IBM Global Technology Services
Thought Leadership White Paper

November 2013

Five essentials for better work force continuity

Integrating the human side into your strategy

Contents

Executive summary

For most organizations, it will be business as usual today. But for a small number of organizations, today could bring a disruptive event. A hurricane suddenly tracks straight toward a primary manufacturing facility. Conditions surrounding a small threat of civil unrest change radically overnight. Or a major power outage occurs without warning.

No matter how slight the risk appears, organizations know that the threat of a disaster is always a possibility. As a result, many organizations—and most likely yours—have taken steps to incorporate disaster recovery planning for their facilities and technology. After all, any event that disrupts business, whether limited or broad in scope, can undermine your ability to remain competitive—and maybe even to survive. But you may not have fully considered the impact of a disruption on your most valuable asset: your employees. Civil unrest, terrorism, and natural and man-made disasters can be life threatening or hinder your workforce from its ability to continue business in multiple ways. Getting into the office may be impossible, and depending on the crisis scenario, working from home may not be available as a solution.

IBM first began this conversation several years ago with a white paper titled, “Business continuity: How to increase workforce resiliency during disasters.” This paper shared insights regarding the most pressing challenges surrounding workforce resiliency and described five key ways to prepare for continuity during business disruptions. Since then, both the risk landscape and technology have significantly evolved. Risks are constantly changing and new types of risk that affect the workforce are increasing in both impact and frequency. Social media has become more widespread and the potential for reputational damage from a negative or erroneous post following a disaster must now be taken into account.

With extensive business continuity and disaster recovery experience gained from thousands of client engagements, IBM recommends periodic assessments to determine how or if planning should be modified. Accordingly, we re-examined the topic of the human element of business continuity planning. This paper shares new insights that have occurred since the initial paper and outlines components critical to workforce continuity based on today’s dynamics.

The coming storm: Are you ready?

A quick survey of headlines makes it clear that disasters and their effects come in many forms. Superstorm Sandy caused widespread flooding and power outages. The storm disrupted the functioning of 25 percent of cell towers in the affected area and prompted the New York Stock Exchange to close for two days due to a weather-related event, the first time in 30 years.[1] Although hurricanes are not a new threat for catastrophic damage, what has changed are the impacts after the event. Not all of the damage resulted from the actual hurricane. Negative and inaccurate information from social media posts, blogs and tweets caused their own very real and significant damage.

Added to the ever-present threat of natural disasters like hurricanes, typhoons, tsunamis, tornados, floods, earthquakes and epidemics are increasing threats of strikes, demonstrations and other forms of public outcry. Despite the many forms disasters can take shape and the myriad consequences that can arise from them, they share one element in common: they impact people. What would happen to your business if your workers were unable to perform their jobs—even after they have made personal arrangements and ensured the safety of family and friends? If critical operations are broken in one area, do you have a well-tested plan to transition the work—and possibly your staff—to another, unaffected area? Severe weather could impact mobility and keep employees from getting to your facility. And in the absence of an authoritative source of information, employees and shareholders could receive faulty updates gleaned from unconfirmed social posts.

Business continuity plans must therefore not only address how to keep business systems running, but also must consider the needs of the workforce. From the obvious requirement of workers being able to resume their jobs, to their important everyday needs of food, shelter and ensuring the safety and security of their families, many components must be factored into your plan.

Operations: How will decisions be made? And by whom in the chain of command, if key decision makers are not available? When? What is your business continuity plan for critical support functions like payroll?

Communication: How will you exchange accurate and timely information with your workforce and the public? How will you interact with the different stakeholder communities like employees, customers, suppliers, partners, authorities, shareholders and the media?

Technology: What technologies will you employ to enable communication? How will your workforce regain connectivity?

Work area: Have you identified alternatives to regain access to information and technology to resume tasks—whether physical, mobile or virtual facilities?

People planning: How will you track the well-being of your workforce during a disruption and what resources will you provide? Have you identified critical skills and provided cross-training for crucial roles? Does your business continuity plan consider the crisis plans of your local communities where your facilities and employees reside?

