last paragraph of the guidance provides a comprehensive list of ways in which pandemic testing can occur.

How will the four documents affect a large financial institution that has been evolving a pandemic plan for several years?

In short, all four documents strengthen the case for banking and financial institutions to connect all the dots sooner rather than later. Perhaps the easiest way to illustrate why pandemic planning takes so long is to examine the course of action Washington Mutual has taken around the business processes that provide the foundation for its ongoing business continuity programme — this will show that planning for a pandemic is not as simple as one might have thought.

Washington Mutual's Pandemic Flu Task Force was founded in October 2005. The agenda has been fairly simple: to increase the probability, year over year, that the company would be able to respond to and recover from a predictable surprise, such as a pandemic, with some degree of finesse. In June 2006, nearly seven months after the task force had begun to shape an initial strategy, a company-wide session was held with senior managers to identify the mission-critical and critical business processes that would be essential to keep running in a pandemic, the processes that could be reduced in frequency, and those which could be suspended. To prepare for this session, the Office of Continuity Assurance (OCA) conducted interviews with subject matter experts in the business segments, focusing on what were then 2,700 company business processes. To facilitate discussion, the OCA team created a draft document sorting each process into one of the three pandemic categories. The predictable surprise in the work with the senior vice presidents was that many business processes — over 1,100 in fact — that were not 'mission-critical' (recovery for those processes defined as 8 hours or less) or 'critical' (recovery defined as 8–24 hours) in the regular programme became vital for a pandemic, the duration of which was assumed in planning to be 12 weeks or more. The work from the day-long session was used as the first cut, and the pandemic questions and criticality ratings have since been integrated into the annual business impact analysis. Every year since then, the processes have been reviewed again to ensure they still fit the criteria, and there is now both a standard and a pandemic designation for business processes. The plans for a pandemic are built around the human resources necessary to maintain processes — including critical workers, delegation of authority and vendor dependencies. The second full year of data entry is now coming to an end. This work has been painlessly integrated into regular programme work.

Still, there remains the very large task of figuring out how to take this information and make it operational and actionable. How will the pandemic plans be driven out from the repository where they sit so that all employees understand what is expected of them when a pandemic occurs? Education campaigns around future unpredictable events are challenging when employees are so focused on immediate projects. Bazerman points out that:

> 'Organizations aren't structured with the intent of identifying threats. They have silos that prevent information sharing, and have dysfunctional incentives that don't provide rewards for investing to fix problems not even apparent.'[16]

The goal for every financial sector institution during a pandemic event is to stay in business and to serve customers. While ensuring that this is done, it is also vital to focus on other critical tasks. Back-room risk management teams must track the processes that have been suspended or reduced across the company in order to enable reporting and analysis once teams are engaged in recovering from the event. Financial institutions cannot afford to lose track of Sarbanes-Oxley and Basel accountabilities around financial reporting and loss data, even as they juggle to keep cash in ATMs, ensure that online banking remains available to customers, prevent fraud, and keep customer-facing employees as safe and healthy as possible as they fulfil the company's responsibilities to its customers. More thought is required to bring firms over the hump once plans have been documented and are sitting in a repository. There is still time to act on the after-action observations and to formulate recommendations. There is also a need to increase horizontal testing across all critical sectors, not just within the financial sector. Washington Mutual has worked with public and private partners across five to six of the 17 critical sectors with varying degrees of success in integrating its plans and its testing programme into something larger than its single efforts.[17] All of this takes time, and at least so far there is still time.

References

(1) Bazerman, M. H. (2007) 'Predictable surprises: Blind spots in pandemic planning', in 'Business Preparedness for Pandemic', Harvard Health Publications, Boston, MA, pp. 30-31.
(2) Department of Homeland Security (2007) 'Summary of the National Infrastructure Protection Plan and the Sector-Specific Plans', Government Printing Office, Washington, DC.
(3) Homeland Security Council (2007) 'National Strategy for Pandemic Influenza Implementation Plan One-Year Summary', Government Printing Office, Washington, DC.
(4) Department of Homeland Security (2006) 'Pandemic Influenza Preparedness, Response and Recovery Guide for Critical Infrastructure and Key Resources', Washington, DC, available at: http://www.pandemicflu.gov/plan/pdf/cikrpandemicinfluenzaguide.pdf (accessed 10th June, 2008).
(5) Financial Banking Information Infrastructure Committee and Financial Services Sector Coordinating Council (2008) 'The FBIIC/FSSCC Pandemic Flu Exercise of 2007 After Action Report', Washington, DC, available at: http://www.treas.gov/offices/domestic-finance/financial-institution/cip/pdf/pandemic-flu-report-012008.pdf (accessed 10th June, 2008).
(6) *Ibid.*, p. 48.
(7) Developed coalitions include Alabama Recovery Coalition for the Financial Sector, BARC*first* (San Francisco), ChicagoFIRST, *dfw*FIRST (Dallas), FloridaFIRST (Miami and Tampa Bay), HawaiiFIRST, HoustonFIRST, Minnesota ISAC, Minnesota Security Board, NCRfirst (Washington, DC), Pacific Northwest Regional Coalition for Finance, and SoCal*first* (Los Angeles). Forming coalitions include: ArizonaFIRST, Colorado, Del-ValFirst (Philadelphia and Delaware Valley), GeorgiaFIRST, MemphisFIRST, Financial Recovery Coalition of North Carolina, ShowMeFIRST (Missouri), and Virginia1st.
(8) FBIIC/FSSCC, ref. 5 above, p. 48.
(9) *Ibid.*, p. 49.
(10) *Ibid.*, p. 49.
(11) *Ibid.*, p. 49.
(12) *Ibid.*, p. 49.
(13) *Ibid.*, p. 50.
(14) Federal Financial Institutions Examination Council (2007) 'Interagency Statement on Pandemic Planning', Washington, DC, p. 3, available at: http://www.ffiec.gov/press/pandemicguidance.pdf (accessed 10th June, 2008).
(15) *Ibid.*, p. 9.
(16) Bazerman, ref. 1 above, p. 31.
(17) For description of second-year efforts, see Searle, A. (2007) 'Pandemic flu planning in the US financial services sector', *Journal of Business Continuity & Emergency Planning*, Vol. 1, No. 3, pp. 292-301.