PARTNER'S GUIDE TO THE

Worst Data Disasters of 2013

SHUTTERSTOCK

Data points for your 2014 discussions with customers about modernizing, bulletproofing or—gasp—actually creating a business continuity and disaster recovery plan.

By Scott Bekker

The year 2013 wasn't that unlucky when it came to data disasters in the United States. Nevertheless, the year had plenty of other disasters and incidents that should give you serious pause if you're charged with data recovery and business continuity.

Here are eight of the biggest disasters with important implications for business continuity and disaster recovery plans:

Super Typhoon Haiyan: Just when it seemed the world had made it through the year without a serious hurricane or tropical cyclone, one of the worst in the history of the satellite era reared its head.

Seasonal hurricane outlooks for the Atlantic hurricane season called for above-average activity this year. The U.S. National Oceanic and Atmospheric Administration projected there would likely be between 13 and 20 named storms, with seven to 11 of them reaching hurricane status and three or four becoming major hurricanes (Category 3 and above). By mid-November, though, there had been just 12 named storms in the Atlantic. Only two were hurricanes and none were major.

"While pre-season outlooks rarely, if ever, have pinpoint accuracy, they don't usually miss by such a large margin," wrote Andrew Freedman of the "Climate Central" Web site in mid-October.

And it wasn't just slow in the Atlantic, either. Across the globe, it was shaping up to be one of the slowest years on record for hurricanes and tropical cyclones.

Then came Typhoon Haiyan—a freakishly well-formed cyclone that made landfall in the Philippines on Nov. 8 and struck Vietnam on Nov. 11. According to a Weather Channel report, "With sustained winds at 195 mph and gusting to 235 mph, the storm was the strongest tropical cyclone on record to ever make landfall and the fourth-strongest tropical cyclone in world history. The previous record was held by the Atlantic's Hurricane Camille of 1969, which made landfall in Mississippi with 190-mph winds."

Rescue efforts and damage assessments from Haiyan, which had an estimated storm surge of 25 to 30 feet, were still being conducted at press time. The storm's toll already was horrific, with Philippine authorities estimating as many as 10,000 people may have died.

For U.S.-based companies, Haiyan serves as a reminder that hurricanes can develop very late in the year and, despite a so-called "drought" of eight years since a Category 3 or higher hurricane made landfall in the

United States, it's only a matter of time for coastal areas before the next major storm arrives.

Superstorm Sandy: The relatively late emergence of Super Typhoon Haiyan recalls the appearance last year of Superstorm Sandy. That storm hit the Northeastern United States and disrupted everything from power grids to the shape of the coastline to the U.S. presidential elections.

In fact, the storm spawned a reassessment of the hurricane classification system used for the last 40 years. While Sandy briefly reached Category 3 on the Saffir-Simpson scale, it only rated a Category 1 on the scale at landfall. The sustained severity of the storm prompted researchers at Florida State University to propose a new, complementary metric called Track Integrated Kinetic Energy (TIKE) to better communicate the destructive power of certain storms.

Although the storm occurred in 2012, its effects lasted well into 2013. A list of major disaster declarations for the year on the U.S. Federal Emergency Management Agency (FEMA) site includes two Sandy-related declarations in January 2013, more than two months after the storm made landfall. The length of power outages and other infrastructure disruptions caused by Sandy threw significant new wrinkles into a lot of disaster recovery plans. The storm also drew attention to previously unrecognized fragility in U.S. power and communications infrastructure.

Fukushima: The failure at the Japanese Fukushima Nuclear Power Plant in March 2011—caused by the massive tsunami—continued to wreak havoc in 2013. Fukushima is the only event other than Chernobyl to rate a seven (the worst rating) on the International Nuclear Event Scale. Three Mile Island in the United States was a five. Estimates for the amount of radiation released at Fukushima, however, are about 10 percent of Chernobyl.

The 20-km exclusion zone around Fukushima remains in effect more than two and a half years after the incident. Meanwhile, during the summer of 2013, reports surfaced that the plant was continuing to release radioactive water into the Pacific Ocean and a storage tank had leaked 300 metric tons of heavily contaminated water.

Around the time of the original Fukushima incident, as concern about proximity to nuclear power plants spiked, CNN posted a tool for using a zip code to calculate the nearest nuclear power plant in the United States. The tool is at http://tinyurl.com/laj838v.

According to CNN, "In a 10-mile radius, the Nuclear Regulatory Commission says the air could be unsafe to breathe in the event of a major catastrophe. Within 50 miles, food and water supplies may be unsafe."

In any case, any complete disaster recovery plan should account for proximity to nuclear sites, even though the ability to plan for such an unlikely event as a nuclear power plant accident and indefinite evacuation is beyond the scope of most local business disaster recovery contingencies.

SHUTTERSTOCK

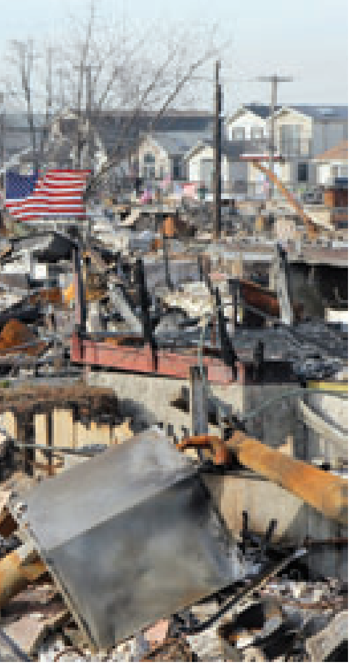
Superstorm Sandy spawned a reassessment of the hurricane classification system used for the last 40 years.

