

# Shrinking Security Threats From Within

**A** laptop computer containing personally identifiable information downloaded from an operational database turns up missing. Confidential information is downloaded to a zip drive and walked out of a federal building. An irate programmer ‘tinkers’ with critical production applications after being passed over for promotion.

Market analysis firms estimate that insiders are responsible for between 80% and 95% of database attacks. While most organizations have strengthened both systems and network ‘perimeter’ defenses, insider threats still jeopardize public and private sector enterprises, and in many cases, government organizations may not be paying enough attention to threats from within.

Indeed, a single individual with malicious intent can bring tremendous harm – ranging from staff hours lost to ‘fix’ systems or data that’s been damaged or altered, to extensive negative publicity, severe citizen distrust and immense financial damages.

Recent survey results indicate access control gaps facilitated most (69%) of the insider incidents in the latest *Insider Threat Study (ITS): Illicit Cyber Activity in the Government Sector*, published in January by a collaborative initiative of the Secret Service National Threat Assessment Center (NTAC) and the CERT Program of Carnegie Mellon University’s Software Engineering Institute.<sup>1</sup> According to the report, “It’s increasingly clear government insiders have the potential to pose a substantial threat by virtue of their knowledge of, and access to, employer systems and associated databases. And the market value of information contained in those government databases, especially identity-related data, is likely to increase the risk of illicit activity to obtain and sell this information for financial gain.”<sup>2</sup>

To protect privacy, ensure national security and help federal agencies achieve regulatory compliance, there’s a need for solutions to ensure information can’t be changed in unauthorized ways. The ‘best practices’ approach to guard against insider breaches is to monitor both network access and databases for unusual activity, and set thresholds for acceptable use by different classes of users. Access audits are also recommended to ensure user accounts don’t still exist for employees no longer working for an organization, and to ensure access privileges haven’t been elevated. Agencies should also regularly audit to identify which users have access to what information.

Oracle is helping government secure sensitive data with solutions such as Oracle Database Vault, Advanced Security with Transparent Data Encryption, Secure Backup and Identity Management. Oracle makes it possible for organizations to ensure their data is protected to meet security, compliance and risk management challenges cost-effectively. To avoid insider threats to their databases, organizations must:

**Resolve ‘separation of duties’ challenges.** Oracle Database Vault can be used to enforce separation of duties within the database, by preventing a database administrator’s access to sensitive application data while permitting daily operational functions.

**Enforce Least Privilege by controlling user access, even for privileged users, to production databases.** With Database Vault’s powerful multi-factor rules, organizations can make database access authorization decisions that take into account IP address, time of day, authentication type and other factors that protect sensitive data and database objects.

**Continuously monitor user activities.** Oracle Audit Vault’s reports, alerts and policies expedite the jobs of audit compliance personnel, while Oracle Enterprise Manager’s Configuration Management Pack continuously monitors security and configuration of hosts and databases.

**Be prepared for forensic analysis and providing evidence.** Using Oracle Total Recall, organizations can automate database change tracking. The tamper proof historical archives are available in the database itself, allowing for seamless queries to determine when and how data was changed.

**Enforce ‘Need to Know’ policies in all applications.** Using Oracle Label Security (OLS) users can get access only to the data they have clearance to see.

**Encrypt data to boost integrity and confidentiality.** Oracle Advanced Security Transparent Data Encryption (TDE) enables data to be transparently encrypted and decrypted without application changes, while Oracle Secure Backup provides an integrated tape backup solution to ensure tape backups are encrypted and worthless if lost or stolen.

**Comply with regulations regarding sensitive or confidential data.** Oracle’s Enterprise Data Manager Data Masking Pack can mask sensitive production data in non-production development, test or staging environments, ensuring original data can’t be retrieved or recovered.

Footnotes: <sup>1, 2</sup> Insider Threat Study: Illicit Cyber Activity in the Government Sector, by the U.S. Secret Service and CERT/SEI, published in January 2008.

For more information, please visit  
[www.oracle.com/security](http://www.oracle.com/security) or call 1.800.633.0584.