Process Improvement
After The Storm

Recent natural disasters have brought to light the need for mortgage companies to take a hard look at disaster recovery.

By Tony Garritano

On the one year anniversary of Super Storm Sandy, I thought it would be helpful to revisit this disaster to see what we can learn from it. Personally I was without power for seven days. Take my word for it, it wasn't fun. However, we had no major property damage and the lights eventually came back on. Others weren't as lucky.

The Associated Press (AP) reported, "Sandy damaged or destroyed 305,000 housing units and disrupted more than 265,000 businesses in New York. In New Jersey, 346,000 housing units were destroyed or damaged, and 190,000 businesses affected.

"Loss estimates in the affected states vary. Six months after the disaster, leading insurance company Munich Re Ag estimated insured losses at $25 billion and total losses at $50 billion. In December, state governments reported a total of $62 billion in damage and other losses."

What was the human devastation of Sandy? Six months after the storm "at least 3,500 families in New York and New Jersey are still living in hotels and motels on the dime of the Federal Emergency Management Agency," according to AP. "As winter settled in, people who still have homes but no means to heat them have taken refuge in tents set up by aid workers.

"Redrawn federal maps indicating flood-prone areas may force many property owners, especially in New York or New Jersey, to pay exorbitantly for flood insurance, raise their homes or move away altogether. In New Jersey, flood insurance premiums could cost as much as $31,000 a year."

So, how do we prepare for the next storm? In New York, a commission formed to examine ways to guard against future storms has called for flood walls in subways, water pumps at airports and sea barriers along the coast. It's unclear whether enough money can be found for all the expensive recommendations.

Matthew Gerber, CEO at IT-Lifeline, said, "The National Credit Unions Administration just issued its report on Sandy and somebody said there are about 2,000 credit unions that were impacted by Sandy, which is a staggering number. We had customers and heard of others sharing experiences where—in this case, credit unions, but I'm sure it applies to all financial institutions—fell down more often than not in trying to resume operations after something like Sandy came through."

IT-Lifeline is a provider of disaster recovery and compliance testing solutions for the financial services industry. Gerber in particular is a 20-year technology industry veteran with extensive global business development experience. Prior to joining IT-Lifeline, he was President and CEO at SprayCool, a leader in advanced direct liquid cooling for electronics. Before joining SprayCool, he served in various senior executive roles at Itronix, a global leader in the mission critical wireless mobile computing industry. In addition to the IT-Lifeline Board, he currently sits on several company and non-profit Boards.

> Sandy damaged or destroyed **305,000 housing units** and disrupted more than **265,000 businesses in New York.**

"In a lot of cases, there are personnel who were not available during Sandy because some of the IT personnel couldn't get to specific facilities," added Gerber. "However, with rigorous testing, any company can avert disaster. We have a lot of customers who test twice a year so that your recovery capability flexes and accommodates to your new technology. From there you have to document that testing so that if you have different people that come into play that may or may not have experience with certain systems and tech-

nologies, if you've been rigorous about documenting those things, we saw institutions that recovered without any issue whatsoever if they had the rigor around testing and documentation."

"I think there's a continued theme around testing, which applies to everything," added Walt Thomasson, the Managing Director at College Station, Texas-based Rentsys Recovery Services, a provider of disaster recovery services for banks, credit unions, mortgage lenders and other organizations. "That's probably the most critical part of what we do with our customers is to walk them through that testing. But as a technology vendor and a service provider, what we're doing to keep our clients protected is mainly stay ahead of them."

Thomasson has more than 21 years of experience in the information technology industry, and founded the company in 1995 to offer organizations with a complete range of disaster recovery solutions. Since establishing Rentsys Recovery Services, he has led the effort to build the company's three co-location facilities and create the largest fleet of mobile recovery trailers exclusively for the disaster recovery and business continuity market in North America. Prior to that, Thomasson worked at Electronic Data Systems, a multinational information technology equipment and services company, as a systems engineer. Thomasson studied economics at The University of Texas.

He cautioned, "We have to stay ahead of the technology. For example, a lot of our customers are moving from the hardened desktop, to a virtual desktop environment. Or they are certainly evaluating it. And they're never, well they're rarely looking at it from a disaster recovery perspective. They are looking at it from a day-to-day production value. We have to go in and look at each of these new developments from a disaster recovery and business continuity perspective, and make sure that we're educating them in advance of their investments."

Natural disasters aside, we also have to beware of criminals that want to hack our industry over the Internet. The frequency of online attacks against U.S. business continues to increase, along with the cost of defending against those attacks and mitigating any resulting data breaches. "Cybercrime now costs a U.S. business $8.9 million per year, an increase of 6% from 2011 and 38% from 2010," added Mike Bridges, President of electronic collaboration vendor PaperClip. "Those findings come from the "2012 Cost of Cyber Crime Study," which was sponsored by security intelligence tool vendor HP and released Monday (10/8/2012) by Ponemom Institute. The businesses profiled in the study also reported that on average, they're collectively seeing 102 successful attacks per week, up 72 attacks per week in 2011 and 50 attacks per week in 2010.

Cybercrime now costs a U.S. business $8.9 million per year, an increase of 6% from 2011 and 38% from 2010.

"The average breach costs $214 per record compromised; another cost factor is that it's taking businesses longer to respond to security breaches. On average, it now takes a business 24 days to spot and resolve an attack, although some cleanup operations extended to 40 days. On average, each cleanup cost $592,000, a 42% increase from the average reported in 2011 of $416,000. (Ponemon Institute and Hewlett Packard- 2013)."

So how does the mortgage industry prepare for these types of disasters no matter if they're caused by nature or criminals? "Simply put, cyber security begins with a plan," concludes Mike Bridges. So, I ask you: Do you have a plan? ❖

Tony Garritano is Chairman and Founder of PROGRESS in Lending. As a speaker Tony has worked hard to inform executives about how technology should be a tool used to further business objectives. For over 10 years he has worked as a journalist, researcher and speaker. He can be reached via e-mail at tony@progressinlending.com.