

Backup Files Put Database Information at Risk

<http://www.darkreading.com/database-security/167901020/security/storage-security/229300828/backup-files-put-database-information-at-risk.html>

March 10, 2011 02:59 PM

By Ericka Chickowski, Contributing Writer

Cord Blood Registry breach a cautionary tale in the need for encryption, key management, and secure physical transport of database back-up media

No matter how many safeguards organizations install to protect their production databases, all that work could be for naught if they aren't layering security into their back-up processes. The potential fallout from such a misstep was illustrated vividly in the recent Cord Blood Registry, which suffered a large-scale data breach when it exposed more than 300,000 records after an unencrypted back-up tape was taken from an employee's car.

According to Diana Kelly, analyst for Security Curve, this kind of breach is caused by a common out-of-sight, out-of-mind mentality that frequently plagues companies today. "Production data is, well, in production, so orgs have -- or should have -- that data in the active protection zone," she says. "But once it's backed up, it's easier to forget about."

Kelly explains that step No. 1 to keep this database information secure is implementing strong encryption practices and key management. J. Wolfgang Goerlich, a network security manager at a financial services firm, concurs. He says the risk of misplaced backup information is at the top of his list of worries.

"Encryption is the No. 1 control to prevent scenarios such as the Cord Blood Registry breach. Encryption does require time for configuration and ongoing maintenance, but it has a very low fixed cost," Goerlich says. "In the Cord Blood Registry scenario, three areas that should have been encrypted: the laptop hard drive, the database backup file, and the LTO4 backup tapes. If encrypted, the stolen media would be all but useless. The personal information of 300,000 people would be unreadable and unrecognizable."

He also believes organizations need to do a better job instituting tape media procedural controls as well. "These ensure that the storage tapes are transported in a manner that is physically secure. From the initial reports, it looks like Cord Blood Registry did not have these in place," he says. "A solid procedure would prevent transporting sensitive backup tapes using an employee's vehicle and prevent leaving those tapes unattended in a parking lot."

Organizations need to remember how valuable that database information on the seemingly inconsequential backup tape truly is, says Kevin Lewis, president of Prodigin Network Services, an IT services and consulting firm.

“Treat your data like a suitcase full of \$100 bills,” Lewis says. “For some companies, the data on those backup tapes is worth much more than that ... Never leave the media in your car or have employees just take it home with them. Companies like Iron Mountain offer services where they will come to your location, pick up your backups, and store them in their secured facility.”

This last point is key, according to John Bambenek, president and chief forensic examiner at Bambenek Consulting: Once you give up physical control of the database information, security becomes inordinately harder. He encourages encryption, but he also urges customers to avoid insecure transport.

“Backups are, by definition, a collection of an organization's most valuable information. If you spend money to back it up, it is obviously of value, which makes it an attractive target,” he says. “If shipping, use a backup storage company whose entire business relies on safe transport of tapes. FedEx and UPS [and others] build in that they will lose X packages into the cost of doing business. A backup storage company simply can't do that. It's worth the extra cost.”