AFTER THE STORM

One year on from Sandy, *HFMWeek* provides an update on business continuity planning and disaster recovery issues and examines what has changed since the superstorm struck

BY WILL WAINEWRIGHT

▲ THE REMAINS OF PART OF THE BOARDWALK IN THE ROCKAWAYS ON 2 JANUARY 2013 IN THE QUEENS BOROUGH OF NEW YORK CITY

It was, in the words of one former hedge fund CTO, the sector's biggest business continuity test since 9/11. When Superstorm Sandy hit the US eastern seaboard a year ago, the tri-state area – which doubles as the hedge fund industry's global capital – was braced for impact.

Unlike Irene the previous year, Sandy was as serious as feared and knocked out power and communications in much of Manhattan and the surrounding region for almost a week. Hedge funds located downtown, such as Leon Cooperman's Omega Advisors and Hagin Investment Management, faced an immense challenge to restore a normal working environment, while the majority of the region's hedge fund managers faced disruption of some kind.

The storm's impact has led hedge funds to fundamentally reassess their capability to function during such extreme unexpected events, according to industry veteran Jerry Levine. "It may have been a historic event but anything that has happened a year ago you just assume is going to happen again," says Levine, who previously held senior technology positions at top-tier hedge funds including Millennium Partners, AQR Capital Management and Soros Fund Management.

EYE OF THE STORM

"Sandy really opened our eyes to the magnitude of potential problems a hedge fund can face," says Aaron Chan, CFO at New York-based Act II Capital. "One of the things Sandy taught us was about power: we had never seen such a wide-scale power disruption. We have totally reviewed our practices in this area and developed back-up options."

Act II is one of several hedge funds that told *HFMWeek* they had fundamentally reviewed their disaster recovery (DR) and business continuity planning (BCP) in the year since the storm. "Disaster recovery is about ensuring you have access to the data and technology you need to operate your business," explains Bob Guilbert, managing director at Eze Castle Integration. "Business continuity planning is more about the people and processes required to run your business, and how they can best be organized to operate if an unexpected event occurs. Sandy highlighted the importance of both."

Fortress Investment Group, headquartered in Mid-

town Manhattan, did not lose use of its office during Sandy, but the storm's impact on the region's infrastructure prevented some employees getting to work. "We have a significant remote computing infrastructure that enables our entire staff to work remotely when necessary," explains Brian Piscopo, CTO of its liquid markets business. "This was an important option for employees who were unable to reach the office due to storm-related logistical factors."

Fortress's experience was shared by many of their hedge fund peers, whose biggest challenges were more frequently personnel-based rather than technology and systems. With the majority of Manhattan funds situated in Midtown above the power-cut line, on-site servers meant it was business as usual – except for employees stranded in outlying areas by infrastructure problems. One technology provider notes that many of the block-booked hotel suites and hot-seat working space booked by clients went unused as employees preferred to work from home and be with their families, meaning some firms may rethink spending money on such contingencies.

Accessing data was a problem, however, for those hedge funds forced to rely on datacentres that failed during Sandy. The storm exposed flaws with centres located in lower Manhattan, some of which were flooded and had to rely on generator power, with mixed results, while several in surrounding areas also struggled. Few, if any, hedge funds were unlucky enough to be situated in a power outage zone and see their offsite back-up fail, which would have technologically wiped them out entirely.

However, the sheer size of the affected region has led hedge funds to consider their back-ups. "Some of the bigger funds may now consider two offsite datacentres rather than one, in particular those who had datacentres located in downtown New York will definitely consider moving it away from the city," adds Levine. "Clients need datacentres in geographically dispersed locations," says Jason Elmer of cloud provider Abacus Group, which in common with many specialist IT firms has sites located on both coasts of the US. He describes Sandy as a "make-or-break moment" for offsite providers.

