Realities of Post-Disaster Data Recovery

Posted @ 1/22/2014 12:21 PM by Cal Beyer and Brian Cooney | Files in **Business,Tech**

The construction industry's dependence on information technology (IT) systems continues to expand with the dramatic shift from document management to data management. With this reliance comes an increased vulnerability to business disruption.

Data management today requires an enterprise view integrating a company's increasingly complex and interconnected networks. Data must be construed to encompass all information generated, received, transmitted, stored and retrieved throughout the organization. Additionally, data must be incorporated from its various physical and virtual locations, including mobile devices.

Following are IT trends impacting AEC companies:

- expansion of email as the predominant form of intra- and inter-company communication;
- growth of online data mobility project management tools using smartphones and tablets to access and transmit data;
- increased adoption of document imaging to replace paper recordkeeping files;
- growth of enterprise resource planning (ERP) platform systems and the integration with best-in-class specialty software programs;
- estimators' use of the same database to work from multiple locations on complex projects;
- increased adoption of, and massive data files generated by, BIM;
- emergence of hosted and cloud-based data recovery systems;
- expansion of e-discovery in litigation, which raises expectations for (and increases the risks of) record retention; and
- proliferation of social media networks combined with bring your own device policies, which creates new portals for hacking, malware and viruses.

The Need for a Comprehensive Business Continuity Strategy

The severity of natural disasters and the escalating number of man-made emergencies and technological disruptions compounds the construction industry's dependence on IT systems. Many of these disruptions "only" result in temporary IT system shutdowns, while others pose a threat to the viability of the business.

A company's vulnerability to data loss can be increased or decreased by the actions taken (or not taken) with regard to data backup and recovery. A robust business continuity plan is the first step. Companies have many choices when selecting the best way to back up their vital information and mission-critical data.

Automatic offsite (hosted or cloud-based) data backup protocols at regular intervals are the best prevention for data loss. These backups must be set for every type of data and for every type of device accessing, transmitting or storing information.

Another data recovery strategy is imaging the company's server and running the restored replica image from a new server in a remote location. However, this strategy requires pre-planning. In a large-scale disaster, obtaining replacement servers may not
be possible.

Causes, Costs and Consequences of Data Loss

Data disruption is a reality of the modern work environment. Causes of data loss include:

- failure to initiate or maintain regular data backups;
- hardware failure;
- human error resulting in accidental deletion, over-writing of data or forgetting to add new IT systems/devices to backup protocols;
- failure to test the backup and data recovery restoration process to determine adequacy;
- software or application corruption;
- power surges, brownouts and outages;
- computer viruses, malware or hacking;
- theft of IT equipment; and
- hardware damage or destruction from vandalism, fire and water (rain, flood or sprinkler system discharge).

The consequences of lost data include direct loss of revenue from missing bid submissions or customer orders, direct expenses to pay for technical specialists to help recover data, decreased productivity during the shutdown and costs to rekey or obtain replacement data. For contractors selling directly to consumers, the loss of Internet connectivity for any extended time could prove costly. Lost data also can result in litigation for breach of confidential information and adverse publicity affecting the company's reputation.

A 2012 study commissioned by cloud-based data backup company Carbonite revealed 45 percent of small businesses (defined as fewer than 1,000 employees) had suffered a data loss. Fifty-four percent of the data losses were attributed to hardware failure and the average cost for data recovery was $9,000.

Best Practices for Data Management

Data management and IT network administration is a strategic, unique function for all companies. It is not possible to delineate all data management best practices, but the following guidelines should help enhance most companies' post-disaster data recovery efforts.

