CURRENT BUSINESS CONTINUITY PRACTICES AND PANDEMIC INFLUENZA: IMPLICATIONS FOR PRIVATE SECTOR RESILIENCY

A Thesis
Presented to the
Faculty of
San Diego State University

In Partial Fulfillment
of the Requirements for the Degree
Master of Science
in
Homeland Security

by
John Gerald Putnoky
Spring 2011
SAN DIEGO STATE UNIVERSITY

The Undersigned Faculty Committee Approves the
Thesis of John Gerald Putnoky:

Current Business Continuity Practices and
Pandemic Influenza: Implications for
Private Sector Resiliency

Eric G. Frost, Chair
Homeland Security Program

Jeffrey S. McIlwain
Homeland Security Program

Robert Pozos
Department of Biology

04.22.2011
Approval Date
Copyright © 2011

by

John Gerald Putnoky
DEDICATION

This thesis is dedicated to Dr. and Mrs. Gilbert Putnoky for their unwavering support in all my endeavors. Your unique ability to provide guidance without interference is something I will always treasure.
ABSTRACT OF THE THESIS

Current Business Continuity Practices and Pandemic Influenza: Implications for Private Sector Resiliency
by John Gerald Putnoky
Master of Science in Homeland Security
San Diego State University, 2011

Business continuity planning is critical to private sector resiliency in the face of numerous internal and external threats in the globally networked business environment. Additionally, homeland security is dependent on the economic viability of the American business community, so the risk of inaction in the private sector is unacceptable. The pandemic influenza threat is especially taxing on businesses, and brings second order impacts with severe economic consequences for the United States as a whole. Lack of business continuity planning effort before the pandemic threat materializes among companies of all sizes will have detrimental impacts beyond the scope of this thesis. The combined pandemic-induced impacts of absenteeism, health care system breakdown, unpredictable government reactions, and general infrastructure failures will severely impact homeland and national security. These impacts will be exacerbated by add-on or seasonal disasters.

Typically government officials have little fluency in private sector resiliency efforts. This thesis provides an outline of current business continuity procedures and uses pandemic influenza to model specialized business continuity recommendations. Business continuity planning is an ongoing project run by a business continuity manager within an organization. The business continuity life cycle is only successful with endorsement from organizational leaders and clear communication of objectives. Business continuity planning must be pan-organizational and include a threat assessment, risk assessment, business impact analysis, and detailed business continuity plan. The plan itself must be updated as the organization evolves over time and must be exercised regularly to ensure employees and managers are confident in its usage.

Effective business continuity can guide decision makers from the time a pandemic (or other threat) emerges to the time recovery starts and help avoid foggy decisions typically caused by the stressors of a disaster. Strong decisions and communication guided by the continuity plan allow the business to avoid undue losses to personnel, capital, and/or reputation. The mitigation and planning efforts of the business continuity project builds resiliency in the business that allows it to contribute to regional response and recovery efforts. Most of all, strong business continuity efforts preserve the most important component of any business—its people.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABSTRACT .............................................................. v</td>
</tr>
<tr>
<td>LIST OF TABLES .......................................................... viii</td>
</tr>
<tr>
<td>LIST OF FIGURES ........................................................... ix</td>
</tr>
<tr>
<td>ACKNOWLEDGMENTS .......................................................... x</td>
</tr>
</tbody>
</table>

## CHAPTER

1 INTRODUCTION ............................................................... 1
   Background ................................................................. 4
   Business Continuity Regulation ........................................ 6

2 DEFINING BUSINESS CONTINUITY ....................................... 12
   The BC Planning Process .................................................. 14
   Project Initiation and Justification .................................... 15
   Risk Assessment ............................................................. 18
   Threat Assessment .......................................................... 22
   Business Impact Analysis ................................................ 23
   Mitigation Strategy Development ....................................... 34
   Business Continuity Plan Development .................................. 35
   BC Plan Exercising and Training ....................................... 38
   BC/DR Plan Maintenance ................................................... 41

3 DEFINING THE THREAT: INTELLIGENCE ON INFLUENZA AND H1N1 ............................................ 43
The Science of Influenza .......................................................... 43
A Brief History of Recent Influenza Pandemics ......................... 48
The H1N1 Outbreak of 2009 ...................................................... 49
General Public Health Implications of Influenza ....................... 52
Shortfalls and Gaps in the Vaccine Supply Chain ...................... 53

4 REVISIONING BUSINESS CONTINUITY EFFORTS TO FACE THE PANDEMIC THREAT ................................................................. 56
  Gauge Government Response ............................................... 56
  Comprehend the Potential Human Impact .............................. 58
  Understand the Pros and Cons of the “Work at Home” Solution .... 60
  Enhance Communication Strategies ..................................... 65
  Go for the Basics by Mitigating the Viral Risk ....................... 67
  Write a Pandemic-Specific Continuity Plan ......................... 67
  Reach Out with Pandemic Preparedness Activities ................. 71
  Effectively Exercise the Pandemic Plan ................................. 72

5 CONCLUSIONS ........................................................................... 74

BIBLIOGRAPHY ........................................................................ 76

APPENDICES

  A KEY ORGANIZATIONAL STAKEHOLDERS IN BUSINESS CONTINUITY PLANNING ................................................................. 78

  B TIME-RELATED DEFINITIONS USED DEFINED BY MANAGER WITH ORGANIZATIONAL STAKEHOLDERS DURING THE BIA ........ 83
LIST OF TABLES

Table 1. BC Proposal Elements Critical to Executive Buy-In ..................... 15
Table 2. Components of Risk to Be Considered in a Risk Assessment ............. 19
Table 3. Sub Risks Defined During Risk Assessment ................................. 20
Table 4. The Primary Purposes of the BIA According to the BCI ................ 23
Table 5. Organizational Impacts of Disruption ........................................ 33
Table 6. Major Pandemic Influenza Outbreaks of the Twentieth Century ........ 49
## LIST OF FIGURES

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 1</td>
<td>The business continuity lifecycle</td>
<td>14</td>
</tr>
<tr>
<td>Figure 2</td>
<td>Example rating system for functional criticality during BIA</td>
<td>26</td>
</tr>
<tr>
<td>Figure 3</td>
<td>Input to output relationship of BIA components</td>
<td>28</td>
</tr>
<tr>
<td>Figure 4</td>
<td>Business continuity exercise variants</td>
<td>39</td>
</tr>
<tr>
<td>Figure 5</td>
<td>Pandemic incidence over time with key waypoints</td>
<td>53</td>
</tr>
<tr>
<td>Figure 6</td>
<td>“PPE” strategy for pandemic influenza mitigation activities over time</td>
<td>61</td>
</tr>
<tr>
<td>Figure 7</td>
<td>Pandemic response plan annexes</td>
<td>69</td>
</tr>
</tbody>
</table>
ACKNOWLEDGMENTS

This thesis would not be possible without the collaboration of my thesis committee, inspiration from my fellow students in the Homeland Security Master’s Degree Program, and the professionals in the business continuity management community who fight the battle for private sector resilience on a daily basis. I am especially thankful to my thesis chair, Eric Frost, for recruiting a “biology guy” into the Homeland Security Master’s Degree Program.
CHAPTER 1

INTRODUCTION

The study and implementation of business continuity planning in the context of a pandemic influenza is extremely timely and imperative in light of current events. In the spring of 2009, the globe was engulfed with a public health hysteria spurred by the emergence of a novel influenza strain in Mexico called H1N1. The rapid spread of this novel strain across the world was well tracked by public health authorities as well as private sector groups such as Google flu trends. From June to September of 2009, the Southern Hemisphere experienced the wrath of H1N1. As schools began to resume in the United States in the early fall, the media increased its coverage of the H1N1 pandemic. Public health and other government authorities, including the Department of Homeland Security, issued statements to the public and private sectors on prevention and mitigation strategies. Vaccine suppliers across the world ramped up production of vaccines and distributors attempted to get the vaccine to patients in a timely fashion. Despite much effort to combat what turned out to be a relatively mild viral foe in H1N1, the vaccine suppliers and distributors ran into many setbacks—failures that will have fatal consequences in the event of a more virulent strain of influenza. The H1N1 pandemic of 2009-2010 was quite minor when compared to other pandemics of the twentieth century, especially when compared to the 1918 “Mother of All

Pandemics.” However, the recent H1N1 outbreak should be considered a “near miss”—next time the impacts might not be so trivial and business continuity management within the private sector must plan for future pandemic threats.

The next great pandemic is not a matter of if, but of when. The US economy is a leader in global innovation and economic influence so that the pandemic actually represents both an extraordinary risk and opportunity to assist the world. Additionally, the US government and associated security apparatus depend heavily on the private sector for survival, so private sector response is of extraordinary importance, not just government response. According to The 9/11 Commission Report, “the private sector controls 85 percent of the critical infrastructure in the nation.” It continues, “Homeland Security and national preparedness therefore often begins with the private sector.” This is doubly true in the case of pandemic. The US Centers for Disease Control and Prevention (CDC) estimates that a mild unmitigated pandemic could infect 30 percent or more of the US population (or approximately 100 million people). Taking into account the combined impacts of seasonal influenza with a novel pandemic strain, the impacts and infection rate will be overwhelming

---


to the health care system. This health crisis scenario and the government response to it will have repercussions beyond the health care industry. Every business would feel the impact on some level. Loss of one or more essential services, school closures, and absenteeism will impact the private sector in an absolute way. When businesses are impacted, local communities suffer. The even more serious combination of a “routine” local disaster such as a hurricane or wildfire with the global pandemic is a plausible scenario that could exacerbate the impacts in an overpowering way. Other disasters will continue and may even be exacerbated by absenteeism from pandemics, so combinations of disasters and their impact on society should be considered as plausible scenarios to prepare for and mitigate.

In the event of a severe pandemic, many businesses will become insolvent without adequate planning or prevention measures to protect their infrastructure and workforce. The aggregation of private-sector impacts resulting from an unmitigated and unplanned for pandemic on a national scale could cause a significant weakening of the US on the global stage. The scale and scope of current business continuity practices do not effectively integrate pandemic preparedness into business continuity plans—especially when one considers the high stakes of an unmitigated pandemic on the business community and the second-order impacts throughout the country.

What follows is an introduction to the field of business continuity and how business continuity planning is carried out in the business environment. As an example in order to

develop the needed specificity, this study focuses on influenza and the last major world influenza event (H1N1), but the business continuity planning process crosses most potential disasters, so this event is a model for what most other disasters would also entail. In order to deal with the real business continuity system, an assessment of the influenza threat in regards to business is discussed as are lessons learned from the lenient H1N1 2009-2010 pandemic. From this detailed example, an analysis is then done to explore how business continuity practices can be improved to counter the next influenza outbreak.

**BACKGROUND**

To comprehend what Business Continuity Management (BCM) is, it is useful to understand its beginnings. From its origins in the 1980s, until the early 1990s, BCM was present, but largely found in the domain of the IT department with a focus on recovery following disruption to technology-driven systems. In its early days, business continuity (BC, for short) was conducted around the backup and recovery of data stored in large anonymous computer server boxes off site. Typically these servers were the size of semi-trucks or larger and only a handful of individuals within the business carried out the backup and server-site location activities surrounding the concept. This is in direct contrast with current IT-intensive business models.

The modern form of BCM has its origins in two impetuses. One impetus was an uptick in terrorist activities in the 1990s and the other was the expansion of the IT

---

functionality throughout business organizations. The terrorist actions brought into focus a recognition by corporations that there was a wider business need for the availability of a response and recovery framework to follow for disruptions outside the IT environment. The spread of IT from a massive-scale server facility to the desktops of almost every employee caused a literal dispersion of the historical IT roots of business continuity throughout the organization, outside the boundaries of the previous IT environment. Business continuity had a significant ramp-up in the UK during the mid 1990s due to the Irish Republican Army bombing of the Manchester city centre and financial district in 1996. An eye-opening fact to come out of this action is that around 40 percent of the businesses that were impacted in the downtown district in this terrorist incident closed after the bombing and never traded again. There was clearly no continuity and the terrorist act had profoundly more impact than might seem obvious, with a significant part of this impact being the lack of viable business continuity plans and practices.

The events of September 11, 2001, are widely regarded as the biggest impetus for the field of business continuity management in its modern iteration. The events of 9/11 heightened regulatory interest in BCM especially in the US, UK, Japan, and Australia where further papers and guidelines were issued in the wake of the disaster. 9/11 woke companies up to the fact that they need to widen the scope of their planning to include failures of national utilities, financial markets, and transportation routes. Since 9/11 the cybersecurity


of critical infrastructure has made companies increasingly aware of their networked dependencies. *The 9/11 Commission Report* makes a valid statement on the matter of business preparedness when it states: “Private-sector preparedness is not a luxury—it is a cost of doing business in the post 9/11 world. It is ignored at a tremendous potential cost in lives, money, and national security.”

