

[Homepage](#)[News](#)[Features & Contents](#)[Industry Comment](#)[Research](#)[From the Editor](#)[Events](#)[Forthcoming Features](#)[Links](#)[Subscriptions](#)[Bookstore](#)[Magazine Information](#)[Magazine Registration](#)[Advertising Information](#)[Enewsletter](#)[Contact](#)[Privacy Policy](#)[Terms & Conditions](#)

In partnership with:



Data evacuation - hurricanes revealed the networks weakest link

Ed Walsh, CEO, Avamar

A recent *Washington Post* report discussed the relief of a New Orleans' school manager upon finding that 170 computer backup tapes storing critical financial information were dry and apparently undamaged in spite of flooding. This and similar stories in the wake of this year's hurricane disasters in the United States are a stark reminder of how vulnerable business data can be. It has become clear that most companies' disaster recovery plans are only as good as the last interruption they experienced. It is likely we will see increases in natural and manmade disasters as well as data theft in the coming years and businesses need to be prepared to preserve and retrieve their mission-critical data.

Most companies have either no plan at all or they rely on tape-only backup. Traditional technologies such as tape serve a purpose but may not always be reliable and readily available to avoid business interruption. It's true tape can't be hacked remotely, but according to one recent survey of over 150 IT security professionals, as a storage method it fails over 30% of the time. Enterprise Strategy Group reports that only seven per cent of businesses encrypt all of their backup tapes, leaving them vulnerable. Also, getting tape offsite and then retrieving it requires clear roadways and secure trucks. As we've seen from the recent hurricanes and cases of tape theft, these factors are not givens.

In an ideal world, systems would be designed from square one with compliance in mind, with an aim to significantly reduce the legal risk of not complying with data storage regulations, requiring multi-year online archives of data to enable on-demand restoration of necessary data. Such a design would ultimately serve disaster recovery well without the need for an additional plan. But the legacy nature of networks means that businesses must first consider the need to make back-up and restore central to their business continuity and disaster recovery plans.

Backing up data to media that only remains on site at the businesses' primary location is no longer an option. Even those businesses which utilize the benefits of urban Ethernet networks to back up data within the city limits should heed the warning of recent hurricanes. By not considering off-site storage, either online or at a facility in another area, some companies' best-laid plans were rendered useless.

By consequence, making the choice to store data off-site also necessitates that businesses make a shift from what they are used to, moving the media, to the safer and more efficient solution of moving the data. New off-site disk-based data protection technology backs up efficiently over the Internet, enabling the transfer of data by secure VPN connection to a safe location. Such systems also allow companies to ensure that even those smaller sites, separate yet tied to the main office, can be included in regular back-up procedures. The location of the data is no longer the

INFOSECURITY
Register today for your
free subscription

INFOSECURITY
Free enews service
Sign up now!

issue; what is important is how efficiently it can be moved.

Indeed, the ability to expedite the process of back-up and restore is key to any successful business continuity/disaster recovery strategy. Moving data quickly means that back-up solutions must optimize bandwidth. The best way to move network data quickly is to simply move less data. How can this be done? Through intelligent disk-based storage systems that don't have to read the entire network every time a back-up is under taken. Such systems only have to add the changes made to files already stored. This can result in a 100-1 reduction in back-up data required, which means a back-up process that could typically take 1-2 days using tape can take as little as 1-2 hours, while also retaining 100% data integrity.

With other media subject to such high failure rates, these time savings can mean the difference between data being saved or lost. In the face of impending disaster, the ability to back-up in a timely manner frees up valuable human resources to focus on other areas of a business continuity plan. Time is also saved in the actual recovery process. The simple fact is that tape does not have random access memory whereas disk-based storage can enable a network to be rebuilt almost as quickly as it took to store.

Recent world events have made it clear that most companies need to revisit their data protection strategies. Solutions that focus on moving the data instead of the media offer a much higher incidence of backing up data quickly in an emergency as well as efficient and complete retrieval of that data. Worrying about the condition and location of hard copies can be a thing of the past, right now.

www.avamar.com