- **Determine the company's recovery time objectives and plan and budget accordingly.** Identify which functions and systems must remain operational at the time of a disruption or disaster. This requires advance planning and budgeting for necessary systems and technical support services. It also helps prioritize risk reduction strategies, including investments in data management backup system and security upgrades.
- **Develop a written business continuity plan that outlines specific responsibilities for protecting vital information and mission-critical data.** The business continuity plan should include protocols for backup and synchronization of all office systems and virtual/mobile devices. It also should address the frequency and format for testing data management integrity and security, as well as how gaps will be identified and addressed.
- **Inventory the company's vital information and mission-critical data and verify it is being backed up.** Key considerations include how the data is being backed up, by whom and how frequently, as well as where the backup data is stored. It is important to ensure the data backup and restoration process work as designed.
- **Initiate automatic scheduled backups, ensure the backup data is stored offsite, and test the adequacy of the data backup and restoration methods.** Consider the added benefits of imaging the company's servers to achieve a complete restoration of the data management system.
- **Develop a comprehensive diagram of the company's integrated data management network, including all physical and virtual/mobile subsystems. I**deally, this will be an "as built" blueprint of the company's configuration consisting of the hardware, operating systems, software and applications comprising the data management network.
- **Institute policies regarding the use of the company's Internet, including security protocols.** Implement policies for user authentication, password verification, unacceptable personal devices and reporting of lost

equipment. It is essential to communicate these policies and security protocols to all users and to train new employees when they are hired.

- **Establish proactive management of the company's data and IT network.** Ensure the company's network administrator has state-of-the-art tools, including remote access, help desk diagnostics, and anti-spam and malware protection. Request periodic updates on all software licensing audits and verification that all security patch updates have been installed on a timely basis. Establish a fixed replacement schedule for hardware and software.

There is good news and bad news regarding business data management and recovery. The bad news is the need for post-disaster data recovery can no longer be ignored. The increasingly complex and connected business world demands pre-planning for business continuity. The good news is data management and recovery services are scalable to meet the custom needs of every business regardless of the size and scope of the operation and its degree of data dependence.

Data management, business continuity and post-disaster data recovery requires a shift in mindset from firefighting to fire prevention. Zero disruptions is a bold strategic imperative that provides a competitive advantage by enhancing field productivity, increasing office efficiency, reducing downtime and preventing data losses. Effective data backup and post-disaster recovery protocols are the essential steps to minimize business disruptions.

Real-World Data Loss Scenarios

- **Laptop motherboard failure.** A project estimator was working offline when the motherboard crashed. Due to a tight deadline, he had to restart the estimate from scratch. Although the bid was successfully submitted on time, the estimator fell behind on pricing other jobs that the company failed to win.
- **Lost iPhone.** Pictures of a project safety incident with documentation of a mismarked "one-call system" utility spot were lost. The photo documentation had not been transmitted to the office and the contractor lost the request for damages against the utility locating service. Moreover, the smartphone was not properly password secured, allowing unauthorized access to contacts, client information and company data.
- **Desktop computer backup location not properly mapped to server.** When a workstation was upgraded with a new desktop computer, it was not mapped to the server for automatic backup. The computer hard drive crashed and no files were backed up. Recovery using the old desktop computer was slow and data created on the new computer was lost.
- **New database not added to the nightly backup protocol.** A company purchased a new customer relationship management database and, after a power outage, realized it had not been added to the nightly data backup protocol.
- **Onsite data backup location destroyed.** The building housing an onsite backup server was struck by lightning, which started a fire and resulted in a total loss of all current and historical data.
- **Disaster recovery software not properly configured.** While conducting a test of a company's disaster recovery plan, it was discovered that some critical data was not being captured in the backup files.
- **Laptop and tablet stolen from a jobsite trailer.** The field equipment had not been backed up for several weeks, resulting in the loss of key project documentation.

Cal Beyer is vice president of construction large account sales and development for Murray Securus, Lancaster, Pa. For more information, call (717) 358-2763 or email cbeyer@murrayins.com. Brian Cooney is executive vice president of finance and administration of Barriere Construction, Metairie, La. For more information, call (504) 569-3141 or email brianc@barriere.com.