

Preparing for Disaster in the 21st Century

Dan Bagus, Vice President, Recovery Solutions, Plainfield, IL



as future costs to maintain the plan. Finally, in carrying out their fiduciary responsibilities, decision-makers must consider the cost/benefit trade-off of these options and elect an appropriate course of action.

While there are a myriad of reasons to avoid consideration of an updated disaster-recovery plan, and many other factors to consider than those offered below, we wanted to address a common belief that the bank can “react” to a catastrophic situation with existing resources and equipment. The belief is that technical expertise on staff or existing relationships can be leveraged to secure technology, equipment, an alternative location, etc. There are many risks and weaknesses in this approach. We have addressed three of the primary issues below:

1. In a disaster situation staff is often personally affected by the situation and is not focused on getting the bank back up and operational, but rather on the safety and security of their families.
2. Under the circumstances, local resources will be depleted with demand for disaster related services substantially higher.
3. The amount of time by which to deploy those resources (if they could be secured) and place them into operational status will be substantial. Those resources include devices such as servers, switches, firewalls, workstations, laser, and teller and imaging equipment, to name a few. Furthermore, this technology must be configured to meet network specifications.

It is unlikely that any one of these three risks can be overcome within standard *Recovery Time Objectives*. If your RTO is not met, the operational analysis and the fiduciary decisions must realistically consider the impact this will have on your business (*business impact analysis*), as noted above.

With the degree of competition in the industry, it is imperative that you prepare **and test** for the worst. If you don't, and circumstances prevent you from “reacting” in a timely fashion it is likely that

With the severe tornados, floods, and storms this current spring season is putting us on pace to set a new record for FEMA declared disasters and a high-risk hurricane season projected, we wanted to take this opportunity to share some thoughts and experience on disaster preparedness.

Obviously, given the state of the economy and the industry, one of the last things that bankers want to consider is another “insurance premium” for something they may never experience. Disaster is often considered a long-shot and preparedness only undertaken when the regulators require it.

Nevertheless, an up-to-date, disaster-related process must be undertaken whereby solutions are analyzed; options considered; and *informed* decisions made. As we all know, technology is changing rapidly and our reliance on it often leaves us more and more vulnerable, particular-

ly given the heightened state of disaster declaration. You should also know that with advanced technology come advanced disaster recovery solutions.

The challenge of the analytical phase of the process is to make a convincing presentation that warrants consideration of the expenditure required for updated preparedness. Think of it as cost-effective protection of your current investment in technology and infrastructure. The days of off-line transactions and trail balances should be left far behind.

An effective analysis should begin with a thorough and honest assessment of the risk of disaster and its possible impact on your business and market share. Next, research should be conducted and information gathered to recommend options for preparedness to decision-makers. A critical component of the analysis and recommendations will be a comparison of the bank's current cost of its plan to restore operations as well

Community Bankers Association of Illinois

you will lose a substantial share of the market you have worked hard and long to secure. This can cause irreparable damage to the reputation of your business.

There is another key component that is often not factored into the analytical and decision-making processes. For the sake of argument, let us assume you were able to overcome the primary hurdles outlined above within your Recovery Time Objective. Perhaps your preparedness had incorporated redundant workstations, printers and the like; and it includes offsite data storage, electronic data back-up, and/or provision for redundant proprietary servers to access core applications.

The underlying issue now becomes: how you will gain access to those back-up services, the Internet, other key correspondent services and phone, if telecommunications are out. In wide-area disasters telecommunications and wireless options are invariably impaired, making the aforementioned redundancy built into the disaster preparedness of little or no value. A key rule to

keep in mind throughout this process is: if you cannot communicate, you cannot recover. Under such circumstances satellite communications is one of, or perhaps the only, effective means of connectivity.

You should be aware that it exists and factor it into your overall evaluation and decision making processes. Furthermore, you should expect your disaster recovery vendor to offer a Live Site Test to provide assurance the solution to which you have subscribed will actually work in a disaster situation. This test should allow you to perform live transactions just as you would in an actual disaster – this is the only real way to have confidence in your provider and to satisfy management, directorate, and the regulators that you have a true turn-key solution. ■

Recovery Solutions is a CBSC preferred vendor. For more information, contact Bagus at 815/577-1999, ext 303. You can also visit Recovery Solutions on the web at: www.recoveryolutions.com.