Five critical components for workforce continuity

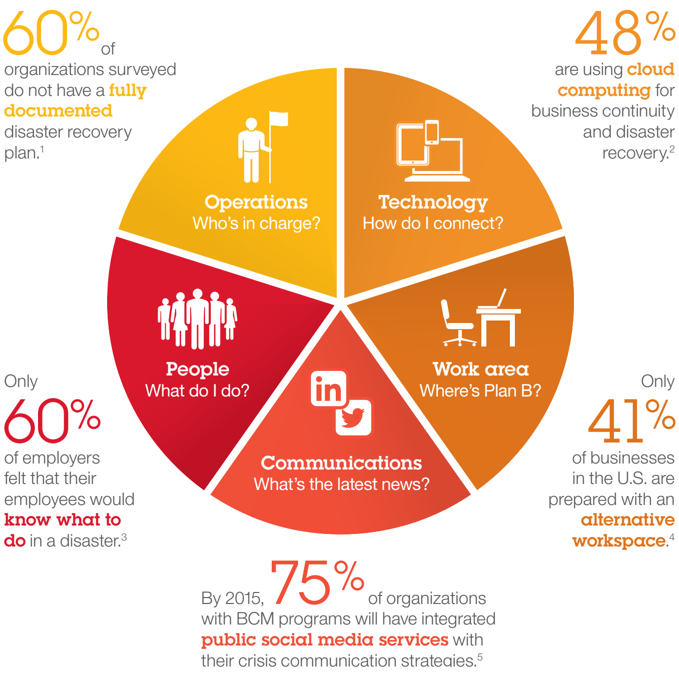

Figure 1. Critical components in workforce continuity planning

Keeping (more than) the lights on: Maintaining operations

If a sudden disruption threatens the continuous operations of your business, how will you maintain operations? Who will be in charge, and how will you maintain an audit trail of authority and access mandated by regulatory requirements? Will you be able to maintain critical functions like payroll services?

Your organization's ability to respond in a timely, relevant manner to a crisis depends, in part, on how well it has identified and documented—ahead of time and as part of the overall continuity plan—the processes, procedures and functions most critical to your business and to your employees. Consider how policies overseeing all employee schedules, including those away from office on leave, vacation or official travel for example, can be adapted to apply specifically to times of disaster. Once a disaster hits, keep policy and procedure updates clear and concise.

Also, you will want to clearly define your company's immediate response roles and responsibilities. Many times, organizational leaders are incapacitated or unavailable during or after a disaster. Assigning the key responsibility of decision making to a single person can be risky. If that person becomes unavailable, individuals at all levels may be forced to take on leadership roles or increased responsibilities. And those individuals may have little or no preparation.

Succession planning, assigning backup responsibilities and defining organizational expectations can help you have someone available to take command and control in a crisis situation. Consider dividing decision-making responsibility. Global enterprises may delegate decision making to point persons in each geographic area, each of whom can adapt the business continuity processes to localized operations and their unique situations. The lead decision maker should have the role of making adjustments as necessary and communicating these changes to the rest of the workforce. Planning and conducting drills is also important to help all stakeholders better understand their responsibilities and what is expected of them during different levels of crisis situations. This can help you troubleshoot issues and improve plans beforehand.

Maintaining key services to your workforce such as payroll and email is both essential and challenging during and following a crisis. If your payroll system—direct deposit or mail delivery service—is inaccessible, funds are limited or the staff members who are responsible for payroll are absent, it is going to be difficult to pay employees in a timely manner. A contingency plan can help make sure workers are compensated if funds, payroll systems or administrators are inaccessible.

Also consider how to provision additional access with proper security controls for your business processes, applications and data. If a key business person is unavailable, a backup will have to be authorized, and an audit trail of authority and access maintained. When possible, these authorizations should be made in conjunction with the current separation of duties matrices mandated by your corporate governance processes as well as insurance and regulatory requirements. There is a tendency during a crisis to bypass data-retention policies and revert to informal processes and communications, so make sure you document the decisions made and the information available at that time that led to the decision.

Taking charge with communications

Your communication strategy is a vital component of an effective business continuity plan. Implement regular communications on emergency preparedness, steps and information to employees and key stakeholders through newsletters, wallet cards, intranet sites, social media and smart devices to reinforce preparedness levels across your organization.