Colorado Flooding: Water-based disasters aren't limited to coastal areas. Just ask the residents of central Colorado. Epic rainstorms in September led to a 100-year flood. The floodwaters covered a 17-county area along and downstream of the Front Range. Storms the week of Sept. 9 brought rainfall of up to 17 inches.

In Boulder County, the rainfall for the week was equivalent to a full-year's average annual precipitation. While early reports had hundreds of people unaccounted for, as the storm-generated confusion abated and communications returned to cut-off areas, the flooding ended up causing about eight deaths.

Infrastructure damage was immense. Water overtopped earthen dams, washed out 200 miles of roads and destroyed or damaged at least 50 bridges. The flood also closed down 1,900 oil and gas wells in flooded areas until they could be checked by industry personnel.

Oklahoma Tornado: On May 20, a powerful tornado cut a path nearly a mile wide across the greater Oklahoma City area, including the town of Moore. Dozens of people were killed. While that is indeed tragic, it's immediately apparent



from aerial photos of the 1,000 buildings destroyed and 1,200 or so other buildings damaged that the National Weather Service and local newscasters and authorities did an incredible job of warning people to get to safety.

Among those destroyed and damaged buildings were many businesses that would have needed to have disaster recovery plans to get their data back from ruined servers. Like the Joplin, Mo., tornado two years before, the Oklahoma tornado serves as a powerful warning to anyone in Tornado Alley and many other places in the United States of the danger.

Edward Snowden: Can a person rightly be called a data disaster? From the U.S. National Security Agency's (NSA) perspective, former contractor Edward Snowden definitely qualifies. There's robust debate about whether Snowden's revelations about the U.S. government's electronic snooping capabilities and practices make him a hero or a villain.

Whatever your feelings, Snowden's action are a reminder of how much damage a disgruntled employee, or even a partner's employee, can do to your company's efforts to protect its intellectual property, confidential communications and other data.

The Snowden revelations fall under a broader discussion of business continuity and disaster recovery than the usual technical questions. Planning for physical disasters requires conversations about technical topics, like whether a backup datacenter is far enough away to be outside the scope of a localized incident or how quickly replacement servers can be spun back up with replicated data.

The disgruntled-employee question requires a broader view that encompasses other types of disasters that can befall your organization's data. Sometimes organizations consider those questions under their security strategy. However, they're all related and forward-thinking organizations consider the disgruntled-employee or partner issue under the same umbrella that includes data recovery.

Government Attackers: This year has been an eye-opener with respect to digital attacks. The year started with a February report by security firm Mandiant alleging that a cyberunit of China's People's Liberation Army was systematically attacking U.S.-based companies to steal trade secrets and obtain other proprietary data.

According to a detailed article previewing the report in *The New York Times* in February, "While [the cyberunit] has drained terabytes of data from companies like Coca-Cola, increasingly its focus is on companies involved in the critical infrastructure of the United States — its electrical power grid, gas lines and waterworks. According to the security researchers, one target was a company with remote access to more than 60 percent of oil and gas pipelines in North America. The unit was also among those that attacked the computer security firm RSA, whose computer codes protect confidential corporate and government databases."

Although Chinese officials denied everything, the allegations drew condemnation from the United States government and U.S. companies. A few months later, however, the revelations were overshadowed by Snowden's leaks through U.K.-based *Guardian* and the *Washington Post*. Snowden released slide decks and other classified documents about secret NSA programs to tap the servers of major U.S.-based cloud providers, among other wide-ranging electronic data collection techniques.

The very public revelation confirmed what many had suspected. The world's biggest government intelligence agencies were after all the data they could get their hands on, and they were quite good at doing so. This adds several new twists to data protection that should be included in any full data protection review.

Island Outage: A major storm isn't the only thing that can cut off Internet communications for extended periods of time, especially for an island. Witness the San Juan County's late-2013 state of emergency. The islands that make up the county northwest of Seattle had their underwater fiber-optic cable severed in early November.

Data and phone service went out for 15,000 people, who mostly all found out at once how much of a problem it is to have almost all of your infrastructural links to the outside world coming in through one cable.

According to a report in *The Seattle Times* about a week after the cable was cut, "The outage has hit the area's economy hard. Some banks have had to close or restrict transactions because data lines cannot connect to the mainland. Difficulty processing credit-card transactions has forced many businesses to accept only cash."

The incident serves as a reminder that disaster recovery plans must account for the limitations of local Internet infrastructure, limitations that can be difficult to determine without the expertise of an experienced disaster recovery/business continuity partner. •

Scott Bekker is editor in chief of Redmond Channel Partner magazine.

Go from complete disaster to complete recovery in less than 5 minutes.

STORAGECRAFT.

RECOVER-ABILITY™ SOLUTION

Introducing the award-winning, #1 disaster recovery solution for physical and virtual environments.

The StorageCraft® Recover-Ability™ solution is a suite of software and services that helps you recover anytime, anywhere, from any disaster. It works as an integral part of your overall business continuity plan by protecting your systems, applications, and data from any disaster, large or small. Here's how…

Backup: Creates a copy of everything – systems, apps, data, services.

Replicate: Duplicates your backups to another location.

Manage: Ensures your backups will work when you need them.

Recover: Gets your business running again immediately following a disaster.

Download our FREE Recover-Ability Guide Ebook, ***"Making Disaster Recovery Easy"*** at **www.StorageCraft.com/EbookRCP**. No registration required.

TechEd

WindowsITPro

Windows IT Pro ★★★★★

Redmond MVP Most Valuable Product

Microsoft Partner
Gold Application Development

STORAGECRAFT®
Backup Fast, Recover Faster