**BUSINESS CONTINUITY REGULATION**

Since September 11, 2001, there has been a general push by governments in capitalist nations for defined regulations specific to the field of BCM. However, this effort has resulted in a multitude of documents, recommendations, and “half-standards” having no penalties or legally binding rhetoric. Currently, the area of business continuity standards is highly controversial and what justifies a “standard” is still up for debate in the BC professional community. With few exceptions, current business continuity standards are not followed with the specificity of other broad-based compliance documents (e.g., Sarbanes-Oxley). The BC standards that are followed by the letter tend to be based regionally (BS25999 in the UK, for example).

Currently, despite the lack of a single broad-based standard or best practice, most regulated private sector organizations (and those entities which regulated organizations deal with through supplier or outsourcing arrangements) are required by regulators to have in place a risk-based BCM framework, including an appropriate business continuity plan. This


BC plan implementation stems from an industry-specific regulation (e.g., financial services) and not from a broader business continuity regulatory body. The financial industry in the United Kingdom and Western Europe are considered the groundbreakers in regulating BCM. It is generally accepted that what the Europeans (and especially the British) do with regard to the field of BCM, other Western countries soon follow. Therefore it is of use to understand BC from the European context.

The origins of European and British regulation when it comes to BCM are found in the Basel II and Civil Contingency Act. These documents required various financial organizations of the EU and UK to have business continuity plans in place. However, they provided no framework for businesses to follow and give no detail on how much detail was supposed to be included in subsequent planning activities. In reaction to the lack of framework laid out by Basel II and the Civil Contingency Act, the British Standards Institute (BSI), in conjunction with Business Continuity Institute (BCI) published Publicly Available Standard 56 (PAS 56) as a guide for BC activities that established the process, principles, and terminology of business continuity management (BCM). Specifically, PAS 56 described the activities in and “outcomes” of establishing a BCM process, and provided a series of recommendations for good practice. PAS 56 was by no means a comprehensive BC standard, but provided an important source document for the formal BSI standards to follow, namely BS25999-1 & 2.


BS25999 is a more detailed UK-published BC standard describing the activities and outcomes of establishing a BCM process.\textsuperscript{16} It also provides a series of recommendations for good practice. It is split into two sections. BS25999-1 officially replaced PAS 56 upon its publishing in November 2006. BS25999-2 defines the requirements for a management systems approach to BCM and was published in November 2007. BS25999 was written by the BCI and Insight Consulting, but also incorporated the insights of other UK companies including EDS, Sainsbury’s and the Post Office. The purpose of BS25999 is to provide a framework for the BC manager tasked with implementing BCM within an organization. It describes a process for the manager to use and offers a range of good practice recommendations. BS25999-2 offers the basis for certification.\textsuperscript{17} It also defines management systems requirements within a specification that can be used by external or internal BC solutions. In US business continuity circles, BS25999 remains controversial as a whole because of a minority movement to adopt BS25999 as an “American” standard for BCM. Despite this backlash stemming from what the author sees to be nothing more than national pride in American financial freedoms, BS25999 is generally respected as the leading standard of the BCM field on the conceptual level.

As mentioned previously, within the US, business continuity regulation has been quite weak outside of industry-specific guidelines. In January 2004, following the terrorist attacks of September 11, the 9/11 Commission investigated the preparedness of private-sector

\begin{itemize}
\item Andrew Hiles, \textit{The Definitive Handbook of Business Continuity Management}, 2nd ed. (Chichester, England: John Wiley & Sons, 2007).
\end{itemize}
organizations and asked the American National Standards Institute (ANSI) to develop a consensus on a “National Standard for Preparedness” for the private sector. The resulting product from the ANSI’s Homeland Security Standards Panel was that the Commission backs a voluntary National Preparedness Standard in the form of an updated NFPA 1600. With NFPA 1600 being a voluntary standard, many companies simply ignore it and do not follow through with its areas. With regard to public health, NFPA1600 in its current iteration mentions the Health and Human Services website and has no specific provisos for pandemic influenza. NFPA 1600 falls short when it comes to pandemic and pandemic-specific BCM efforts are critical to successful pandemic response. The initiative to ensure pandemic preparedness should come from within the business, not from an overarching government regulation or mandate.

BC regulation regarding outsourcing is worth special mention because the network of outsourcing and supply chain agreements comes under special stress during a pandemic event. Cost reduction and finding new customers are key business considerations in recent times due to the restrictive economic climate. One of the key ways companies are achieving these considerations is through outsourcing. From the UK regulatory standpoint, BS2599-2:2007; 3.2.3.3 states: “Top Management shall appoint or nominate a person with appropriate seniority and authority to be accountable for BCM policy and implementation.” Based on


20. “BS 25999 Business Continuity.”
this specification it seems clear that the BCM should be involved in any outsourcing project, since it represents a significant change in the way business is being conducted. In reality, however, this is not always the case. The company outsourcing its process to a contractor is prone to use a “out of sight, out of mind” mentality since if the process were highly important it would most likely have been kept in-house.

Outsourcing is a business activity surrounded by good practices, standards, and regulatory requirements (especially in bio/pharma, information technology, and financial industries). Depending on which regulatory requirements are consulted, one or more specifications can be found. To produce significant and beneficial results, outsourcing must be based on a written contract. The outsourcing organization must have an outsourcing policy covering procedures and continuous follow-up on the risks involved in outsourcing. In outsourcing one must include the establishment of ongoing and effective business continuity and information security monitoring programs. In an ideal scenario, the BC manager will be consulted during the formation of the outsourcing contract. If this is not the case, it is imperative that the BCM manager does see the contract at some point before project initiation for comment. Outsource providers will go to great lengths to limit their liability. This could be related to a fixed financial amount or to the level of service fees paid, or any other limiting condition.

Outsourcing contracts typically contain a clause for Service Non-Performance or Force Majeure. When analyzing the definitions of Force Majeure we often find that situations like fire, flood, explosion, social event, etc., are all included as part of the definition. In the

context of business continuity planning, this is unacceptable. One of the key reasons to set up a business continuity management system is to build a response-and-recovery capability that is able to handle major operational disruptions. Another observation that outsourcing companies systematically do not yet take advantage of are the business continuity standards available today laid out today, especially the BS25999 series. Rather than referring to the business continuity standard of choice and imposing a certification process on the provider, the outsourcing party should clearly describe what the provider should be doing with regards to BC management (plans that need to be written, tests that must be executed, etc.).

Contractual definitions regarding business continuity management must be the same as the BCM standards (BS25999-2:2007, SS540:2008, NFPA1600:2007, etc.). Reality shows that there is often room for confusion when citing standards in contracts. One example is the varying definition of “incident management.” This term as used in NFPA 1600 is not the same as what is meant in BS25999-2—where an incident is considered to be a major operational disruption.
CHAPTER 2

DEFINING BUSINESS CONTINUITY

Now that the background and regulatory status of business continuity have been laid out, the appropriate context is available to define the field of business continuity management (BCM) for the purposes of this thesis. BS25999 defines BCM as:

A holistic management process that identifies potential threats to an organization and the impacts to business operations that those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.\(^{22}\)

This amalgamation of management seminar buzzwords is actually quite descriptive if the reader breaks it down to its core. A leading figure in the BCM field, Andrew Hiles, simplifies the definition to “a management system that enables an organization to improve its security and resilience and make sure it can respond immediately and effectively to a major incident.”\(^{23}\) One key product of the BCM lifecycle—to be discussed in more detail later in this thesis—is the Business Continuity Plan (BCP). A continuity plan focuses on sustaining the company’s business activities, particularly those related to revenue generation and management of corporate commitments\(^{24}\) (employee payroll and health care insurance are


two notable examples). A business continuity plan can be written for a specific business process or all key business processes.

It is the author’s opinion that no current definition of business continuity captures the essence of what business continuity is in practice. In practice, business continuity has no set definition because it means different things to different companies and is as varied as each individual corporate culture. Some companies have set continuity of operations plans that focus solely on staying open during a crisis at all cost. Other companies have plans that define how to get started after a disaster. The business continuity process tries to plan for the time between the striking of the disaster and when the recovery starts. This tumultuous period is when the company is most vulnerable to clouded judgment leading to bad decisionmaking. Planning during “fair weather” allows for logical and rational decisions to be made before the disaster strikes.

For the purposes of this thesis (keeping in mind the expansive temporal and geographic uniqueness of a pandemic event) business continuity management is not just about a response to a disaster situation. BCM is about building resilience to strengthen an organization in light of inevitability before the crisis. BCM builds a structure to gain intelligence on what might be at risk and developing strategies for when things do go terribly wrong. BCM is about having enterprise-specific plans not one-size-fits-all solutions. Legitimate BCM must be embedded in the organizational culture and in day-to-day management practice. Business continuity builds private-sector resilience following a disaster.
THE BC PLANNING PROCESS

Business continuity is an ongoing sequence that encompasses key definable waypoints throughout a methodical process. The individual or team who becomes responsible for this process would be best served to take a broad-based approach to planning and work with individuals throughout the business, from the CEO to the custodian staff. BS25999-1 defines business continuity as a cycle (Figure 1).

Figure 1. The business continuity lifecycle.

This representation is useful for defining the overall vision for a BC program within an organization because it emphasizes understanding the organization and exercising, but leaves out details important to building a more resilient organization. The six elements of the BS25999-1 lifecycle are action items that should all be incorporated into any successful
business continuity program. Typically, the BC lifecycle becomes more useful if it is broken down into more definable waypoints. The following portion of this thesis will do just that.

**Project Initiation and Justification**

Getting a BC planning project off the ground is a challenging and daunting task, but is critical to determine the BCM strategy that will be moving forward. Making the right decisions, taking the right actions, and setting up a plan for successful implementation starts with a robust justification process. Any good project starts off with a proposal. Proposals for BC planning projects should incorporate the elements laid out in Table 1. Once the proposal has been accepted, the BC manager should start engaging with the key contributors to the plan and letting them know what responsibility they hold.

**Table 1. BC Proposal Elements Critical to Executive Buy-In**

<table>
<thead>
<tr>
<th>Proposal Element</th>
<th>Executive Question Being Answered by Element</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business case</td>
<td>Why is a BC plan needed, and what is the mission?</td>
</tr>
<tr>
<td>Financial analysis</td>
<td>How much will the project cost?</td>
</tr>
<tr>
<td>Metrics: Timeline, budget, and quality</td>
<td>How will the project manager be held accountable?</td>
</tr>
<tr>
<td>High-level resource needs</td>
<td>How many people are going to be working on this?</td>
</tr>
<tr>
<td>Phase schedule</td>
<td>Since everything cannot be done at once, how will the project be created?</td>
</tr>
<tr>
<td>Success criteria</td>
<td>How will the leadership know if the project is truly adding value to the company?</td>
</tr>
<tr>
<td>Risks, mitigation, and alternatives</td>
<td>How might the project come to fail or lose value for the company?</td>
</tr>
<tr>
<td>Recommendations</td>
<td>What can the board (or other senior leadership) give in terms of guidance or insight to the BC process?</td>
</tr>
</tbody>
</table>
The buy-in obtained from upper management through the approved proposal gives the BC manager the leverage to take the time and resources of the key contributors. Key contributors will vary from company to company, but typically they include key stakeholders in a few areas outlined in Appendix A.

Engaging key stakeholders without buy-in from senior leaders within the organization is generally counterproductive. Therefore, it is imperative to have the blessing of the senior leaders before the BC manager uses his or her time and the time of the key stakeholders. Justifying the BC planning process to executives or corporate leadership is a daunting task. In business today, budgets and capabilities are often stretched to the breaking point. Highly charged issues such as security and regulatory compliance garner the most visibility. Some organizations are reluctant or even unwilling to devote time or money to developing business continuity plans, much less pandemic plans. Even though foregoing a BC program is a sub-optimal long-term business decision, the demands on a company’s resources can be such that BC planning is not valued or appreciated by the senior leadership.

When pitching BC to executives, it is important to contextualize it for them. Executives understand business and finance, not business continuity planning. When explaining the BC project to them, the BC manager must avoid using technical lingo and BC-specific terminology that can lead to confusion. It is important to stay on point and keep the justification for the project simple. Corporate leaders are busy and want things explained in a way to help them quickly assess the situation and make a rational decision. The BC manager should strive to help them come to the decision on their own. Consequences of not building resilience and planning might include: loss of work to competitors, failure in the supply chain, loss of reputation, human resource issues, health and safety liabilities, or higher
insurance premiums. Typically disasters impact the business with more than one of these consequences leading to a worst-case scenario that will quickly put a company out of business.

One useful strategy for getting executive support is to show them that it is possible to win new business by using the BC plan as a sales differentiator. Companies are slowing down their spending and are reviewing every buying decision with greater scrutiny. The competition for these few available dollars is intensifying, as every company is looking at the value (return on investment) that they supply. Leveraging the business continuity plan as a differentiator can help the company stand out as a leading and trusted supplier, thus adding specific value for obtaining business and not simply being a cost item. Having a valid and tested business continuity plan demonstrates to customers the preparation to meet contractual timelines despite unforeseen disasters. Sales representatives are always looking for a reason to get in front of their current and potential customers in order to build closer relationships to gain their trust. Discussing the BC efforts with a customer is just such an opportunity and can be a significant differentiator of companies, which can actually assist in building revenues for the company even if the plan is never actually used.

