

Cimarex Energy Case Study from *SearchSecurity.com* (October 1, 2007)

... While an increasing number of state and federal regulations has made life difficult for IT shops, many readily admit the compliance work has forced them to improve security in ways that greatly reduce the chances of a data breach.

Ann Auerbach, IT and compliance manager for Denver-based Cimarex Energy Co., acknowledges that the biggest concern for the oil and gas exploration company is that it is able to adequately respond to auditors examining its security controls. She manages a security program designed to protect a Windows-based environment used by some 800 employees.

"Because we're public we fall under Sarbanes-Oxley and one thing we need to do is prove our IT folks aren't changing financial data," she said, noting that the company employs 40 IT professionals to support six offices with 50 or more employees each, plus 30 additional field offices. "In the oil and gas business, the ownership of a well and royalty distribution are the keys to the kingdom, so **we need to be sure insiders aren't trying to change information in the data.**"

To that end, the company must provide auditors with reports proving that only authorized users are making changes to data. "We need alerts when anyone outside that small list tries to make a change," she said.

For that, she chose technology from database security vendor Guardium. She said version 6 of Guardium provides her, among other things, with regular reports auditors can study to see who is doing what on the network.

Cimarex's focus on documenting data changes made from within is wise, if the results of a recent study from auditing and accounting firm Deloitte Touche Tohmatsu is any indication. After interviewing senior IT executives from 169 global institutions, the firm found that almost [two-thirds of respondents had reported repeated external security breaches](#), and the top three breaches this year were viruses and worms, email attacks, and phishing/pharming-- all unwittingly perpetrated via the customer.

The survey also showed a shift in priorities from protecting sensitive data from attack by outsiders to addressing internal threats. Ninety-one percent of respondents said they are most concerned about employees, while nearly 80% cited the human factor as the root cause of data security breaches.

This isn't the first time IT professionals have cited insiders as their biggest security concern. A vast majority of [IT executives interviewed by SearchSecurity.com for a series on the merging physical-cyber threat](#) two years ago showed that insiders were a major cause for concern.

Indeed, many of the data breaches reported since early 2005 have been rooted in the actions of insiders. In the case of DuPont, [a malicious insider was caught giving proprietary information to a DuPont competitor](#). But in a [security breach at the U.S. Department of Veterans Affairs](#) last year, the damaging actions of an insider were more careless than malicious. The employee had been storing data on millions of veterans at home. The data was compromised when burglars broke into the home and stole computer hardware housing the data."