Tech Trends
How Much Data Can Your Agency Afford to Lose?
Study shows 93% of small businesses that have major data losses are out of business in five years. Plan now for the worst case scenario.

Imagine your worst nightmare. A server overheats, starting a fire that consumes your computer room before the sprinkler system kicks in and completes the disaster process. You've lost facilities, hardware, network and data. Now what?

There are four primary assets needed to effectively operate an information system – facilities, hardware, network and data. In the unfortunate event of a disaster, hardware and networks can be replaced, and facilities can be moved to a new location. In fact, with the exception of data, virtually every company asset can be replaced. Therefore, your top priority should be to protect the asset that's most at risk and hardest to replace: your data.

Businesses need to strike a balance between the level of business risk they can tolerate and the cost of perfect security. Initially, all businesses would say they can't afford to lose any data and they can't tolerate any downtime. But protection on that scale is probably cost-prohibitive and overzealous. It's unlikely that all applications are equally mission-critical and all systems are equally vital.

Gartner Group research found that 93% of organizations that have experienced a significant data loss are out of business within five years.
Businesses should look for a solution that incorporates the following four components:

Requirement #1: Continuous Backup
Only half of U.S. businesses perform data backup, and surveys find these businesses do not always do an adequate job. Because some agencies have limited or no IT staff, they perform bulk server backup sporadically, use traditional tape for backup and typically perform the task after business has closed for the day. That means to restore data, companies can only expect to recover from the previous night. How can you eliminate this window of vulnerability? Ask your provider for continuous backup that allows data to be captured as it is changed – essentially in real-time.

Requirement #2: Automatic Off-site Storage
Even if your business is rigorous about backup, are you equally rigorous about ensuring that the tape is safely stored offsite? Look for a service that provides safe and accessible data-vaulting, and transmits the data via the Internet, so physical damage to tapes or theft of tapes is avoided entirely and the data is immediately available for system recovery.

Requirement #3: Immediate Recovery
Recovery is the process of restoring operations and specifically, data, after an outage or disaster. It's an obvious point, but often overlooked: being able to immediately recover data is critical to ensuring business continuity. Online services provide a means of recovering data immediately from any Web interface. Look for a service that offers this level of convenience and control.

Requirement #4: The Guarantee
Backup and recovery software vendors will have RTO and RPO ranges within their service level agreements, but none will provide an absolute guarantee because there are too many elements outside of their control, like tape quality or the ability of the internal IT staff. Online backup and recovery services, however, are able to provide the luxury of a guarantee because the entire process is managed by experts at the service provider, and the technical components of the service are fully automated. When evaluating any backup and recovery solution provider, make sure to ask if it guarantees the recovery, rather than just

the backup, of data.

Establishing business continuity metrics such as RTO and RPO is critical in business continuity planning. Devoting attention to RTO and RPO is the only way to guarantee your agency will still be able to operate in the event of a disaster. After all, when it comes to disaster recovery planning, do you want your business up and running quickly, but operating with data that's a week or even a day old?

Bob Chaput (rchaput@amtechgroup.com) is president of American Technology Group, Inc., a disaster recovery and data protection services firm. To read the entire article, go to: http://www.iiaba.net/VU/Lib/Tec/TI/Security/ChaputDataLoss.htm. If you do not know your Big "I" website user name and password, email logon@iiaba.net to request your login.

http://www.iamagazine.com/NewsViews/2011/February_24/Tech-Trends.aspx