Executives can sometimes be sold with the promise of cost savings. Corporate insurance is generally expensive and getting more expensive every year. Leveraging the business continuity plan, as well as its managers’ knowledge of the environmental-and


business-related risks, can help the company reduce the cost of insurance and thus directly enhance the company’s bottom line. As will become clear later in this paper, the business continuity process can expose organizational redundancies and inefficiencies. Exposing these can help the company survive during difficult economic times and squeeze every drop of possible profit out of the business during good times. Sometimes corporate leaders mandate across-the-board cuts such as “reduce headcount by 10 percent in all departments.” When the unpleasant time comes to cut the size of the workforce, executives have a difficult time determining where to make cuts while maintaining the strongest possible productivity.

Business continuity planning can minimize the impact of a reduction in force by using the business continuity manager’s knowledge of where to cut costs with the smallest impact on the business as a whole. If the business continuity planner has been doing his or her job, he or she should understand where the resiliency of the organization is highest. He or she should know what resources are underutilized or overlooked.

When trying to gain support for the BC process, the manager should demonstrate that the project has a clear and definable end-point and is not a bottomless drain on time and resources. The manager should provide the company leaders with a ballpark estimate of how long the project will take and how much it will cost in terms of time and money up-front. The finance key stakeholder should be consulted at the inception of the project, defining cost and time estimates as best as possible early on.

**Risk Assessment**

After company leadership and key stakeholders are behind the project the BC manager should move on to building an understanding of the organization’s risk profile. Risk
is “the chance of injury, damage, or loss.” Table 2 gives an explanation of how the definition of risk can be parsed out into its components for further understanding the relationship between common terms thrown around in the risk management and emergency management community.

Table 2. Components of Risk to Be Considered in a Risk Assessment

<table>
<thead>
<tr>
<th>Risk Equation Component Definitions</th>
<th>Component Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk (=) Threat (+) (\text{Likelihood} + \text{Vulnerability}) (+) Impact</td>
<td>Pandemic</td>
</tr>
<tr>
<td>Threat (=) \text{the event}</td>
<td>High</td>
</tr>
<tr>
<td>Likelihood (=) the probability of the event occurring and impacting the business</td>
<td></td>
</tr>
<tr>
<td>Vulnerability (=) The extent in which the organization is not prepared or defended from the threat</td>
<td>Many unvaccinated employees, so highly vulnerable to pandemic disruption</td>
</tr>
<tr>
<td>Impact (=) the severity of the threat on the organization</td>
<td>High. Losing two sales representatives during bid season will cause $1M loss.</td>
</tr>
</tbody>
</table>


There are a few different approaches an organization can take to risk. Management can accept the risk and do nothing. They can avoid the risk by doing something else, like moving to a safe location when a hurricane is approaching. They can reduce the risk by changing the equation, like installing a generator to ensure backup power. They can contain the risk by spreading their assets around. Finally, they can transfer the risk by giving it to somebody else. One example of transferring risk would be outsourcing.

There are various types of risk including, but not limited to, business risk, financial risk, compliance risk, and operational risk. Each type of risk has a sub risk defined by its potential impact and likelihood (Table 3).

<table>
<thead>
<tr>
<th></th>
<th>High Impact</th>
<th>Low Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Impact</td>
<td>High Likelihood</td>
<td>Low Likelihood</td>
</tr>
<tr>
<td>Low Impact</td>
<td>High Likelihood</td>
<td>Low Likelihood</td>
</tr>
</tbody>
</table>

By defining what types of risks an organization faces, the leadership can classify or determine the stance the company will take in face of the risks. The leadership can determine the level of risk they find acceptable. They can allocate resources to develop strategies to avoid or mitigate the risk. They can determine who is accountable for managing the risk and maintaining controls. They can determine what risk will be left over after accounting for mitigation activities. Most importantly, they can determine an early warning system for detecting risks that are becoming active dangers to the organization. The business continuity manager is responsible for understanding the risk detection mechanism because later it will need to be integrated into the business continuity plan.

While the senior leaders are responsible for the overall internal control systems and policies of the organization, it is the management of the subdivisions who bear responsibility for implementing policies adopted by the senior management. The inherent risk management of these day-to-day business decisions is separate from the BC plans until the decision leads to an outcome. A formal risk manager in a large company usually manages day-to-day business risk. This individual or team should be a close ally of the BC manager, but not a
substitute. The risk manager conducts ground-level audits and generates reports for the senior leaders. By spreading this accountability across the different divisions of the organization, the leadership gets a holistic approach to risk management, and the BC manager has a wide view of the organization’s risk profile.

While on the topic of risk, it is important to point out that a common objection to BC planning is that there are too many things that could go wrong for an organization to effectively plan for them all. This is in some ways true, but just because thousands of things can go wrong, an exponentially smaller number of things are actually likely to go wrong. Just because something may not happen does not mean that it shouldn’t be planned for. It is up to the BC planner to integrate a risk assessment into his or her planning process to determine the scope of what can go wrong, what the likelihood of it is to go wrong, and then to integrate this risk assessment into the broader context of the BC planning cycle. The BC plan is only one component of risk management within a company, not the other way around because the BC planning project within a company is a risk mitigation strategy.

As stated previously, most organizations have already done some risk assessments in relation to decision-making within the company. This is especially true on the financial, legal, and regulatory fronts. Most companies take a simple process of looking at the possible threats their decisions can lead to, and how vulnerable the company is to becoming impacted by those threats should they go through with their decision. The BC manager should consult with management about data and processes used to make decisions for the organization, since these data typically provide the raw materials for assessing risk.
Threat Assessment

Threat assessment targets certain disaster scenarios and determines what their impact would be on an organization. The outcome of the threat assessment should be two separate ranked lists of threats. One list should be a list of threats according to likelihood. The second list should be a list of threats according to impact. For example, if a company supplied by one power line that transverses a windy ridge to get to the facility, it is likely that there will be a power outage. If the business sits on top of a major earthquake fault that is overdue, it is likely that the business will be highly impacted if the fault ruptures causing a quake larger than 6.0 magnitude. There are many types of threats outside the scope of this paper, but it is worth mentioning them as to provide context for the typical BC process. Flood, fires, earthquakes, drought, sabotage, theft, vandalism, labor disputes, terrorism, workplace violence, cyber attacks, war, oil supply disruption, utility loss, regulatory shifts. The threat of H1N1 will be defined later in this paper.

The threat assessment should be completed using past history, sensor networks, visualizations, and public/private cooperation as references. This combined strategy to determine where threats are likely to occur and what business-critical infrastructure will be impacted can give the BC manager a nice springboard into the next phase of the BC lifecycle. Combining risk management efforts (piggy-backing with previous work done to support organizational decisions in the recent past) with a list of potential threats puts the BC manager on solid footing to start the cornerstone of BC planning, called Business Impact Analysis (BIA).
Business Impact Analysis

The fundamental task of Business Impact Analysis (BIA) is to identify which business processes are vital to ongoing operations and understanding the impact a disruption on these processes would have on the broader mission of the organization. “The BIA purpose is to correlate specific system components with the critical services that they provide, and based on that information, to characterize the consequences of a disruption to the system components.”

According to the Business Continuity Institute, a recognized leader in business continuity management and certification, there are four primary purposes of the business impact analysis. They are laid out in the Table 4.

<table>
<thead>
<tr>
<th>Table 4. The Primary Purposes of the BIA According to the BCI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obtain an understanding of the organization’s most critical objectives, the priority of each, and the timeframe for resumption of these following an unscheduled interruption.</td>
</tr>
<tr>
<td>Inform a management decision on Maximum Tolerable Outage (MTO) for each function.</td>
</tr>
<tr>
<td>Provide the resource information from which an appropriate recovery strategy can be determined/recommended.</td>
</tr>
<tr>
<td>Outline dependencies that exist both internally and externally to achieve critical objectives.</td>
</tr>
</tbody>
</table>

In the simplest of terms, BIA is a process of figuring out which processes are critical to the company’s ongoing success, and understanding the impact of a disruption on those processes. Various criteria are used including information technology, customer service,


operations, legal, regulatory, and financial. In business impact analysis, it is critical to identify interdependencies. Recovering one system or process may be useless if its dependent process or system is not on-line beforehand. Sequences, workflows, and protocols help determine what critical processes and systems may be. The BIA will help the BC manager hash out what the interdependencies are.

The two primary impacts on any business resulting from a disruption are generally operational and financial. The operational impact addresses the nonmonetary impact including how people, processes, and technology are impacted by a business disruption and how best to address that impact. The financial impact addresses the monetary impacts and how a business disruption will impact the company’s revenues.

In addition to the direct impact of a business disruption such as an earthquake or flood, there are also indirect impacts that must be considered during the BIA process. These indirect impacts can be better understood by identifying them as upstream and downstream losses. Upstream losses are those that are suffered if a key supplier is affected by disaster. Many companies rely on regular deliveries of products or services by another company or companies. This supply chain dependency must be investigated during the BIA so that the organization can understand how a geographically distant event may impact local operations. Downstream losses occur when key customers or the lives of people living in the local community are affected even if the facility is not impacted directly. When potential customers are more concerned with restructuring their own lives after being impacted, they are less likely to spend time or money on typical pursuits such as an outing of golf or a trip to the mall.
As the BC manager dives into the details of the company and its critical functions, he or she should develop a rating scale to determine the criticality of the functions within the organization. A rating system helps determine what functions or areas the BC plan should focus on initially and secondarily based on their importance. Mission-critical business processes and functions are those that have the greatest impact on company operations and potential for recovery. Almost everyone working within an organization has a vague concept of understanding when it comes to knowing what the mission-critical areas are within their department. The BC manager in charge of writing the BIA has the task of stepping back with his or her perspective and gathering the data to take a look at mission-critical operations throughout the organization. The most basic question that should be asked is, “What are the processes that must exist and continue to function reliably for the company to continue to stay in business?” It is important for individuals across the organization to contribute to the mission-critical functions. During the BIA it is the job of the BC manager to ask what the view of the organization is when it comes to defining “mission-critical.” The BC manager should ask what the first three to five actions employees would take in their specific department directly following a disruption. Asking for these actions can shed light on exactly what process or organizational element is the “mission-critical” element (Figure 2). Gathering these responses across the organization and observing where they overlap can identify “super mission-critical” areas that require the highest level of attention in the BC planning effort.

“Vital” business functions may fall somewhere between mission-critical and important, so it is important to account for these functions properly when gathering BIA responses. These functions are almost mission-critical, but not quite elevated to that response
Figure 2. Example rating system for functional criticality during BIA.

level. Examples would be systems like payroll, which are not critical to functioning as a business, but can have highly detrimental impacts in terms of employee morale and even legal ramifications.

It is essential that vital functions are addressed and restored shortly after the function of mission-critical elements. “Important” business functions and processes won’t stop the business from operating in the near term but they usually have a longer-term impact if they are missing or disabled. When missing, important functions can cause some disruption. A great example of an important system that is not mission-critical (depending on how it is used, of course) is the email system. “Minor” business processes are often those that have been developed over time to deal with small, recurring issues or functions. They will not be missed in the near-term and certainly not while business operations are being recovered. They will need to be recovered over the long-term. Some minor business processes may be lost after a significant disruption. In some cases, it is for the best. Many companies develop numerous redundant processes that should at some point be reviewed, revised, and often discarded. However, this lifecycle rarely occurs during normal business operations due to more demanding work. In some sense, a business disruption can be good for those small business functions and processes as they may be revised or optimized by necessity. Once the BIA has been completed and waypoint or status updates are being presented to upper
management, it may be of value to provide feedback on these redundant minor processes to resell the value of the intensive BIA process to the key stakeholders.

Some business processes are cyclical in nature and during most of the year they may seem minor while during other times, they are high priority for the organization or even “mission-critical” status. Each department should be asked if they perform any such process for incorporation into the BIA. Gaining temporal alignment with critical processes in the BIA allows for a more relevant and useful BC plan later on. It is important to follow-up on BIA assumptions throughout the year to make sure any cyclical processes are accounted for properly.

With criticality in mind, the BCM usually incorporates temporal objectives based off feedback from various stakeholders across the organization. In the realm of business continuity, there are various terms used to describe time-related objectives. These terms are typically used in the information technology realm, and the BC manager can choose to use some or all of them based off what the scope of the project. It may be necessary to loosely define time and point objectives based off ranking alone (e.g., charge the warehouse forklifts before restoring the picking system). Time objectives should also encompass interdependencies as described earlier. Definitions of temporal waypoints used in the BIA activities can be found in Appendix B of this document.

Now that various items that comprise the BIA have been defined, it is possible to elucidate what the entire BIA process looks like. The BIA needs inputs data to make the various output assessments incorporated into the BC plan later on (Figure 3).

