

How to Use This Guide

Protecting customer information during a disaster has historically been a major focus point of financial institutions. Recent disasters have further underscored the importance of protecting information with respect to backup and recovery, as well as security against identity theft. Disasters today sometimes create multiple losses, not only at the moment of the destructive disaster event, but also continuing for weeks after if confidential personal information is stolen.

Your institution may not be located in a flood plane or near a fault line, but keep this in mind: Online systems fail an average of nine times per year, with an average outage duration of four hours per failure. Hardware and software failures still account for nearly 75 percent of all business interruptions and data loss or corruption, despite continuous improvements in computer equipment. While predicting disasters may well be impossible as you develop your plan, the fact remains that disasters of one kind or another do occur with some frequency.

REFLECTIONS ON ONGOING PREPARATION EFFORTS

In 1993, when terrorists attacked the World Trade Center for the first time, financial services company Morgan Stanley learned a life-saving lesson. It took the company 4 hours that day to evacuate its employees, some of whom had to walk down 60 or more flights of stairs to safety. While none of Morgan Stanley's employees were killed in the attack, management decided its disaster plan just wasn't good enough. Morgan Stanley took a close look at its operation, analyzed the potential disaster risk and developed a multi-faceted disaster plan. Perhaps just as importantly, it practiced the plan frequently to provide for employee safety in the event of another disaster.

On September 11, 2001, the planning and practice paid off. Immediately after the first hijacked plane struck One World Trade Center, Morgan Stanley security executives ordered the company's 3,800 employees to evacuate from World Trade Center buildings, two and five. This time, it took them just 45 minutes to get out to safety! The crisis management did not stop at that point, however. Morgan Stanley offered grief counseling to workers and increased its security presence. It also used effective communication strategies to provide timely, appropriate information to management and employees, investors and clients, regulators, and the media. Morgan Stanley still lost 13 people on September 11, but many more could have died if the company had not had a solid disaster plan that was practiced over and over again. In making a commitment to prepare its most valuable asset, its people, Morgan Stanley ensured the firm's future.

Source: Office of Homeland Security

Knowing this should help you to avoid fruitless speculation on future events and to keep focused on developing the best possible disaster recovery program to protect your bank against any eventuality. As

significant emphasis is placed on remote financial services, including electronic banking, the importance of disaster response and timely recovery will continue to grow. Banks must be prepared for any number of threats, including:

- IT system failure
- Flooding
- Tornado
- Hurricane
- Fire
- Earthquake
- Terrorist attack
- Power failure
- Workplace violence
- Pandemic influenza

SMALL FINANCIAL INSTITUTION RECOVERS

The people who work at a small financial institution in Jackson, Tennessee, know what it's like to have their business devastated by Mother Nature. Fortunately, because they had a disaster recovery plan, they also know what it's like to recover. On May 4, 2003, Aeneas was among the more than 400 businesses in Tennessee hit by an F4 tornado, packing winds greater than 200 miles per hour. The tornado resulted in eleven deaths and more than \$50 million in damage throughout the community.

The small community bank had more than \$1 million in damages, including loss of hardware and software, with part of the main office reduced to rubble. "There was nothing left of the second story of our building. Just piles of bricks and concrete. We lost everything upstairs, including our primary servers and telecommunication systems," offered Executive Vice President Handley. "But back-up systems were in place and our employees worked from other locations. And because we were ready, many of our customers were able to conduct financial transactions within a matter of hours."

Less than 72 hours later, the bank was back, fully serving its customers' needs. In fact, many of its smaller business and consumer customers never were delayed or asked to wait. This small community bank was able to protect itself against a worst-case scenario because it had planned for a worst-case scenario. Its business recovery plan was based on the idea that even if its facilities were destroyed and services halted, it would have back-ups in place and ready to go.

Throughout the recovery effort, bank management was careful to keep customers abreast of their progress. The bank also benefited from the quick work and dynamic spirit of its employees and the local community who refused to let a tornado bring down what they had fought so hard to build in the first place.

Source: Office of Homeland Security

To conduct ongoing research for *Banker's Guide to Disaster Recovery Planning*, the authors have surveyed financial institutions across the United States and its territories. The initial survey was conducted in December 2005, and the next was in January 2007; other surveys are planned for the future. The results of the surveys are used to guide the direction this manual takes in focusing on real-world solutions for disaster recovery. A chapter at the beginning of this manual compares and discusses the results of both surveys.

Banker's Guide to Disaster Recovery Planning details how your financial institution can plan for and react to the unexpected events that can have a devastating impact on your bank. Part 1 discusses the reasons for launching a disaster recovery initiative for your bank, reasons which range from the paramount concern of protecting bank employees and customers to the less obvious but important considerations of insurance benefits and regulatory compliance.

Part 1 offers an overview of the disaster recovery planning process, a flowchart of the planning process, and a systematic approach for developing a disaster recovery plan. It includes a set of planning-focused worksheets that will guide you step-by-step as you begin your disaster recovery planning effort.

Part 2 of this guide provides you with a comprehensive model disaster recovery plan, complete with sample policies and procedures, supporting documents, checklists of the tasks to be performed by various individuals and entities during a disaster, and checklists of the regulatory guidelines. This chapter will give you an idea of the scope of a disaster recovery program for a typical community bank. The model plan contained in this chapter is included on the accompanying CD to allow you to conveniently modify the documents in the model to fit your institution's specific needs.

Part 2 also focuses on materials that would be most useful to your disaster recovery teams in the event of a real disaster. The disaster recovery teams are the people who will implement your plan and provide the leadership necessary for a successful recovery. This chapter discusses the training of disaster recovery teams and offers a sample training handbook for distribution to them. The team handbook is also on CD to provide you with an easy-to-use means of customizing the handbook for your bank's disaster recovery teams.

Separate sections highlight considerations for shaping the sample disaster recovery plan offered in this guide to fit your own institution. Other sections address the necessity of testing disaster recovery plans, testing approaches and procedures, and the evaluation of test results.

Regulatory agency examiners place a heavy emphasis on preparedness. The appendixes present the text of various regulatory agencies' issuances concerning contingency planning. These will help you stay apprised of the compliance aspects of disaster recovery planning. If an institution chooses not to address contingency planning, the board of directors and management may face regulatory enforcement action and/or legal liability if a viable disaster recovery/business recovery program is not developed and implemented.

This manual will be updated periodically to bring you current on any regulatory changes pertaining to disaster recovery. It will also be expanded to give you the latest guidance on how to effectively prepare for disasters of all types and how to train your staff and management to reach the highest level of preparedness.

Your institution can gamble on the odds that disaster will never strike and ignore the disaster recovery process, or you can take simple steps to minimize or avoid the catastrophic events that can potentially destroy your organization.