RLR
MANAGEMENT CONSULTING, INC.

Business Continuity Plan – Are You Prepared?

By Ruth Razook and Neva McCormick

The disasters of late remind us that we need to have a solid Business Continuity Plan. June 1st each year marks the beginning of hurricane season, we have known that for years. How bad could it be? We did not know. Nor did we expect a 7.1 earthquake in Mexico. With Harvey, Irma, Maria (and even Jose), the hurricanes left trails of destruction. We see the pictures of the devastation to homes, businesses (and whole islands). However, do we consider as a Bank, How prepared are we?

Now is the perfect time to take a good, hard look at your Business Continuity Plan and formulate your plans for how you can minimize the potential impact of not just a hurricane or earthquake, but any kind of disaster to your financial institution. Not everyone lives where a hurricane or earthquake could be disaster, but have you also considered the impact to your customers of

- A major server crashing?
- A security breach?
- Extended power outages?
- Sabotage?
- What about cybercrime?

The key is to develop a business continuity plan to not only recover after a disaster but to continue providing services your customers may desperately need after the disaster. Your plan must lay out the detailed processes and procedures for the steps your company will take after a disaster or any other type of business disruption in order to get your operations back up and running again as quickly as possible.

In the 1994 southern California earthquake our Bank had “an earthquake kit” in the garage, ready to go, attributable to a school project. After the 6.4 earthquake hit, we went to retrieve the kit. This was going to be the solution to help us recover the Bank’s services. Instead, during the earthquake, cans of paint on the shelf fell on top of the kit, breaking open the bottle of chlorine bleach and ruining everything in the kit! Needless to say, “Best laid plans!”

Thoroughly review and evaluate your plan, look at it with a critical eye with a goal of identifying the weaknesses in your plan and then providing solutions to those weaknesses. Once you have identified and addressed the plan's weaknesses, test your Plan. Truly test your plan to ensure you would be able to recover and continue to serve your customers. Testing is a critical part of the program!

A business continuity plan should consist of two main parts:

1) Short-term planning to minimize the immediate impact of the disaster or business interruption. The goal must be to have your critical infrastructure and systems back up and running as quickly as possible. This includes your physical facility, telecommunication and IT systems, hardware and software, and other critical business equipment.

Facilities are often the first priority after a natural disaster, since employees who don't work from home will need to have somewhere to report to work. One option some of our clients have opted for is to contract with a disaster recovery hot site that will provide office space where employees can work temporarily until your facilities are operational. If you have that solution, have you thoroughly tested that solution? Have you considered what happens when there is an area-wide disaster, do you have priority at that solution? Will there still be a work area available?

Telecom and IT systems usually are the next disaster recovery priority. Cell phones may not work post disaster, so you need to consider alternative communication methods like two-way radios, for example. Securing offsite hosting might be another option for your IT systems, while software should be backed up regularly with copies stored offsite. Using cloud computing is one way to maximize the risk of these disruptions after a disaster. Have you tested these solutions?

2) Longer-term planning is included as part of your plan to ensure recoverability and continuity for business operations in the weeks and months after the interruption. Once you have made it past the first few post-disaster days, your Plan must include steps for how your financial institution will ramp back up to pre-disaster interruption protection and service levels - how will you maintain them?

Where do you start? Determine where your financial institution is most vulnerable to specific business interruption risks. Quantify the potential impact of those risks on your business so you know how to prioritize your planning time and resources.

Rank each of your business applications, operations and functions as either critical, sensitive or non-critical. Restoring critical functions that your business cannot operate without should be the highest priority and receive the bulk of planning resources, while sensitive functions are next.

Non-critical functions should be last on the priority list and addressed only after all other functions are up and running.

Be sure you have a list of *current* contact information for all your employees, customers, vendors and regulators. Store them in a safe place where it is accessible after a disaster or disruption, such as in the cloud. You need to make your employees aware of when and how they are to report to work post-disaster. Also let your customers and vendors know how the disaster or interruption could impact them. Communicate with your regulators letting them know your status if you have been impacted. Training and testing is key to the company's recovery and continuity.

Disasters can and will occur when you least expect them. Proactively prepare and have a business continuity plan in place.

RLR Management Consulting
For more information, visit www.rlrmgmt.com and follow the company on LinkedIn and Twitter