Critical business functions, processes, and IT systems all need to be defined. Business functions are defined as activities like sales, marketing, research, or manufacturing. Business processes are how the activities occur. For example, sales can be conducted through a website or research is conducted in a laboratory with specialized personnel and instruments documenting their findings in laboratory notebooks that are audited by a quality assurance unit. The third category mentioned in Figure 3 is IT systems. In most companies, business processes are carried out in part through computerized systems, applications, and other automated systems. Identifying mission-critical business functions and processes and how they interact with IT systems can be a great way to map out business continuity and recovery strategies. Once the data from business functions, processes, and systems have been
collected, an analysis should be performed to generate outputs including the criticality assessment, the impact assessments (both financial and operational), required recovery objectives, dependencies, and work-around procedures. The work-around procedures will enable critical business functions to be restored as quickly as possible. Work-around procedures can be used during the RTO and WRT periods (Appendix B). The final output is a correlated into the finalized corporate business continuity plan.

Understanding a business comes down to communicating with those who know their function and their process to accomplish the overall mission. Collecting data for the BIA requires talking to subject matter experts throughout the organization (usually department heads or designee). BC professionals recommend collecting BIA data through questionnaires, interviews, or workshops. Additional data can be gathered using documents and research, but this data should be gathered only to support or supplement data gathered through direct contact with business subject matter experts. Only those who actually perform various business functions can assess the criticality of those business functions. It is important to involve the right people from across the organization in the BIA process. One of the best places to start is the organizational chart for the company. Some companies may not have a formal organizational chart, but they probably do have a phone directory or a similar document that can give the BC manager a place to begin his or her BIA data gathering. It may be useful to incorporate more than one functional subject matter expert (SME) in this meeting (e.g., include the BIA responder from legal and regulatory) so they can bounce their responses off one-another for increased clarity and accuracy in the bigger context of both

related departments. It may also be useful to include employees who are not managers, but are on the management track so they can come to understand the moving parts of the business from a broader perspective.

Questionnaires can often be used to gather data from SMEs in a fairly efficient manner. Though it takes time to develop a highly useful questionnaire, SMEs’ responses will be consistent, focused, and concise. They can fill out the questionnaires regarding their business units, business functions, and business processes at a time that is convenient for them (within a specified timeframe), thereby increasing the likelihood of participation. On the downside, questionnaires that are sent out may be ignored or forgotten. The questionnaire should be clear, concise, easy to understand, and fast to fill out. Web-based questionnaires are a great option because it is tougher for the responder to physically lose them and it is quicker for the BC manager to collect and correlate the data. It is also important to explain the purpose of the questionnaire to the participants in a manner that helps them buy into the process. It is important to include a statement that gains their trust in the BC project and that it exists to benefit them. It is useful to put contact information on the survey so respondents can resolve confusing questions in a timely manner with the BC manager. The BC manager should also sponsor a kickoff meeting that goes through the survey and gets the SME group buzzing about the survey to come. Once the results are in, it is appropriate to share the results of the questionnaire with the respondents. If they are willing to take the time needed to provide this data, there should be some reciprocity. For example, if the data is all pumped into a database, a report on each respondent’s data could be provided back to them for verification. Once the BC manager reviews the data, there may be additional questions.
Respondents should be told, in advance, about the process for following up with them regarding their responses to the questionnaire.

Interviews are another means to gather data for the BIA. A questionnaire-type document will still need to be created to provide the interviewers (designated by the BC manager) with a set of questions with which to gather responses. Free form or informal interviews will yield inconsistent data across the organization and will often create meaningless data. Each interview should follow a predefined format and the questions asked of each respondent should be the same. A questionnaire, interview, or question sheet from which the interviewer will work should be created. A corresponding data sheet should be created so the interviewer can record responses. Once an interview is conducted, the data needs to be reviewed and verified by the interviewee. Due to the nature of an interview, it is possible one of the people (interviewer, interviewee) may misunderstand the questions or responses. Therefore, once the data are prepared, the interviewee should review it before being finalized. Follow-up interviews, if needed for clarification, should be scheduled as quickly after the initial interview as possible so that the data, response, and topic are still fresh in the interviewee’s mind.

Data collection workshops can be an effective method of gathering BIA data. If you choose this method of gathering data, you might still choose to create a questionnaire so that you can be sure you cover all the required data points. An appropriate time and place for the workshop should be chosen for the workshop, ensuring the appropriate amenities will be available (white boards, refreshments, etc.). A clear agenda for the meeting must be laid out and distributed, in advance, to meeting participants. The workshop completion criteria must be defined so the facilitator and participants are clear about what is expected, what the
required outcomes are, and how the workshop will conclude. The facilitator’s job is to ensure the workshop objectives are met, so these objectives must be clearly articulated prior to the start of the workshop. Some companies use the concept of a “parking lot,” where issues are written up on note cards and collected or written on sticky notes and posted on a white board or an empty wall. An issue-tracking methodology should be used that allows you to stay on topic but make note of issues. Also identify the method you will use for addressing those issues that cannot be (or should not be) resolved during the course of the workshop. Finally, the BC manager and facilitator (may be the same person) of the workshop are to ensure that findings are written and well documented and that participants have the opportunity to review the results for errors and omissions before they are finalized. It may be useful to video or have a few designated people taking minutes to ensure nothing is missed.

After determining the business functions and gathering the data from the SMEs throughout the organization about their processes, it is possible to draw out the “impact” in the Business Impact Analysis. Impacts of disruption take many forms (Table 5), and often are interrelated to one another.

The biggest pitfall at this stage of the BIA process is the BC manager becoming overwhelmed with the data he or she has collected. The process can and usually does generate huge volumes of data that need to be collated and analyzed. To avoid full overload the BC manager needs to step back and take a broad look to narrow down the critical functions and processes of the company from the field of background “noise.” These functions will begin to stand out especially when the BC manager uses the mindset of scenario planning. Influenza is one scenario that should always be in the back of the BC manager’s mind because of the flexibility in operational capability it requires to survive.
Table 5. Organizational Impacts of Disruption

<table>
<thead>
<tr>
<th>Type of Impact</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial</td>
<td>Loss of revenues, higher costs, potential legal liabilities with financial penalty.</td>
</tr>
<tr>
<td>Supply Chain</td>
<td>Customers and suppliers may be lost due to upstream or downstream disruption (or both).</td>
</tr>
<tr>
<td>Employees and Staff</td>
<td>Loss of employees due to death, injury, stress, decision to leave in the aftermath.</td>
</tr>
<tr>
<td>Public Relations and Credibility</td>
<td>Any failure that causes the company brand to appear in a negative light such as identify and theft stemming from security failures, data loss, or embarrassing information about a company leader.¹</td>
</tr>
<tr>
<td>Legal and Regulatory</td>
<td>Regulations regarding worker health and safety, information security, and sector-specific regulatory obligations regarding quality, reporting, or customer complaints.</td>
</tr>
<tr>
<td>Operational</td>
<td>Operations are impacted by any business disruption, but it is important to rate operational impacts in terms of criticality.</td>
</tr>
<tr>
<td>Human Resources</td>
<td>How staff will be impacted by all manner of business disruption in a quantitative and emotional way.</td>
</tr>
</tbody>
</table>

¹From Cunningham et al., *Best Damn IT Security Management Book Period.*

Once the BC manager has analyzed the data, it should be synthesized in a report. This report should take the format that company management and executives are familiar with so they can comprehend the findings in the best way possible. The BC manager usually schedules a draft review meeting with stakeholders before presenting the formal report. This draft review is useful because it resolves conflicts with regard to time ratings (Appendix B) since there is a direct correlation between these ratings and the cost of mitigating the risks. Most managers want the function they are in charge of running in the shortest window possible, without realizing other factors in the business. With the BIA completed for each business function
and process, the BC manager has provided management with comprehensive insight into what happens after a disruptive event. More work is required after the BIA has been performed because the BIA is not specific to one disruptive event, nor does it mitigate the impacts of a disruption.

**Mitigation Strategy Development**

Now that the BIA is completed and the management is aware of where their vulnerabilities lie, it is time to form a strategy to mitigate the risks. In simple terms the mitigation strategy determines what money will be spent on to reduce the risk of disruption. Since mitigation involves spending money, the BC manager should regroup with management at this stage and show them what their financial options are. Cost-benefit analysis of various levels of mitigation versus potential loss due to inaction should be presented.

First, the impact analysis carried out by each SME for the impact areas shown in Table 5 should be applied to the top three threats on each list of the threat assessment. Then a mitigation strategy should be defined for each impact area. For example, if the top threat defined on the threat likelihood list is data loss, then the IT department should look into backup solutions and should price how much each solution option would cost. Another example would be if the top threat defined on the threat impact list is earthquake, then the facilities department should look into tie-downs and warehouse shelving solutions that could mitigate the risk of inventory damage or employee injury.

Mitigation strategy is a proposal to management with cost options. It is useful to give three levels of mitigation cost for each threat so as managers can tailor their response with a
balance of expenditure and risk (a scenario most executives drool over). The outcome is an allotted budget that the BC manager is in charge of for actually implementing the mitigation strategy along with the SMEs and ground-level managers. Obviously the mitigation strategy will not erase the risk of a threat turning into a disruption, but the mitigation activities will prevent a small disruption from turning into a larger one. All threats cannot be mitigated. There is no way for executives or the BC manager to know all possible outcomes. One example of an unforeseen threat turning into a costly, multimillion-dollar disaster is the recent eruption of the Eyjafjallajokull volcano and its resulting ash plume. Since disaster is inevitable despite the best-laid mitigation strategies, the BC manager should bring together his or her knowledge gained thus far through the BC process (initiation, threat/risk assessments, BIA, and mitigation) to form a plan of action for the time when the disaster actually occurs.

**BUSINESS CONTINUITY PLAN DEVELOPMENT**

The business continuity plan document takes all the previous steps of the BC process and synthesizes them into a ready-to-use document that can be pulled from the shelf during a crisis scenario so that rational and logical decisions can be made in a timely manner to get the company into the recovery mode as soon as possible. The BC plan itself should not define how recovery will be accomplished, but should make it possible to get to the stage where recovery can happen. Business continuity plans vary from company to company depending on the BIA outputs and unique organizational structure in many industries, but all BC plans

---

should have a few critical elements. Like the BIA, the BC plan must be created with cooperation of subject matter experts throughout the organization. Each element of the BC plan should be a clear bulleted list of clearly worded sentences that leave no room for ambiguity. Each element should also list the responsible party by name and title so the task can be performed if the named person has been replaced due to unavailability.

The first element of the business continuity plan should be a detailed organizational chart with names, locations, contact information, and titles. This human terrain map is often critical to successful continuity of operations when faced by disaster or disruption. This chart will be of high utility in almost any continuity plan activation because it defines the most critical element of the business—the people. Having detailed contact information for each employee in the business allows for all other elements of the continuity plan to play out. During a crisis, even simple activities like remembering a phone number or the name of the IT specialist at a far-flung backup facility can be daunting. The organizational chart should also have a secondary contact list of external contacts like first responders, critical suppliers, and crucial customers so that communication data is up-front and accessible for defined waypoints later in the plan.

The second crucial element within a useful business continuity plan is a section that deals with communication. The organizational chart defines who is who and where he or she is located, but it does not tell people how to talk to one another. Strategies for communication should overlap and leverage all available communication resources including email, telephone, mobile devices, and even more archaic practices like note passing with messengers. One of the most critical areas within the BC plan is to determine how executives will communicate important decisions like closing the facility, telling employees to stay
home, or addressing the media regarding a sensitive incident. The BC plan should lay out step-by-step planning for how communication will occur and present alternatives if one or more means of communication is not available.

The third element all business continuity plans must have is emergency accounting procedures. Business survival depends on knowing where the money is and leveraging that money to accomplish the mission. Emergency payroll procedures should be laid out carefully keeping in mind that the facility may not be accessible. Employees that know if they are getting paid will respond more resiliently to disaster and will do their best to get the business into recovery mode. Expedited financial decision-making workflows should also be laid out so that what used to take a chain of people to accomplish can be achieved with one or two.

The fourth element critical to a BC plan is crisis monitoring. Monitoring may take drastically different forms depending on if the crisis is internally driven or externally driven. An external example would be if the business were located in the fallout zone of terrorist dirty bomb detonation where the government conduits of information, media outlets, and first responder frequencies should be monitored to determine the appropriate response. An internal example would be an active shooter within the headquarters office where security personnel would monitor the position of the shooter within the building to pass along evacuation or shelter-in-place orders to employees and first responders.

The fifth crucial element of a robust business continuity plan is alternate site contingencies. If the primary facility becomes unavailable, it is important to lay out the plan for transitioning to an alternate, working from home, or leveraging other company-owned sites to take on the tasks critical to the inaccessible site. Here it may be necessary to include
blueprints, capabilities, maps of the area, and personnel located at potential alternate sites to
determine their feasibility based off situational awareness.

The business continuity plan is in essence an aid to building resiliency in the face of
crisis. The plan itself may not be perfect when faced with a horrible crisis like the death of
many employees, but it will provide the survivors with a path forward that has been thought
out before the fog of the crisis has set in. The plan should also be scalable and have action
points dependent on what monitoring dictates. If the plan has successfully combined the BIA
findings and situational awareness to give decision makers a way forward during a crisis,
then the BC plan is successful. No plan is going to be successful if nobody knows how to use
it and for the plan to be effective, it must be updated on a routine basis to keep up with the
changes in the business.