After an incident, once you have identified and isolated the crisis and assessed its effects, communications should offer assurance that you are taking control and implementing a plan to return to normal conditions. A successful communication plan lets you exchange authoritative, accurate and timely information with the different stakeholders within and across your organization: internal employees, the media, customers, suppliers and business partners, and authorities and government agencies. Your communication strategy should employ different messages and channels for each of these stakeholder communities with central coordination among them. For instance, when civil authorities are involved, you have to make sure your instructions do not contradict public announcements.

Your communication strategy for your workforce should include facilities for two-way communications apart from normal channels, where employees can sign in and communicate their status and make specific requests for help and assistance if needed. Internal workers' family members may need a way to inquire about a disruption that affects your workforce, so you will want to consider a strategy for responding to their queries, as well as an external communication strategy to proactively address media and outside questions. Your message should be clear, consistent and concise, and take into account the situation's level of severity and human emotions. Maintain a predictable schedule for updates to your workforce as well as the surrounding community.

Communication plays a major role in preserving relationships and collaborating with customers, suppliers and partners. Because your suppliers' ability to deliver could also be affected by a disruption, working with them is essential to making sure your workforce has what it needs to continue or restart business operations.

Another aspect of communication includes how you will interface with civil authorities. Your plan should include collaboration with local authorities and adherence to possible restrictions they mandate, including building access, travel restrictions and curfews. Collaborating with civil authorities may also involve participation in their drills and exercises that test responses to emergencies. Along these lines, you should test all facets of your workforce continuity plan—including your internal and external crisis communication methods as well as how you collaborate with vendors and suppliers—to make sure your plan is current and reliable.

As you devise a communication strategy, consider the following:

- Does your company have a procedure for issuing instructions to workers at home?
- Are there ways for the key decision maker to communicate with your workforce? Are there backup methods in case the primary ways (for example, phone connections) are unavailable?
- Do members of your workforce have a way to reach someone in charge to inquire about the situation and provide an update of their own situations and availability?
- Have you prepared communication templates, with agreed upon language that can be configured to the actual crisis?
- Have you prepared key authorization messages in advance? Have you identified the different stakeholders within and outside your organization for whom you will need to build communication strategies?

Using technology in times of crisis

A technology outage can be crippling for organizations, and regaining access to it is a top priority during a crisis. At the same time, technology is the means through which you can provide communication to your workforce.

A crisis notification service may be helpful during an emergency, when normal lines of communication fail. Using a hosted communication platform to contact your workers and other stakeholders through email, Short Message Service (SMS), fax and voice and various communication tools can enable you to collect and distribute information during the event, and potentially accelerate recovery times.

A return to normal communication is aided by re-establishing connectivity. After workers' immediate needs have been met in the wake of a disruption, you can then focus on what they require in order to continue working. For those working from home, make sure you provide high-speed Internet access, voice lines and the ability to cross a secure gateway. Cloud computing can further support connectivity objectives by delivering applications independently from the underlying infrastructure, so you can put resources where they need to be in order for your workforce to access them and continue business operations. Cloud-based services can also be used for voice-related user capabilities like voicemail, call recording and emergency responses.

Desktop virtualization is another solution to help make your organization more resilient and productive in the face of short-term or small-scale disruptions. By storing a virtual copy of a worker's desktop on a remote server rather than on the worker's hard drive, you can allow access to that desktop from any location. Desktop virtualization can increase the effectiveness of your remote-access plan by enabling your workforce to access business-critical applications from home or an alternate work location.

Keeping the call centers open

When it comes to disasters, utilities are on the front line. A natural gas company in the United States realized that its call center lacked a feasible failover plan, leaving it vulnerable to any unforeseen event or disaster and preventing employees from being able to communicate with customers. To provide reliable customer service for its nearly four million subscribers, NiSource needed to invest in a solution that would facilitate its availability to customers during a disaster or outage. By engaging IBM Global Technology Services – Integrated Technology Services to implement a remote call center based on IBM System x servers housed in a remote IBM location, NiSource gained a more secure business-continuity environment that will allow it to support customers during a disaster or outage without interruption.

