

Re-thinking Recovery

When was the last time you really looked at your disaster recovery (DR) strategy? Not just the big binder on the shelf that documents downtime procedures. I mean the actual “strategy” to recover your operations. If there were a “disaster” at your bank today, how soon could you recover?

Investing in DR is a tough pill to swallow. It’s difficult to justify an investment that: 1) you hope you will never have to use and 2) doesn’t contribute revenue.

Hot Sites May Not Be a Cure All

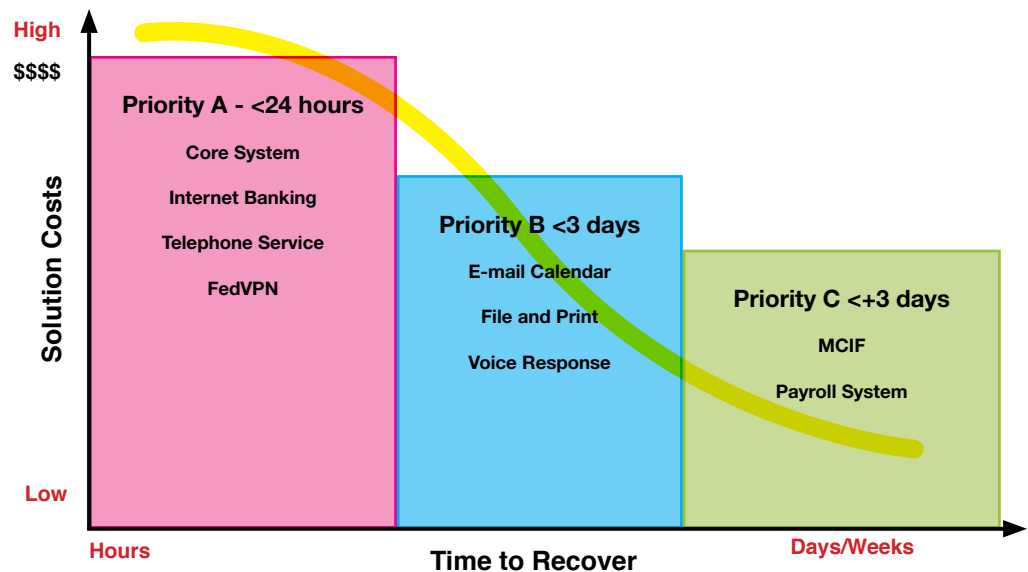
To solve this problem, many banks contract “hot-site” services—an alternate data center with vendor-owned equipment. By sharing (and over-subscribing) access to these resources, vendors are able to offer attractive pricing. And, the chances are pretty slim that multiple banks will need access to these resources at the same time, which makes this a pretty sound plan, right? Possibly, provided that the relationship is diligently managed.

Some common problems include:

- The equipment originally contracted from the hot-site vendor is no longer what the bank uses for its core system. The production environment changes, but your recovery contract does not.
- All the add-on critical services (ATM provider connectivity, Fed interface, lending applications) are not addressed.
- Insufficient telecommunications recovery capabilities
 - Branch data connectivity to DR site
 - Internet services re-direction for web, e-mail and vendor connectivity (e.g. FedVPN)
 - Voice telecommunication re-direction
 - Limited or inadequate testing

How to Begin Assessing DR Strategy

First, define your business requirements—acceptable IT services and recovery objectives. The “Priority Graph” shown below defines the recovery priorities and corresponding acceptable timeframes.



Once management concurs with the defined requirements, begin to assess how the strategy meets the business requirements.

Commenting on Fidelity Bank’s (Edina) recent assessment of its recovery capabilities and strategy, Teresa Keegan, CFO of Fidelity Bank, said, “Recovery and continued operations have always been our top priorities—driven by our customer commitment more than any regulatory requirement. More and increasingly complex systems, as well as Internet banking, dramatically changed our business requirements. We owe it to our customers to recover critical systems in less than one day.”

Fidelity Bank reviewed the alternatives with Assurity River Group: modifying the existing “hot-site” agreement; bringing DR in-house at its branch; bringing DR capabilities in-house using a commercial data center; reciprocal agreements.

Based on thorough risk and financial analyses involving all departments, Fidelity’s executive management decided to bring DR capabilities in-house by hosting recovery equipment at an off-site commercial data center. “We were pleasantly surprised to find that for comparable overall cost, we could own dedicated equipment and significantly improve our recovery time,” explains Ms. Keegan. “Reduced costs for equipment, data center space, and telecommunications made this a more practical arrangement. We can make improvements, such as real-time data replication, as our recovery timeframes continue to shrink and we can frequently test and verify quality assurance.”

The CIO of Excel Bank Minnesota (Minneapolis), Craig Boivin, is also adamant about IT service availability. “Downtime is not acceptable for our most critical applications, such as Internet banking, so we have combined DR with high availability to ensure that if we lose capabilities at our main data center, we automatically fail-over to our alternate site with minimal impact to our customers and employees. In fact, we periodically fail-over our mission-critical applications to our DR site and run the bank from there, and our customers and employees never know.”



Does One Strategy Fit All?

Each bank is unique with different business requirements, capabilities and budgets. The following approach will help you determine the best strategy for your bank:

Step 1 – Define Requirements

- Prioritize your business functions
- Determine which IT services are required
- Determine if manual procedures can be implemented
- Set recovery time objectives (RTOs) for each IT service

Step 2 – Assess Current Strategy and Risks

- What is covered under the current agreement?
- Where will data be recovered?
- Does the DR site have sufficient power, HVAC, space, etc.?
- How will recovery equipment be obtained?
- What about distributed (Intel) systems (e.g. home banking, file server, e-mail)?
- How will the bank connect to the DR site?
- How will people and branches connect?
- What about telephone and Internet services?

Step 3 – Review Alternatives and Conduct Cost / Benefit Analysis

- Outsource to hot-site / warm-site service vendor
- Utilize branch or alternate data center

Step 4 – Implement

Step 5 – Document Recovery Procedures

- Declaration Guidelines
- Roles / Responsibilities
- Communication Plan
- Recovery Sequence and Procedures
- Hardware and Software Configurations
- Critical Vendors

Step 6 – Test, test, test

Senior management should ask the following questions:

1. Worst case, how long would it take for the bank to recover from a disaster?
2. What functionality and IT services would be in place at that time?
3. Has the strategy been proven through sufficient testing?

If you are not comfortable with the answers, it is time to re-assess the recovery strategy.

By: Jeff Olejnik, President
Assurity River Group, Inc.
4500 Park Glen Road, Ste. 120
Minneapolis, MN 55416
952-230-6488
jolejnik@assurityriver.com
www.assurityriver.com