**BC Plan Exercising and Training**

After all the necessary activities associated with a developing business continuity plan
have been completed, the work of the BC manager is not over. He must acclimatize the
organization’s employees and management to use the BC plan effectively. Effective
exercising trains the managers and stakeholders throughout the organization to become
comfortable with the plan and gives them the confidence to use it in a time of stress and
disruption. Three fundamental exercise types can be defined: the plan review, tabletop
exercise, and simulation exercise (Figure 4).

In a plan review exercise, the business continuity plan owner and business continuity
team discuss the business continuity plan. They look for missing elements and
inconsistencies within the plan or with the organization. This type of exercise is comparable
to plan auditing, and is useful to train new members of a team, including the business function owners and their manager. In a tabletop exercise, participants gather in a room to execute documented plan activities in a stress-free environment. Tabletop exercises can effectively demonstrate whether team members know their duties in an emergency and if they need training. Documentation errors, missing information and inconsistencies across business continuity plans can be identified in a tabletop exercise.

To determine if business continuity management procedures and resources work in a realistic situation, a simulation exercise is desirable. This exercise uses established business continuity resources, such as the recovery site, backup equipment, services from recovery vendors, and transportation. It can require sending teams to alternate sites to restart technology as well as business functions. Errors, omissions, missing or insufficient resources, incomplete coverage, and limited vendor capabilities may surface in this exercise. Simulations may also uncover staff issues regarding the nature and the size of their tasks. The use of a scenario is highly recommended for simulations. One way to add realism is for the BC manager to sit all individuals involved in a room and give 10 to 20 of the people (2 to
4 individuals in a room of 20) red cards. These red cards signify that the person is dead in the exercise. Taking out key knowledge adds a true layer of realism that reflects how a disaster will progress when the real thing happens.

A cooperative simulation exercise includes the elements of a simulation exercise but also integrates outside partners such as first responders, volunteers, and business partners in the supply chain. This type of exercise also includes a scenario and stretches over a significant period of time. The cost of this type of scenario may be prohibitively high, but the benefits are truly noteworthy. Ideally all elements of business continuity plans should be exercised at least once a year. Each exercise may have different objectives, beside the primary one. Main exercise objectives include identifying weaknesses and shortcomings, verifying communication objectives and procedures, validating efficiency of plans, verifying the adequacy of alternate sites, and achieving specific recovery time objectives (RTOs) and recovery point objectives (RPOs).

Exercises may be highly useful, but they are generally resource-intensive, so it is important to find balance when budgeting for exercises. Exercises often present human resource issues. A good exercise spans into off-work hours but people could refuse to work overnight, weekends, or be away from home even a few days. HR managers should help resolve these issues and recruit individuals within the organization passionate about being a part of the exercise.

The primary reason to exercise is to identify limitations of business continuity plans. Recognizing that most organizations change frequently, even mature business continuity

plans may be inappropriate in a given situation or at a given time. Exercises that appear to be “successful” and uncover no problem should be suspect. Maybe the objectives were too easy or the situation was unrealistic. Exercises present opportunities to fix problems before a disaster happens. Ideally, a successful exercise uncovers and documents problems, so it is crucial to have breakout sessions and note takers to document issues. Once the problems have been fixed, the BC manager should consider running a follow-up exercise to ensure the repairs work. Measuring the success of business continuity exercises means having relevant objectives that will help uncover problems. Exercising is where the rubber of business continuity meets the road. It makes planning for a disruption realistic and hones the response to a real disaster scenario.

One danger of having a plan in place for business continuity is that the plan and exercising can become routine and stale. With the daily challenges of running a business, it is easy to relax and fall into a habitual pattern of security and safety procedures. After a few months, employees will become complacent and take the BC plan for granted without understanding how to utilize it effectively. Testing the plan frequently by throwing in realistic and novel scenarios keeps things fresh and puts employees on their toes so they can respond effectively.

**BC/DR Plan Maintenance**

Keeping the BC plan up to date with the changing business is critical to ensuring the plan is effective when activated. An out-of-date plan can be worse than having no plan at all because it allows staff across the organization to make assumptions about business continuity readiness that are plainly wrong. Changes in the HR database, organizational chart, and
contact information should be integrated into the business continuity play. Additionally, significant changes to the business model—such as a key supplier changes, new system implementation, or strategic restructuring—should also be quickly integrated into the business continuity plan.
CHAPTER 3

DEFINING THE THREAT: INTELLIGENCE ON INFLUENZA AND H1N1

Influenza may be common and familiar in our national consciousness since its occurrence waxes and wanes throughout the year, but it should not be taken lightly. Influenza is a serious disease. When a pandemic of influenza occurs much of the nation is stuck on the couch or in bed with uncomfortable symptoms. National economies are temporarily affected across many sectors such as transportation and supply chains, as well as disruptions like classrooms being empty with parents needing to care for children instead of being at work. Due to the high rates of infection the social, political, and economic repercussions of epidemic disease can be wide-ranging and significant. To understand the threat, one must understand what composes the influenza virus.

THE SCIENCE OF INFLUENZA

Influenza is a virus. Viruses are not cells in the classic biological sense, but they are “infectious particles consisting of nucleic acid enclosed in a protein coat, in some cases, a membranous envelope.” The tiniest viruses are only 20 nanometers across, smaller than the ribosome in a mammalian cell. An electron microscope is required to see even the largest

34. Centers for Disease Control and Prevention, “Podcasts at CDC.”

viral particles. Viruses use the cellular machinery of the organism they infect to reproduce. Viruses attach to a host cell, its viral nucleic acid genetic code enters the host cell, viral proteins are synthesized to the specifications of the viral nucleic acid sequence using the host cell machinery, the virus’s DNA or RNA replicates, the new viral particles assemble, and the new viral particles are finally released to carry on the cycle with surrounding host cells.³⁶

Viral influenza is usually limited to viral involvement of the cells of the upper respiratory tract, the mucous membranes of the nasopharynx (nose and throat), the conjunctiva, and less often, the lower intestine.³⁷ All it takes is a badly timed sneeze by an influenza viral host for the viral particles to become airborne. If influenza viruses do enter the respiratory system, they invade the superficial susceptible cells of the respiratory membranes. It is within the superficial susceptible cells that the viruses reproduce, a process that takes about six hours. To reproduce, the virus binds to and then enters a living cell, where it commandeers the cellular machinery, inducing it to manufacture new copies of the viral components. The pieces then assemble themselves into new viruses that escape the host cell, proceeding to infect other cells within the respiratory tract. Recent research shows that influenza A (the family to which H1N1 belongs) is largely confined to the respiratory tract with occasional involvement of the intestinal tract and sometimes the brain.³⁸ The clinical symptoms are generally explained by the effect of the immune response to viral infection.

³⁶ Allan Tobin, Asking about Cells (Fort Worth: Saunders College Publications, 1997).


³⁸ Hans-Dieter Klenk, Avian Influenza (Basel: Karger, 2008).
Sometimes a strong immune response prevents the influenza virus from entering the superficial cells of the nose and throat. Even if some viral particles enter the superficial cells, the process of viral replication may not occur. Without reproduction, a generalized infection does not occur. Even in this case of minimal exposure, the human immune system can ramp up antibodies to the antigenic proteins on the influenza virus.

The influenza virus is composed of numerous antigenic proteins, not just one. Each antigen varies in importance in determining the likelihood of whether or not the victim will develop a clinical case of influenza. Influenza is a spherical virus particle. Viral particles are commonly called “virions.” A virion is structurally intact and infectious. A complete influenza virion is made up of 75 percent protein, 1 percent RNA, 6.5 percent carbohydrate, and 18 percent lipid. Within the core of the virion, also called the nucleocapsid, resides the RNA. The RNA is the genetic material of the virus. Related to the viral RNA is the major nucleoprotein (NP) antigen, the antigen used for classifying influenza viruses into Types A, B, and C. Surrounding the nucleocapsid of the virus are double layers, an inner protein and an outer lipid membrane. On the outer membrane are two types of spike-like projections, glycoproteins called hemagglutinin (H or HA) and neuraminidase (N or NA). These glycoproteins, which are morphologically and antigenically different substances, are also major antigens. Their discovery made the classification of influenza into types A, B, and C inadequate, and are now used as signature proteins to identify signature strains of the virus. There are at least fifteen known variations of the HA protein, and nine of the NA protein. Since the identification of HA and NA antigens, it has become evident that there are still other significant proteins within the influenza virion. Understanding these proteins is

necessary to see how the virus enters the human system and exploits the human body’s own cells to replicate itself.

The influenza RNA genome has eight genes, each of which gives rise to one or more proteins. The protein products of each gene have a role to play in the influenza virus’s nefarious activities. For infection to occur, the HA protein binds to receptors called sialic acid on membrane of the host cell. The specific receptors differ among species, which determines the type of host the virus is able to infect (be it human, bovine, equine, or avian). For the HA protein to become activated within the host cell, it must be cleaved into two pieces. To achieve this cleave, the virus ingeniously uses the pre-existing enzymes of the host cell. Any small change in the HA protein sequence (caused by mutation of the source RNA genetic code) can allow the virus to infect a new host or even a completely new species. Even a small change in the protein sequence can cause drastic structural changes for the virion. The neuraminidase (NA) protein enables new virions produced within the host cell to escape thus setting the virions free to infect other cells using their other component protein (HA) discussed previously. NA is an enzyme and a protein, so it can cleave receptors on the new target cells. NA has become a target for antiviral drugs because inhibiting its enzymatic action can prevent the release of virions that cause widespread infection of the host’s respiratory tract. Oseltamivir, commonly referred to as Tamiflu™, is one such therapeutic.

Viral proteins are highly immunogenic, meaning that the human immune system vigorously produces antibodies specific to the viral proteins on the surface of the influenza virus. Antibodies specific to the HA molecule on influenza confers protection against influenza, but its specificity is strain-specific and is readily bypassed by any antigenic drift in

the virus. Antigenic drift, to be discussed in more detail below, in the HA molecule results in amino acid substitutions in several antigenic domains at the exposed portion of the molecule on the virus’s surface. Human antibodies produced against the HA molecule on influenza are important in blocking initial viral infectivity because they bind to the active area of HA. The antibody titers peak within a few days of infection and then decrease slowly over the next six months. The titers then plateau and remain stable over the next several years. This antibody plays a significant role in resistance to reinfection by the same strain. Interestingly, influenza has evolved to suppress the immune response of its host using non-structural proteins (NS1 and NS2). These proteins target the interferon system of the mammalian immune system thus lessening the initial response that would typically occur to a viral antigen. Having the ability to suppress or block this response gives the virus crucial time after initial infection to establish itself and reproduce many thousands of times without interference from the host immune system.

Influenza virus is characterized by the frequency with its genetic material changes. These changes can be minor (referred to as drift) or they can be major (referred to as shift). Antigenic shift in one or more viral surface antigens is known to be a trigger for an influenza viral strain to infect a new species or many individuals on a pandemic scale. Polymerase enzymes are used to reproduce the genetic code of the virus during viral replication. Some types of polymerase, have proofreading activity, which actually corrects errors that have occurred when genetic material is being replicated or copied thus preventing change from occurring. Such proofreading activity is vital for survival of a complex organism like a mammal. However, influenza RNA polymerase molecules lack proofreading activity, contributing to the ease with which the influenza virus acquires genetic changes. Genetic
shift is an advantage for the virus because it helps it evade the immune system of a host that may already possess antibodies to an earlier iteration of the virus that produced different antigens with shifted genetic material. It has been noted that the three polymerase genes are often co-transmitted with the HA gene, and in the case of the 1918 pandemic strain, were likely to have contributed to the rapidity with which the virus was able to reproduce itself once inside the body. 41

**A BRIEF HISTORY OF RECENT INFLUENZA PANDEMICS**

Three worldwide pandemic outbreaks of influenza occurred in the twentieth century. The major influenza epidemics of 1918, 1957, and 1968 showed no predictable periodicity or pattern. 42 The 1957 and 1968 pandemics were in the era of modern virology and most thoroughly characterized. Their presumed sites of origin as Spanish, Asian, and Hong Kong influenza have informally identified all three pandemics, respectively. The three major pandemics are now known to represent three different antigenic subtypes of influenza A virus as demonstrated in Table 6. The 1918 pandemic is widely regarded as the most deadly natural disaster of all time and it has been well documented that it impacted not just the extremely young or extremely old, but also impacted otherwise healthy 15- to 34-year-old young adults. 43 The pandemics of 1957 and 1968 were unusually deadly and spread globally.

