

Plan a Better Disaster: Getting a Handle on Planning and Recovery

Disasters, both natural and man-made, can instantly cripple a bank and the surrounding community without warning, leaving your bank and community without the resources needed to rebuild.

Examiners require a working business recovery plan to show evidence that the plan is still viable. But just having a plan is not enough. A bank has to know the plan works when the worst happens, which makes the difference between minimal customer impact and total loss.

“Working” Plan Considerations

The first component of disaster recovery plan is to identify the most likely scenarios threatening your bank. For example, for Laurie Leighty, senior vice president at Santa Barbara, Calif.-based American Riviera Bank, this includes natural disasters such as fires, earthquakes, and mud or flood issues. For another bank, it might be snow, ice or heat. Besides natural disasters, banks should also consider technological disasters, domestic terrorism, breached security or even the loss of communications or other infrastructure systems such as transportation or utilities.

Next, banks should identify critical systems and services required for limited operations immediately following a disaster. Developing a plan can be made easier by choosing and working with a quality core provider with the latest technologies and expertise, and one that will coordinate with third parties and other crucial system suppliers. After human safety, one of the highest priorities for all banks is reconnecting to their core system to access customer data and enable communications for required bank functions.

The core provider should be intimately aware of, and able to provide, multiple disaster contingency technologies, methods and tests, and should serve as an expert source of assistance when putting together the plan. For example, core processors utilizing new technologies and practices in communications, virtualization and redundant mass storage mean a bank should be able to recover the core processing system – including live data – in a matter of minutes to a few hours.

Practice Practice Practice

The true key to disaster preparedness is testing the plan to ensure it will truly recover the bank, and that the emergency plans are complete.

The key to successful testing is to focus on the objectives that are most critical to reopening basic services quickly. In any disaster, the primary objective is to save lives, reduce injury, reopen with basic services as soon as possible until auxiliary services can be added as necessary.

Again, collaborating with a core processor that is knowledgeable, experienced and prepared is a step toward successful testing.

“Our core processor has continually worked tests with many banks over the years,” Leighty said. “When we complete our tests, they are able to walk us completely through the software, hardware and settings we need to quickly reconnect our bank.”

Working with the core provider, the bank set up the ability to remotely connect to their processor and recover data “...from any computer,” Leighty said. “I also tested it by successfully connecting from multiple off-site locations even before conducting the official test.”

Additionally, the bank’s core processor provided a simple set of written instructions that any employee enacting the emergency plan could follow. To truly test whether the emergency plan works, American Riviera Bank sends their least tech-savvy person to conduct the official tests.

“When our employee arrives at the test site, using the instructions in the emergency plan, he or she is able to securely connect into our core processor immediately,” Leighty said. “In our last test, the test site agency said that it was the first time they had seen a bank like ours connect successfully the first time.” Leighty attributed the successful test to a clear and focused plan and the strong relationship with the core processor that helped establish the needed protocols during planning.

When Disaster Strikes

Emergency plans are written with the hope that they will never have to be used. Unfortunately disasters do happen. When a bank is faced with a crisis, the first thing to do is assess what actually happened, the severity of damage and the human impact.

First take care of any injuries or life-threatening situations. Then the first call should be to your core provider and other necessary functions identified in the plan. With the right plan and core provider using

the right technology, basic services can be restored to pre-disaster live status in less than an hour. Within a day, a bank can even be set up for full service in a new building.

Proper evaluation of disaster scenarios and the help of a capable, caring core processor can ease the burden on banks before, during and after a crisis so they can continue to serve the community and stay competitive whatever disasters may arise.

Robert Ross is a Certified Disaster Recovery Planner, the senior vice president of Network and Technical Services, and the Chief Security Officer of Hutchinson, Kan.-based DCI, a bank-owned provider of processing and technology products and services nationwide. For more information, visit www.datacenterinc.com or e-mail sales.dci@datacenterinc.com.