Whichever technology you ultimately decide to employ, it is essential to conduct drills to test the various technologies that you plan to use to help stakeholders understand how to apply them and to uncover potential issues so that they can be addressed in advance.

The rising role of social media

Since we first discussed the role of social networking in work-force continuity several years ago, social media has become perhaps one of the most important ways to reconnect with your workforce, issue instructions, to send an important message or for two-way communications between you and your employees during a crisis. A well planned and well managed social media strategy can be a significant resource that can aid not only internal communications with employees but also externally. Blogs, wikis and social sites can easily be accessed by your workers through a web browser. These forms of communication can also be used as effective public relations channels to update those external to your organization about how you are handling the crisis—or even to dispel rumors. Despite their accessibility, social communications must be controlled carefully, with active listening for negative or false messages that unchecked could proliferate rapidly, potentially harming your reputation. Essentially, your organization's ability and reputation to better handle crisis situations by leveraging social media for communications depends on how your social strategy enables communication of the right information to the right people at the right time.

Recovering the work area that supports your employees

To be adequately prepared for virtually any situation, your workforce continuity plan needs to be flexible and extensible to address specific disruptions. For workers who must report to a physical location, you might need to evaluate options for work area recovery services, which could include physical work seats, virtual workplaces, mobile work units or a combination of all three.

Physical recovery centers can enable you to give key personnel access to a secure-rich, more comfortable work environment during a disaster or outage emergency. Recovery centers can be equipped with work area spaces, imaged PC workstations, voice communication, and network connectivity and other critical office equipment such as printers. These centers can be dedicated or shared, depending on business need. Dedicated solutions can provide immediate access to a custom engineered environment for your exclusive use during recovery exercises or outage emergencies. Shared physical work area solutions spread costs across a larger community of interest while still providing fully configured work environments for business operations.

In some cases, employees may not be able to get to the recovery facility or an organization may require recovery operations to be based next to or close to an affected site. Depending on the scenario, a mobile recovery center can help your employees return to work quickly at a local site. Mobile recovery centers can provide network connectivity, workstations, voice communication, office equipment, HVAC and generators for a fully functioning work environment independent of local utilities.

An alternate worksite helps keep workers productive

When one of Ireland's leading insurance companies suffered a major flooding incident at its main office, the building was out of action for nearly four weeks. Thanks to its disaster recovery plan, the organization was not. Key IBM staff from IBM Business Continuity and Resiliency Services mobilized rapidly and were available around the clock to support the insurance company's continuity and recovery plan. Employees from the insurance company were able to quickly relocate to an alternate work area where PCs, phones, parking and catering facilities helped the organization continue with business as usual until its office could be restored.

Remote, security-rich access to necessary systems can help keep your workers productive, especially if they have to remain home for long periods of time or if they have been displaced from their normal place of work. If your workers simply cannot be at a corporate facility but are not hampered in any other way, remote access should be a significant component of your business continuity plan.

Providing support for your workforce

Although the initial focus of the strategy is getting your workforce back online and being productive, the effects of some events are often personal and could extend from school or day care closings to general shock, loss of a loved one or a home being destroyed. In severe crises, employees may be uncertain if they will return to work at all. Especially during a calamitous event, your business continuity strategy needs to factor in the emotional and physical impacts on your workforce.

In general, you should plan to provide critical support services, or at least have resources at your fingertips, for services that can include:

- Healthcare and crisis intervention services
- Transport
- Repair services
- Temporary housing
- Child care accommodations
- Financial assistance and incentives

Your continuity strategy must also take into consideration the crisis plans of your local communities where your facilities and employees reside. Contingency plans for your workers' safety and return to normalcy might mean being prepared to transport them to a shelter or provide alternate accommodations for those displaced from their homes, including pets. Care should be taken to also plan to support members of your workforce with special needs. Even if employees are able and willing to work through a disaster, they may simply not be able to get to their work location. Public transportation systems may be disrupted, or travel restrictions could be in force. Even smaller-scale disasters, such as transit strikes and blizzards, can significantly impact employees' ability to get to work.