41. Taubenberger and Morens, “1918 Influenza.”


Table 6. Major Pandemic Influenza Outbreaks of the Twentieth Century

<table>
<thead>
<tr>
<th>Outbreak</th>
<th>Year</th>
<th>Antigenic Subtype</th>
<th>Deaths</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spanish Influenza</td>
<td>1918</td>
<td>H1N1</td>
<td>~50-100 million</td>
</tr>
<tr>
<td>Asian Influenza</td>
<td>1957</td>
<td>H2N2</td>
<td>~2 million</td>
</tr>
<tr>
<td>Hong Kong Influenza</td>
<td>1968</td>
<td>H3N2</td>
<td>~1 million</td>
</tr>
</tbody>
</table>

Interestingly, a few pseudopandemics also occurred in the twentieth century, all of the subtype H1N1. Each of these pandemics has been described as “mild” by the scientific literature. However, it is also worth noting that the severity and unpleasantness of the resulting sickness in 1968 was notable. In some ways this reflects the H1N1 experience of 2009, where the symptoms were highly unpleasant but caused few deaths in comparison with previous pandemics.

**THE H1N1 OUTBREAK OF 2009**

In April 2009, a government worker in Oaxaca, Mexico, became the first victim of H1N1. At the bedsides of other men and women struggling to stay alive in Mexican critical care units, health care professionals noticed a novel H1N1 flu virus was deviating from influenza’s usual pattern of action. H1N1 2009 began in the Northern Hemisphere, not in Asia as has been typical of novel influenza variants over the past fifty years. H1N1 also made its first appearance in mid-spring, not late fall or winter like usual. H1N1 also had a worrying


45. Kilbourne and Loge, “Influenza A.”

tendency to infect children and young adults, not the elderly and newborn population as is customary for seasonal strains of influenza.

In the months after those first deaths in Mexico, the virus ignited a global pandemic and a public hysteria of media coverage and political response. While the epidemic never became as deadly as many initially feared, it was not as mild as some experts now believe. Additionally, it exposed some grave shortcomings in the world’s public health response. Those who now describe the pandemic as mild base their conclusion primarily on what, at first, seems like a mortality rate in the United States similar to those seen after seasonal influenza. However it is important to point out that data is unreliable outside the U.S. for exact death rates attributable to H1N1. In the United States, the vaccine arrived later than estimated, and only about 80 million Americans received it. In developing nations, far fewer individuals were vaccinated. In fact, only twenty-six of ninety-four poor countries in need of the vaccine had received it as of Spring 2010.\(^\text{47}\)

H1N1 was also particularly dangerous for young adults, along with pregnant women, obese patients, and minorities. The H1N1 virus was quite difficult for clinicians to identify. Whereas doctors associate fever and cough with outbreaks of influenza, one-third of patients admitted to hospitals and up to half of infected outpatients in this pandemic had no fever, yet they were infectious. If this characteristic of H1N1 were to recombine into a novel, more deadly form of influenza such as H5N1, the prospects would be bleak.

It is likely that H1N1 went under-diagnosed and that the number of infected was actually much larger than has been publicized. A British study shows that “one child in every

three was infected with 2009 pandemic H1N1 in the first wave of infection in regions with a high incidence, ten times more than estimated from clinical surveillance. H1N1 2009 posed huge infection-control problems, especially in hospitals. This was because it was found not only on hard surfaces in the environment, which is common to all influenza strains, but in the stool of patients, a feature of avian influenza.

Public health groups emphasized the necessity of frequent hand washing, which surely helped reduce transmission. But those groups also disagreed on other preventatives: for instance, the World Health Organization and Society for Health Care Epidemiologists of America recommended the relatively inexpensive surgical mask, whereas the Centers for Disease Control and Prevention argued for the –95 respirator mask.

Offhandedly, H1N1 came to the United States at a time when Americans seemed particularly incredulous about government and large institutions. The CDC faced an uphill battle to characterize the trajectory of the pandemic, to define its impact, to offer suggestions and to convince a wary public to get vaccinated.

At times, health officials erred in their recommendations. CDC authorities often said that ill children and adults could go back to school or work twenty-four hours after their fever disappeared—even though young children are contagious for up to three weeks and adults for _______________________


five to seven days. H1N1 should be considered a “near miss” as pandemics go. Public health authorities should learn from their shortcomings and work hard to produce clear communications to the public without making the public jaded with pandemic overload.

**GENERAL PUBLIC HEALTH IMPLICATIONS OF INFLUENZA**

According to the CDC, 36,000 Americans die annually as a result of the seasonal flu. In fact, the number of deaths attributed to the flu has risen four-fold between the late 1970s and the late 1990s. Seasonal influenza is still a significant public health threat causing considerable deaths among the young, sickly, and elderly. However, if a new antigenic subtype emerges in a population not protected by immunity influenza can cause a major public health crisis on the same order of magnitude as the famous 1918 pandemic. Pandemics typically occur over many months and can peak one or more times (Figure 5).

The peak pandemic activity of a novel strain will most likely overwhelm the current health care system in a significant way. This is especially true since “Influenza A is unique among the major pandemic threats in that it could potentially infect 30% of the world’s population within a matter of months. Even at a conservative overall mortality rate of 2%, it would result in around 135 million deaths worldwide within the first year of a new pandemic outbreak.” Such an occurrence would have unspeakable public health implications and could detrimentally impact the global community.

---


During the 2000-2001 flu season, federal officials were caught unprepared when one of the four vaccine manufacturers had to cease production as a result of FDA concerns over plant conditions. Shortages, delays, and 200 percent price gouging ensued. The situation was investigated by the General Accounting Office, which reported in May 2001 to the Department of Health and Human Services that “the circumstances that led to the delay and early shortage of flu vaccine during the 2000-01 flu season could repeat themselves in the future . . . . Now, a production delay or shortfall experienced by even one of the three remaining manufacturers can significantly impact overall vaccine availability.”

Figure 5. Pandemic incidence over time with key waypoints. Source: Adapted from Allely, Eric. “National Security Implications for a High Impact Pandemic Influenza on U.S. Critical Infrastructure.” Paper presented at the Pandemic Influenza Conference, San Diego State University, San Diego, California, Summer 2009.

Three years after this shortage and many warnings from public-health experts in between about the dangers of continued consolidation among pharmaceutical companies, the United States experienced another shortage. Chiron, one of the two companies relied on to manufacture the flu vaccine for the 2004-2005 season, had its sole vaccine plant in the United Kingdom shut down by the UK health authorities on October 5, 2004, due to contamination. As a result, half of the 100 million doses of vaccines the United States needed were not available. Rationing, long lines, panic, and price gouging followed. And again, there was no easy and quick solution since the other manufacturer was already at 100 percent capacity and no manufacturer around the world had extra capability.

Relying on a small number of suppliers, with no extra capacity to cover for one another, meant that the United States government had put itself and the health of its citizens into a single-sourcing situation. Despite this risky situation, the US did not carefully monitor their supply. In June 2003, a year before the 2005-2005 crisis took place, US officials learned that Chiron had reprocessed contaminated batches of flu vaccine, but the problem was not investigated vigorously. As late as September 28, 2004, one week before his plant was shut down, Chiron CEO Howard Pien assured a US Senate committee that his company would deliver 48 million doses of the vaccine for the upcoming flu season. Worryingly, Congress took his word at face value. The vaccine shortages and viral culture issues faced during the recent H1N1 pandemic demonstrate that the vaccine supply chain has not shown


improvement over the previous decade. This is an ominous omen for the next major pandemic.
CHAPTER 4

REVISING BUSINESS CONTINUITY EFFORTS

TO FACE THE PANDEMIC THREAT

Now that the influenza threat has been defined, it becomes evident that current business continuity practices fall short when it comes to pandemic preparedness and pandemic-driven disruption. It is important for businesses to take the pandemic threat seriously and consider actions beyond the typical business continuity planning cycle described earlier in this thesis. The BC updates and action items about to be presented can provide business resiliency outside of the pandemic threat, providing a template for “outlier” disasters that seem to come out of nowhere and have widespread geographic impacts.\(^{56}\)

**GAUGE GOVERNMENT RESPONSE**

It is important for the BC manager to plan for the government response and listen carefully for signs of how the government will respond to a future pandemic. One means of gauging government response is for the BC manager to build a close relationship with public health officials in the community and county where the business is located so that information is close at hand during a pandemic. Despite good intentions, government response is often drastic and even detrimental to the prospect of business continuity. Strong government reaction can exacerbate an already serious disruption scenario.

The risk-averse culture of politics and the legitimate need to instill public confidence breed a strong predilection toward being visibly “in control” during disruptions. Following the 9/11 terrorist attacks, the US government tightened security at US borders and shut down all flights in and around the United States. The intermittent plant closing by Chrysler Corporation in the weeks that followed and the 13 percent reduction of output at Ford Motor Company during the fourth quarter of 2001 were not the direct result of the terrorist attack, but they were the result of the shutdown of the Canadian and Mexican borders for truck movements and the resulting delay because of tighter border security. The US government reactions disrupted numerous just-in-time manufacturing systems that depended on reliable international shipping.

When the Kobe earthquake of 1995 injured over 30,000 people, many made their way to Kobe’s hospitals. Yet 85 percent of these hospitals suffered damage from the earthquake and sustained a combined loss of one billion dollars. Additionally, the lack of running water, gas, and electricity hampered medical care even at the healthcare facilities that were not directly damaged by the quake. Naturally the Japanese government rushed to aid injured people. In order to fill the massive healthcare gap, the government established free health clinics to cover the needs of the homeless and injured. Ironically, this massive aid effort proved too successful by staying operational for too long. The free clinics almost bankrupted most of the area’s private hospitals, which couldn’t compete with free care. Again, a well-intentioned strong government intervention caused unintended secondary damages.

It is impossible to tell how the government will respond, but if there is a chance for drastic action, the BC manager should integrate such an eventuality into his or her pandemic planning process. This includes the impact of closing schools, huge absentee percentages in the workforce, and lack of critical infrastructure usually taken for granted (water, power, sewer, trash, etc.). The BC manager should adapt the general business continuity plan to address this broad infrastructure deficiency threat and should gear the pandemic plan to dealing with the broad geographic and temporal footprint of a pandemic.

**COMPREHEND THE POTENTIAL HUMAN IMPACT**

The BC manager must take the broad based approach to understand the human impact of influenza within an organization. Some or all employees may be impacted by influenza during a pandemic. Some may be impacted more than others. During the BIA, it is crucial to personalize the process by identifying key positions, key knowledge, and key skills needed for business continuity. This personalization process crosses into what is traditionally called “succession planning.” In publicly traded companies or high-profile start ups, the company often purchases what is called “key man insurance.” This insurance covers the cost of losing a high-ranking executive in the company, the assumption being that if someone at that level were suddenly unavailable to carry out that function, the business would suffer financial losses. Succession planning in companies covers many areas, but typically it’s discussed in terms or replacing key employees as well as how to transfer the reigns of the company from one leader to the next. Succession planning can include training employees to move up the corporate ladder and assume leadership positions.
When looking at pandemic, the BC manager should use strategies from succession planning to address who will replace key employees in the tragic event of a death due to a pandemic-like influenza. Before the outbreak (or other disaster event), putting a plan in place to identify who should step up should something happen to the company’s founders or executives can help smooth the transition thus preventing battles for power or lack of leadership that could harm the company even more than the loss alone. Beyond looking at “higher-ups” within the organization, a BC/DR plan needs to analyze key positions throughout the company and understand the role of each in the business continuity realm. This planning comes down to strong human-centric BIA where managers identify personnel associated with critical processes and knowledge to the BC manager for incorporation into the plan. The key stakeholders or SMEs mentioned previously, should identify who they would like from their department to replace them in the event that they are not available to work because of the pandemic.

A good business continuity plan will address the human factors for two reasons. First, addressing employee needs is ethical business. Although there are companies that may demand employees to work following a serious disruption and threaten termination, most companies understand that everyone will have different needs. Some may report back to work, some may need to deal with sick family members, and some may be physically or emotionally unable to return to work immediately. The company’s policies with regard to employee needs and requirements in the aftermath of a disruption, and especially an influenza outbreak, should be developed with the HR department. The second reason for addressing employee needs in the BC/DR plan is because it makes good business sense. The ideal scenario might be that everyone turns out to be healthy and shows up to work, but if faced
with a choice between work and family, between work and health, most people will naturally choose health first. In some cases, insisting people return to work before they are ready can make things worse because they might not be able to concentrate and therefore may make recovery efforts worse instead of better. Incorporating this reality into the BC plan will mean that the BC management team will have to strike the perfect balance of alternatives that can address the lack of key staff during the pandemic while ensuring that they don’t force employees to come back to work too soon, worsening the spread of the pandemic. Strong planning can help the employees who may be unable to come back immediately and also helps the company recover in the fastest and most cost-efficient manner possible.

The human effects will cause various types of disruption to the business. A supply disruption will result from absenteeism and voluntary withdrawal from the workplace. A demand disruption will result from a sharp drop in consumer demand for products (with notable public health-related exceptions). During peak pandemic activity—in the face of daunting absenteeism and disruptions—actions can be taken to ensure the impacts on a business are as small as possible (Figure 6).