PRESSURE ON PROVIDERS

A range of sources told *HFMWeek* how CTOs and other hedge fund tech personnel spent the weeks and months after Sandy comparing experiences. Crucially, this often boiled down to which providers passed the test and which did not. "Our clients and potential clients ask about this a lot more now, and in particular how we coped during Sandy," says Bruce Cooper, CTO at technology provider Liquid Holdings, which experienced no trading downtime. "It is yet another reason not to be in Manhattan for your main tech systems."

Ray Bricknell, the former CTO at RAB Capital in London, agrees that hedge funds now put much more thought into which outsourcing providers they employ. "A lot of this is investor-driven," says Bricknell, who now runs IT consulting firm Behind Every Cloud in London. "Institutional investors continue to pay a great deal of attention to a fund's internal BC and DR plans, but are now taking a far greater interest in the operational risks presented by the fund's IT counterparties. This has forced funds to respond."

Deborah Prutzman, who runs industry consulting firm the Regulatory Fundamentals Group, agrees that the core BC/DR issues highlighted by Sandy now have a more prominent role in the due diligence check lists of institutional investors. She says example questions include: "What happens if senior decision makers cannot be reached? Do enough people have the discretion to trigger the use of the procedures? What if staff cannot make it into backup sites?

"Investors are asking these types of questions and managers, by necessity and in their own self-interest, are now focusing on the appropriate procedures to take," adds Prutzman, whose experience in the realm extends back to being the most senior officer at data firm Dun & Bradstreet present during the 9/11 attacks. "Certainly at the more sophisticated institutions more time and money is being spent on this topic."

REACHING FOR THE CLOUD

The industry's extensive examination of BCP and DR procedures in the wake of Sandy has coincided with the industry's increasing uptake of cloud computing services, and funds, including Act II, have increased their usage in the 12 months since. "We now do more of our work in the cloud but we realise this is solution does not cover all potential problems," says Chan. Levine agrees that the development of the cloud will not impact BCP and DR plans as much as other factors. "The cloud in theory removes the need for onsite servers, but only a very small handful of hedge funds operate solely in the cloud."

But Bricknell cautions that cloud vendors, in particular, are being asked how well they can cope when unexpected events strike. "A key advantage of the cloud is the ability to access data remotely, but that becomes redundant if it relies on one centre in an at-risk area like Lower Manhattan," he points out, adding he has been surprised there has not been more conversation among London hedge fund COOs about potential UK disasters. "With the whole London finance market centred around the Thames, one has to wonder what would happen if the city was hit by a once-in-a-century flood or other weather event."

Chastened by Sandy, New York's hedge fund sector will hope it is not its turn again soon, but with instances of such landmark weather events seemingly increasing, it will at least have its defences prepared. ■

REGULATORY REVIEW

In the year since Sandy, financial regulators in the US have taken a keener interest in how firms prepare for unexpected events. On 16 August the SEC, CFTC and Finra released a joint review of business continuity and disaster recovery planning and called on financial firms to review their procedures. "With hurricane season underway, and with the problems from last year fresh in mind, we trust that our member firms will review their business continuity planning procedures against these best practices," said Finra's executive vice-president Grace Vogel.

Based on testimony gathered from 40 firms, the review suggested effective practices in six areas: preparation for widespread disruption; planning for alternative locations; telecommunications services and technology; communication plans; regulatory and compliance considerations; reviewing and testing.

This has led to physical change, with the National Futures Association (NFA) amending its compliance rules as a consequence. The NFA previously required emergency contact for two key individuals in the event of disasters or unexpected events, but now demands contact details of all key management personnel plus details about its disaster recovery site.

The SEC followed the joint review with a 'risk alert' issued on the 27 August that focused on investment managers. The report found that "some advisers adopted BCPs that did not adequately address and anticipate widespread events" and identified a series of weaknesses. These included key personnel, such as portfolio managers, being unable to work remotely and the failure of some advisers to evaluate the BCPs of their service providers.