



Business Continuity

"External Intrusion"

The Boston Globe recently managed to expose as many as 240,000 subscribers to identity theft –no hackers or viruses required. Here's how: The Globe shares a computer system with a sister newspaper, the Telegram & Gazette, in suburban Worcester, Mass. On Jan.29, 2006, the Telegram & Gazette sent 9,000 bundles of Sunday papers to retailers and delivery people wrapped in recycled office paper happened to be printouts that included subscriber's credit card numbers and checking account information.

Is that a creative way of violating customer privacy or what?

The Globe/Telegram & Gazette snafu followed two incidents in which other companies customer information was stolen from employees' cars. A thief broke into a car in a suburb of Portland, Ore., and stole backup disks containing information on 365,000 patients of providence Health System, a West Coast medical group. Another smash-and-grab thief stole a laptop belonging to an employee of Ameriprise Financial that contained unencrypted data on 158,000 customers.

Here's the scary part: In each case except the Ameriprise incident, the information was handled according to standard operating procedures. The recycling was approved. The home-stored backups were SOP. Even the Ameriprise employee was allowed to have the data on a laptop as long as it was encrypted, but the employee failed to follow encryption procedures and was fired for it.

Well, threats like these are real. However data which contributes to nearly 80% of most business are often neglected even with such great importance. In order to protect information, it is wise to encrypt and back up these sensitive data. Accessing such data can only be done by knowing the encryption algorithm and the specific decryption key being used. The access to the decryption keys could be limited to certain users.

REDiSAFE provides a token system that allows backing up of data and encryption to these sensitive data. The token will give access to retrieving encrypted data that were backed up on the REDiSAFE server, and further, different users could be given different access rights. Specifically, it is preferred to use a so-called granular security solution for the encryption of data, instead of building walls around servers or hard drives.

In such a solution, which is described in this paper, a protective layer of encryption is provided around specific sensitive data-items or objects. This prevents outside attacks as well as infiltration from within the server itself.

Encryption of whole files, tables or databases is not so granular, and does thus encrypt even non-sensitive data. With REDiSAFE, intruders are prevented from gaining full access to any database stored as well as ensuring that your data are kept protected and safe.