**UNDERSTAND THE PROS AND CONS OF THE “WORK AT HOME” SOLUTION**

Within the public and private sector, it is assumed that when a pandemic peaks business will go on with employees working at home. Public health officials will likely prevent public gatherings in some form. Many BC plans are predicated on enabling employees to work from home during a severe pandemic. Little analysis has been carried out to assess the impacts of a surge in home workers on corporate provision and Internet
infrastructure. What research that has been carried out suggests that Internet bandwidth supply may not meet demand during a severe pandemic. Work-at-home (WAH) strategies may be in jeopardy, as residential Internet bandwidth supply might not meet demand, according to Gartner, Inc.

According to the CDC, the rule of thumb for worst-case pandemic planning is that 40 percent of the workforce will not be in the workplace for an extended period of time. According to experts, existing bandwidth capacity held by the large telecommunications infrastructure. What research that has been carried out suggests that Internet bandwidth supply may not meet demand during a severe pandemic. Work-at-home (WAH) strategies may be in jeopardy, as residential Internet bandwidth supply might not meet demand, according to Gartner, Inc.

According to the CDC, the rule of thumb for worst-case pandemic planning is that 40 percent of the workforce will not be in the workplace for an extended period of time. According to experts, existing bandwidth capacity held by the large telecommunications infrastructure. What research that has been carried out suggests that Internet bandwidth supply may not meet demand during a severe pandemic. Work-at-home (WAH) strategies may be in jeopardy, as residential Internet bandwidth supply might not meet demand, according to Gartner, Inc.

According to the CDC, the rule of thumb for worst-case pandemic planning is that 40 percent of the workforce will not be in the workplace for an extended period of time. According to experts, existing bandwidth capacity held by the large telecommunications infrastructure. What research that has been carried out suggests that Internet bandwidth supply may not meet demand during a severe pandemic. Work-at-home (WAH) strategies may be in jeopardy, as residential Internet bandwidth supply might not meet demand, according to Gartner, Inc.

According to the CDC, the rule of thumb for worst-case pandemic planning is that 40 percent of the workforce will not be in the workplace for an extended period of time.

According to experts, existing bandwidth capacity held by the large telecommunications infrastructure. What research that has been carried out suggests that Internet bandwidth supply may not meet demand during a severe pandemic. Work-at-home (WAH) strategies may be in jeopardy, as residential Internet bandwidth supply might not meet demand, according to Gartner, Inc.

According to the CDC, the rule of thumb for worst-case pandemic planning is that 40 percent of the workforce will not be in the workplace for an extended period of time.

According to experts, existing bandwidth capacity held by the large telecommunications infrastructure. What research that has been carried out suggests that Internet bandwidth supply may not meet demand during a severe pandemic. Work-at-home (WAH) strategies may be in jeopardy, as residential Internet bandwidth supply might not meet demand, according to Gartner, Inc.

According to the CDC, the rule of thumb for worst-case pandemic planning is that 40 percent of the workforce will not be in the workplace for an extended period of time.

According to experts, existing bandwidth capacity held by the large telecommunications infrastructure. What research that has been carried out suggests that Internet bandwidth supply may not meet demand during a severe pandemic. Work-at-home (WAH) strategies may be in jeopardy, as residential Internet bandwidth supply might not meet demand, according to Gartner, Inc.

According to the CDC, the rule of thumb for worst-case pandemic planning is that 40 percent of the workforce will not be in the workplace for an extended period of time.

According to experts, existing bandwidth capacity held by the large telecommunications infrastructure. What research that has been carried out suggests that Internet bandwidth supply may not meet demand during a severe pandemic. Work-at-home (WAH) strategies may be in jeopardy, as residential Internet bandwidth supply might not meet demand, according to Gartner, Inc.

According to the CDC, the rule of thumb for worst-case pandemic planning is that 40 percent of the workforce will not be in the workplace for an extended period of time.

According to experts, existing bandwidth capacity held by the large telecommunications infrastructure. What research that has been carried out suggests that Internet bandwidth supply may not meet demand during a severe pandemic. Work-at-home (WAH) strategies may be in jeopardy, as residential Internet bandwidth supply might not meet demand, according to Gartner, Inc.

According to the CDC, the rule of thumb for worst-case pandemic planning is that 40 percent of the workforce will not be in the workplace for an extended period of time.
carriers on their Wide Area Networks (WANs) can handle the added 40 percent capacity. However, the limiting step is in the last mile of network leading from the WAN to the residential Internet access loop. The surge in demand during a large-scale WAH scenario will likely overload the local connection because carriers do not design for excess residential capacity. WAH Internet usage for commercial purposes usually takes place during the daytime, when online shopping and other home consumer traffic are at a lull. However, during a pandemic WAH event, consumer usage and WAH usage will overlap. If children are kept home from school (a population that increasingly drives bandwidth ratios today) they will exacerbate the problem if they continue using the Internet as they would on a normal weekday evening.

DSL users are vulnerable to oversubscription, a condition in which potentially dozens of users share a single digital subscriber access multiplexer (DSLAM) connection to the backbone. This reality constricts the response to a spike in last-mile demand during a sudden WAH event. It has been suggested by some commercial communications providers that the last-mile limitations and pressures during a WAH even on DSL and cable modem networks can be eased using 3G or other non-tethered access. They encourage commercial organizations to assess and integrate 3G as a backup/emergency solution to mitigate last-mile failures. However, this solution puts more strain on a presumably already strained wireless network.

Gartner, Inc. suggests possible alternatives to improve Internet bandwidth for WAH strategies.⁶⁰ These strategies should be implemented into a pandemic continuity plan.

⁶⁰. Ibid.
When employees are forced to work from home, they lose the benefits provided by their office WAN optimization controller (WOC). Some organizations are deploying software WOC client software on every laptop to help mitigate the bandwidth and latency issues. On a congested network, a SoftWOC can make the most of the little bandwidth available with 80-90% reductions for many applications. If it’s only necessary to accelerate browser-based applications, or if software cannot be installed on an employee’s home computer, a second solution is to use client applets that work with data-center-resident application delivery controllers or WOCs. A third solution is to bypass the wired last mile altogether and switch to a wireless connection, such as 3G or WiMAX, or satellite. In contrast to these wireless offerings, new or expanded wired broadband services can take weeks to deliver under normal circumstances.\(^{61}\)

However, while last-mile bypass may fix the access network problem, it cannot fix the common latency-induced problems that arise during stages of unplanned emergency access. In an emergency, it is a safe bet that wireless services will be oversubscribed. The takeaway is that businesses need to set up a variety of strategies for WAH including pandemic and WAH impact planning in all negotiations with network service providers, deciding in advance which business operations require heavy Internet usage and possibly staggering hours of operation to increase the chance of getting the needed bandwidth.\(^{62}\)

There are other societal influences that may deeply influence the success of a WAH policy. The employee at home may not have the software or hardware compatibility to interface with the work network. Bandwidth may not be sufficient to handle an increase in networked demand. For example, this occurs when large numbers of people begin using cell phones simultaneously after an earthquake or on New Year’s Eve, causing an outage. Another example is that home broadband speeds become significantly slower on school

---


\(^{62}\) Ibid.
holidays when many kids are online using social media, browsing the Internet, or playing online games.

During a pandemic, there is a high probability that Internet service providers will also be affected by absenteeism resulting in less reliable services and increased response times and longer downtime resolution. Health and safety legislation requires that suitable risk assessments be made regarding the workplace (ergonomics, lighting, etc.) Every company should assess the home workplace or provide guidelines to employees expected to work from home during a pandemic plan invocation. This should be a formal process that documents employee WAH capability. When many workers are at home, management needs to hold employees accountable for strong productivity. This ability will be stressed if management cannot control and review employee tasks effectively. Managers or other critical employees must be accounted for during the pandemic because they may be less replaceable. IT managers are hypercritical when many employees are working from home; therefore, they should be separated from other employees if at all possible.

Succession plans for critical managers is key to a successful home IT environment, so the IT managers with critical knowledge should have backups in case they cannot perform their job. Activation of company IT-recovery facilities or hot sites may be in order during a pandemic to help increase bandwidth and capabilities. This presents its own unique sets of challenges including contract seat availability and the pandemic readiness activities of the supplier. It is most likely that service levels will also be impacted.

Cost-benefit analysis should be performed on the action of mothballing the company for the short term rather than run the regulatory and infrastructure risks of employees working from home. During a time of massive business disruption it will be very tough to monitor the
amount of work being carried out and ensure the quality of that work being performed. It could be very costly to pay out sickness benefits to a low productivity workforce. This analysis will need to take place to determine what is best for each individual company.

**Enhance Communication Strategies**

Communication in any situation is critical for success. However, during a crisis it is even more important. A pandemic presents some unique challenges on the communication front that should be addressed in a dedicated annex of the pandemic response plan. Most importantly, businesses need to determine sources of accurate and current information prior to communicating to employees. Secondly, it is important for the business to communicate with one designated voice. The plan should designate who communicates and should also specify non-emergency tests for this person to communicate to employees so they are acclimatized to hearing important information from the source. Outgoing messages should be simple and should avoid any complicated language or concepts. Communications should also address language or cultural barriers as needed. The communication annex should have predetermined trigger points for communication to employees based off the pandemic status. The plans should also provide a way for employees to communicate back to the company leadership in an effective manner.

During severe disease outbreaks fear and hysteria can become widespread. Because of this fear, establishing recurring communications early on is an effective method to educate and reassure employees that actions are being taken to address the situation. Universities, hospitals, and some businesses utilize mass notification systems to distribute messages to select groups of individuals in a timely and efficient manner. The BC manager should
determine if mass communication is a good fit for his or company should assess the various
mass notification vendors. Mass notification systems tend to be quite pricey, but are typically
quite easy to use and are customizable to the individual needs of many different business
types.

Twitter, Facebook, and other Web 2.0 technologies may have significant utility for
pandemic mass notification. It may be useful to set up a private company-specific Twitter and
Facebook accounts for disaster notification so that a controlled member list of critical
customers and supply-chain partners know the status of the business for their own continuity
purposes. If the business supplies critical customers, those customers will be more
understanding if they are kept in the loop. Twitter forces the communication to be concise
and also allows for accessibility using a number of Internet-capable devices—ideal for a
disaster scenario. Additionally, by looking at the message history a Twitter account provides
a time-stamped diary of the disaster for post-disaster analysis allowing the BC manager to
build a list of takeaways to improve on for the next disaster.

Posting company pandemic response status updates to Twitter and Facebook accounts
can show business partners how the corporate culture and response attitude favors their
service, possibly leading to more business in the future. Having a closed communication
posture and a culture of complacency in the face of a seemingly uncontrollable disruption can
cause massive losses in revenue and business. During the West Coast port lockout companies
like Dell and Intel were disappointed by the attitudes of some of their suppliers who saw the
labor troubles as an uncontrollable “act of God” over which they had no control. Dell and
Intel believed these suppliers should have taken more action to reroute traffic, find
workarounds, expedite shipments, and ensure faster resumption of the flow of goods instead
of just sitting around to wait out the lockout. For some of the suppliers, the disruption did not end with the resumption of port activities, so Dell and Intel fired many of their unresponsive suppliers costing the suppliers millions of dollars in losses.\textsuperscript{63}

**GO FOR THE BASICS BY MITIGATING THE VIRAL RISK**

It may seem obvious, but one of the best pandemic response policies is to mitigate the risk of the virus spreading in the workplace. This involves telling employees to stay home when they are sick to avoid spreading the virus. The BC manager should provide materials to employees so they know what the symptoms of influenza are and when they should stay home. Such materials are available from www.flu.gov. Employees should be encouraged to wash their hands frequently and avoid touching their face during the workday. Facilities personnel should be consulted about extra disinfection in high traffic and touch areas like elevators, kitchens, doorknobs, bathrooms, and banisters throughout the facility. Often these measures offer the most bang for the buck and are something that management can support fully.

**WRITE A PANDEMIC-SPECIFIC CONTINUITY PLAN**

A specific emergency response plan for pandemic should be a sub-activity of any business continuity program regardless if the company uses department-specific planning or an enterprise-wide model. The pandemic-specific plan should take the approach of being enterprise-wide and even encompass key upstream and downstream vendors. It would be

highly useful to form a Pandemic Operations Team (POT) for pandemic response. This team should have at least three-person redundancy for each position so that the team can function during likely absenteeism at the height of the pandemic. The titles and roles of each person on the team should be clearly defined. The chain of command for the individuals should also be clearly defined. This chain of command and individuals involved will vary from industry to industry, but it is better to involve too many people than too few.

One way to tailor a pandemic-specific business continuity plan is to distribute a questionnaire specific to pandemic to the SMEs who were consulted for the broader business impact analysis to get a feeling for what impact influenza would have on their individual departments or functions. In a seven- or eight-page questionnaire, scenarios should be presented to the SMEs ranging from WHO/CDC Pandemic Alert Phase II all the way up to Alert Phase VI. Each scenario described should reflect the global and local implications of each Alert Phase so that the SME has a broad context. After SMEs from across the organization have entered their responses for the various Alert Phase impacts, the BC manager should host an awareness meeting where he or she presents the findings of the survey and encourage cross-functional discussion among the POT members and SMEs. Specific attention should be paid to preventative measures, quarantining, and absenteeism.