With civil unrest, terrorism or natural disasters, the ability of your workforce to maintain business operations can hinge on your ability to account for their safety. For some industrial enterprises, such as power and manufacturing plants, contingencies for safe evacuation are essential. Innovative use of technologies such as radio frequency identification (RFID) can help track workers and visitors, and account for their safety—even easing collaboration with first responders from local authorities. Your lead decision maker should determine contingencies based on the local effect and adjust the plan accordingly.

An RFID solution helps track workers and monitor their safety

A multinational petroleum refinery engaged IBM to develop an emergency mustering solution that is designed to translate RFID data into actionable, visual information that serves as the cornerstone of new safety procedures. By integrating active RFID technology with its business processes, the refinery gains a graphical, near-real-time view of all employees—wherever they are. Flexible business rules developed for the solution can enable the refinery to extend the benefits of near-real-time RFID into major improvements in emergency evacuation preparedness and employee safety.

In addition to these immediate contingencies, your business continuity strategy should incorporate cross-training of your workers in emergency and business-critical processes. If you form a team of workers to be your first phase of recovery following a disruption, you must plan for members of that team to operate in shifts to allow them to recuperate, supporting a steady stream of alert minds. It is imperative to build flexibility into your plan for maintaining continuity of critical skills because the makeup of your workforce can change rapidly.

Listening and learning from social media

The massive hurricane known as Superstorm Sandy was one of the most widely covered disasters in recent history. Social media played a pivotal role in the coverage (nearly 5,852 Superstorm Sandy disaster recovery and resiliency-related discussions were recorded in that quarter) with the majority of the volume generated on the day Sandy hit the United States.

IBM conducted a listening study of social media activity that took place during the storm to help understand volume, sentiment, venue and messaging around the hurricane in relation to disaster recovery, continuity and resiliency discussions. Specifically, IBM wanted to better understand what types of messaging were generated and perceived, and what we could learn from them.

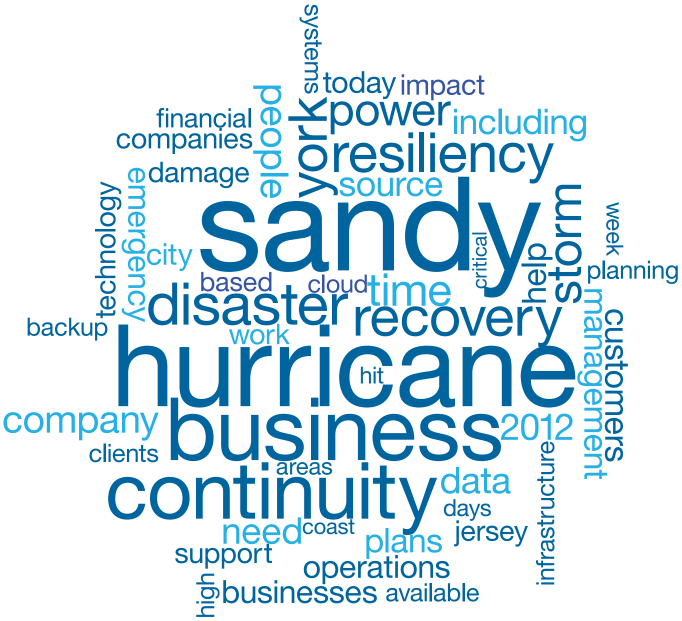

Figure 2. A word cloud generated during the social listening study of Superstorm Sandy

Key highlights from the study:

- Analysts emphasized the need for more comprehensive business resiliency and workforce continuity plans. Their conversations highlighted the severity that a disaster can reach and underlined the need to focus on not just resiliency but specifically workforce continuity for an effective continuity strategy.
- Industry specialists emphasized adoption of disaster recovery as a service (DRaaS) and strong business continuity plans to deal with natural disasters like Sandy, highlighting the growing push toward new approaches to disaster recovery like SaaS and cloud-based services.
- Many data recovery companies reported on the impact on their data center operations, emphasizing the need for organizations to think about their business continuity and disaster recovery service providers and underlining the necessity to evaluate their capabilities and levels of preparedness.
- Journalists and bloggers posted news on power, data center and website outages, highlighting the reality that the disaster recovery plans and failures are being picked up by social media and are impossible to hide.