Based off the pandemic impact analysis, the POT should create a pandemic response plan and update it yearly based on public health threat assessments and changes to the business. The POT can use the structure of government documents like the National Incident Management System as a template and should include specific annexes or response categories. At the very least, the plan should include the annexes mentioned in Figure 7.
Unlike geographically isolated disasters like terrorism or earthquakes, pandemics are typically global in scale. Therefore, modern supply chains will likely be heavily impacted during a severe pandemic. Within the pandemic response plan an entire annex should be dedicated to supply-chain resiliency. Supply chains on which modern companies rely span dozens of countries under a variety of regimes; dealing with this reality is a must.

When looking at the supply chain, warehouse strategies should be closely examined including the concepts of extra inventory, surplus capacity, or alternative supply sources. Extra inventory is a great way to give a company time to organize its response and recovery to disruptions caused by a pandemic. Alternative suppliers should be determined and vendors should be negotiated with before the pandemic breaks out so that the business will be first in line for critical products or services when disruption occurs. It is also important to incorporate downstream customers into the supply chain resiliency annex. Key customers
should be prioritized or triaged to determine who gets limited shipments first. Metrics from knowledgeable accounts receivable personnel or input from sales management can help determine customer priority. These metrics and input should be used to form a triage list for customer supply within the supply chain resiliency annex. It would be useful to divide the customers into tiers (e.g., A, B, and C). A level customers getting limited supply before B level customers, and so on.

Since influenza is not a computer virus, it is generally assumed by employees that IT functions will be unaffected during a pandemic. This is actually faulty logic. Despite the increasing prevalence of automatic systems, IT support functions are human-centric. It is important to dedicate an entire annex of the pandemic response plan to IT functions. Normal systems may not be operational because of power shortages or lack of personnel support. Secure remote-access systems may be critical to continuation of business operations during a pandemic. IT support infrastructure is typically international in character with service call centers and hardware support based on other continents. Identifying geographic locations of all IT-related supporting functions should be a critical portion of the IT annex. Inclusion of maps and figures can be highly useful for easy interpretation when the plan is being interpreted during a crisis scenario. Worst-case scenario planning for loss of IT services and infrastructure including power loss, unavailability due to high demand, and phone outages should be thought through in the IT annex. It may be worth visiting old “paper-based” methods of business processing to mitigate the fallout of a downed IT system.

During a pandemic, it is imperative to preserve site/information security and the security posture should be laid out in a dedicated annex of the pandemic response plan. It is possible that certain supplies or items within companies will become valued commodities
within the community. Shortages of critical supplies will necessitate higher levels of security to protect critical assets. Social disruption may occur in the surrounding the facility increasing the likelihood of public panic and disorder. If alternative work sites are set up—the most likely of which is the home of the employee—it is critical to ensure security of proprietary information and the use of secure remote access. The security annex should look at physical security and IT security. The annex should consider site proximity to places where medical supplies, vaccines, or other pandemic-related healthcare resources are being stored or distributed. If the business may close down because of the pandemic, physical security personnel should provide feedback on the proper logistics required to secure the empty facility.

Subcontracting is an area where current BC and pandemic planning falls short. The outsourcer is keen to access vital skills and a pool of experts within the provider’s organization. It is often the case, however, that the provider subcontracts specific pieces of the outsourcing contract. The outsourcer must be aware of this situation and should take appropriate measure so that their interests are preserved, especially when addressing business continuity and pandemic planning efforts. It is likely that the BC practices of the subcontractor are not as robust as the primary contractor, leaving a dangerous shortfall in the outsourcer’s supply chain that will be easily exposed during a pandemic.

**Reach Out with Pandemic Preparedness Activities**

No one entity—be it government, businesses, or non-profit—can address pandemic preparedness alone. Cooperation is critical to responding to the coming pandemic. Companies need to collaborate with their local suppliers, customers, logistics providers, and
global trading partners in order to form effective pandemic response plans. Learning from
other companies' experience, and from the experience accumulated in various regulatory and
law enforcement agencies, is also crucial to reducing the likelihood of a catastrophic
disruption in a pandemic. Working together with trading partners along the supply chain
creates a safe and secure chain of custody for shipments. Working with other companies
within the same industry, including competitors, leads to benchmarking within the supply
chain annex. Organizing events and conferences where BC and pandemic preparedness
activities are discussed would be highly constructive. It may be useful to schedule an annual
conference for BC managers to discuss strategies for the upcoming flu season and include
local public health officials, first responders, and health care/hospital management. Often
relationships built before the disaster can help mitigate the impacts when the heat of disaster
begins. The phrase, “When a disaster occurs is not the time to exchange business cards,” is an
encouragement to build relationships prior to being needed in a disaster.

**Effectively Exercise the Pandemic Plan**

Once a pandemic-specific plan has been written, it is important to exercise it against a
pandemic scenario. Ideally this exercise would be a cooperative simulation integrating public
and private-sector partners who would be interacted with during a pandemic and the follow-
on disruptions. Exercising the plan just to exercise it is not sufficient. All too often,
company’s business continuity plans are not tested realistically. Prior to the exercise a “Red
Team” should think up a realistic but highly straining pandemic scenario, possibly
incorporating a second disaster like a hurricane or wildfire. By adding levels of complication,
it is likely that the business continuity plan and the pandemic plan would be activated
simultaneously, exposing weaknesses in both. Additionally, added levels of complication will most likely cause the pandemic plan to fail. This is actually a favorable outcome to the exercise because it forces the BC manager, the individuals involved directly with the exercise, and the management to realize where there are shortfalls or gaps in the existing plans. It is better to exercise to failure than to exercise mildly and assume incorrectly that the plans are robust.
CHAPTER 5

CONCLUSIONS

The threat of influenza looms and it is only a matter of time before another major pandemic breaks out. Despite best efforts to vaccinate an obstinate US public, H1N1 still lingers and may yet recombine to become more virulent. H5N1 still lingers in Asia, a few mutations away from exploding into widespread human-to-human transmission. H5N1 will not be as gentle on the public health as H1N1 was. After being warned incessantly to prepare for Hurricanes Gustav and Hanna, Gulf Coast residents were jaded when monster Hurricane Ike slammed into Galveston Island with only 60 percent of residents evacuated.

When the pandemic finally comes, it is imperative that the private sector knows what the impacts may be and what they can do to minimize those impacts with detailed and well thought out plans. Current business continuity practices are a good start to build a resiliency in the private sector, but fall short when it comes to the pandemic threat. Updating continuity plans to include pandemic-specific activities such as government monitoring, realistic exercising, communication, and mitigation should be a first priority for private-sector leaders. Lack of private-sector preparation will lead to deaths later. A large pandemic will make the country more vulnerable to the impacts of a follow-on disaster like terrorism or earthquake. It is up to the private sector to minimize the pandemic impacts so as to build national resiliency.

Businesses—large and small—are the life-blood of America, sustaining the public sector by caring for the national critical infrastructure. When the private sector is prepared
they can minimize second order pandemic impacts on supply chains, critical infrastructure, and the national economy thus protecting the country’s economic well-being and Homeland Security.
BIBLIOGRAPHY


APPENDIX A

KEY ORGANIZATIONAL STAKEHOLDERS

IN BUSINESS CONTINUITY PLANNING
Human Resources

The Human Resources department of a company is typically responsible for helping recruit new employees, managing legal issues tied to hiring/firing, and performance management. They also manage the payroll processes, benefits, and qualification profiles. Leveraging the knowledge an HR stakeholder within the organization is critical to success since BC’s number one function is to protect the well being of the organization’s employees. The HR specialist on the BC team should know how a disaster will impact their critical functions, systems, personnel, records, and how they could cross-functionally hurt seemingly non-related functions within the organization.

Information Technology

IT is a critical resource in most companies these days, and they are usually the easiest to work with when building a business continuity plan. One reason for this is because they know if there are structured plans to restore IT function in a disaster scenario, they will have an advocate in the BC planner. IT is also an area of the company that probably already has a set of plans to react to disaster scenarios with regard to their function and can provide other stakeholders on the BC team with insights and experience.

Facilities/Security

Subject matter experts from the facilities/security side of the company must be integrated into the BC planning process. They manage many unseen actions on the site of the organization including cleaning, maintenance, set up, build outs, and remodels. They deal with occupancy and tenant issues as well as other legal or licensing requirements related to business operations of the facility. These folks also usually handle the installation,
management, and monitoring of key utilities such as electricity, gas, water, and in some companies, communications equipment and infrastructure. Security personnel control access to the building and grounds. They also monitor the premises for unlawful or hazardous activity. They are usually the first responders to any structural, mechanical, or electrical failures and sometimes have to deal with unruly employees. Security personnel need to be involved with the BC planning from day one.

*Finance/Legal*

In a business, the company’s very survival depends on being able to keep track of the money. What is owed versus what is due defines the functioning of the business. Without the ability to manage the inflow and outflow of funds, the company cannot survive for long. No company can survive the loss of information related to monetary transactions, so the finance department must be able understand what systems track that data as well as how and where that data is stored, backed up, and archived and contribute that understanding to the BC process. Any company has contractual, regulatory, and other legal-related obligations they must fulfill to prevent litigation. The legal department must contribute their critical functions to the BC process because the legal ramifications of a disaster scenario on a company can be high.

*Functional Groups*

Different companies provide diverse services or products. Each functional group that leads to that service or product should have a high-up representative during the initiation phase of the BC planning process so they can identify key drivers of their function and what the implications of their loss would be during a disaster. For example, companies have
warehouses or facilities with inventory, manufacturing, research, or other activities that would need to contribute knowledge to the BC process. Because this group could be very large, a representative from each sub-function may not be practical until later in the BC process.

**Purchasing/Logistics**

Purchasing and logistic functions of the company should be integrated into BC initiation because they are the direct controllers of the company’s vendors and supply chain. They also can help buy services or back-ups for critical functions should they go down in a disaster and can provide their insights as to current and needed agreements for goods and services when getting started on the BC plan.

**Marketing and Public Relations**

This component of an organization is typically the “face” of the company. Marketing staff mine data to determine what is the best way to market and advertise the company brand. Customer Relationship Management data resides with these groups. Public relations folks are critical to communicating with the outside community of business and non-business contacts regarding the state of the company during a disaster. They ensure brand image with the public and can help a company save significant amounts of money by giving clear and accurate information in a disaster.

**Sales**

Sales representatives are also a face of the company, but solely to the company’s customers. Preserving customer relationships during a disaster can ensure a timely and
lucrative recovery. The sales staff must communicate their insights to have a complete and effective BC plan. They have a unique perspective and knowledge of the customer’s needs and insight into their psyche. It is important to point out that the sales team is also exposed to disasters in a unique way since they can be distributed over a large geographic area outside the vicinity of “headquarters.”
APPENDIX B

TIME-RELATED DEFINITIONS USED DEFINED
BY MANAGER WITH ORGANIZATIONAL
STAKEHOLDERS DURING THE BIA
Maximum Tolerable Downtime (MTD)

This is the maximum time a business can tolerate the absence or unavailability of a particular business function. If a business function is categorized as mission-critical, it will likely have the shortest MTD. There is a correlation between the criticality of a business function and its maximum downtime. The higher the criticality, the shorter the MTD is likely to be.

Recovery Time (RTO)

This is the time that is available to recover disrupted systems and resources. It is typically one segment of the MTD. For example, if a critical business process has a three-day MTD, the RTO might be one day. This is the time the functional manager will have to get the system or process up and running. The remaining two days would be used for work recovery.

Work Recovery Time (WRT)

This is the second segment of the MTD and comprises the maximum tolerable downtime (MTD). If, for example, the MTD is three days and Day 1 was the RTO, Days 2 and 3 would be the WRT. It takes time to get critical business functions up and running once the system is available again. WRT is typically overlooked in BC plans. If systems are back up and running, they could be all set from one perspective (the IT department, for example). From a business function perspective, there are additional steps that must be undertaken before it’s back to business. These critical steps getting the business function fully operational and up to normal capacity must be built into the MTD. If WRT is not accounted for, the requirements could be missed, putting the company at risk.
Recovery Point Objective (RPO)

This is the amount or extent of fallout from the disaster that can be tolerated by critical business functions. RPO has its origins in the IT realm with regard to data storage; RPO is the amount or extent of data loss that can be tolerated by critical business systems. For example, some companies perform real-time backup, while others perform weekly backups. In the weekly case if the data is backed up Saturday evenings and the system fails on Saturday afternoon, an entire week’s worth of data has been lost. If this amount of loss is not acceptable for the business, then the RPO should be changed to bi-weekly basis or even more frequent. The RPO has few applications in the broader business outside the IT department. The RPO is based both on current operating procedures and the estimate by the company leadership of what might happen in the event of a business disruption. However, if the data loss causes any system to become unavailable altogether, the RTO would kick in and RTOs can have applications outside of the IT department (like the closing down of a manufacturing line, laboratory, or warehouse because one of their dependent systems is unavailable).