How IBM can help

Factoring your workforce into a business continuity strategy requires expertise in a variety of areas—such as disaster recovery, human resources and organizational culture and psychology. It may also require the deployment of remote-access technologies, communications tools, cloud computing and dynamic provisioning of resources. As a global leader in business continuity and resiliency services and human capital management, IBM has the experience to help you incorporate critical success factors for workforce continuity into your overall business continuity strategy.

As part of our portfolio of business continuity and resiliency services, IBM can provide the facilities, technology, application and data recovery, and network connectivity you need for workers to continue their jobs after a sudden disruption. By assisting you in deploying cloud computing and virtualization solutions, IBM can help you keep your workforce productive regardless of circumstances or location.

From the initial step of performing a risk analysis through the important phases of validation and testing, our services are designed to increase the resilience of your workforce and their ability to continue business activities when an event disrupts your operations. With IBM Resiliency Consulting Services, our consultants can develop and implement a strategy to balance your risk level with the cost of continuous availability—for optimum productivity. Combined with IBM human capital management solutions that help you nurture and grow talent, track skills and improve collaboration, our consulting services can identify, create, architect, assess, implement and help manage your current plans for business continuity and augment them to include the workforce recovery components. IBM® SmartCloud® Resilience offers cloud-based services such as IBM SmartCloud Managed Backup services that include both onsite and remote data protection for your data center servers, applications and databases as well as email, laptops and desktops—enabling you to more quickly back up, restore, archive and maintain access to critical data. IBM SmartCloud Content Management is an integrated service for content and record management that includes centralized archiving, indexing, search and retrieval of data that can help you better manage compliance and eDiscovery. Another cloud-based service, IBM SmartCloud Virtualized Recovery services, provides similar capabilities for servers and applications for faster, more reliable and affordable IT infrastructure recovery.

IBM Infrastructure Recovery Services cover both work area recovery and IT recovery. IBM's work area recovery services allow organizations to better protect alternate work environments with IBM's worldwide network of over 150 business resiliency centers during times of disruption or disaster. These highly security-rich facilities offer ready-to-use workstations equipped with personal computers, phones and other work tools. The facilities are equipped with redundant communications capabilities, multivendor IT equipment and uninterruptible power supplies and are staffed by IBM recovery specialists. In some regions, IBM offers a mobile IT recovery option through which mobile units are delivered to a site of the organization's choosing for temporary use.

IBM Managed Resiliency Services can help organizations keep their critical business processes operational and business information accessible in the event of an outage. These services support integrated administration, monitoring, data protection and disaster recovery. By managing and operating these services—either fully or partially—IBM can help businesses avoid downtime, improve staff productivity, handle operational expenses and manage regulatory requirements.

For more information

To learn more about implementing a world-class workforce continuity and recovery solution through IBM Business Continuity and Resiliency Services, contact your IBM representative or IBM Business Partner, or visit the following website: **ibm.com**/services/continuity/

Additionally, IBM Global Financing can help you acquire the IT solutions that your business needs in the most cost-effective and strategic way possible. We'll partner with credit-qualified clients to customize an IT financing solution to suit your business goals, enable effective cash management, and improve your total cost of ownership. IBM Global Financing is your smartest choice to fund critical IT investments and propel your business forward. For more information, visit: **ibm.com**/financing

IBM Corporation
IBM Global Technology Services
Route 100
Somers, NY 10589

Produced in the United States of America
November 2013

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

[1] http://drbenchmark.org/wp-content/uploads/2013/08/REPORT_DRPBenchmark_Survey_Results_Aug_20131.pdf

[2] www.dataprotection.com

[3] www.storagecraft.com

[4] http://vaultit.com

[5] Gartner, "The Do's and Don'ts of Using Social Media in Business Continuity Management," 19 January 2012 G00223615, Gartner Foundational: 2 July 2013.
Analysts: Andrew Walls and Roberta J. Witty.

♲ Please Recycle