



Best of ThreatChaos

## Ten best practices for avoiding data loss during layoffs

An economic downturn is one of the most difficult times to protect data. Layoffs create disgruntled employees and provides them with motivation as they face the prospect of loss of income. This afternoon I am presenting a webinar on how to protect your organization's data during these tumultuous times.

Citi Group announced 53,000 layoffs yesterday, mirroring numerous layoffs on Wall Street and Main Street. Unemployment is at levels not seen since 1994. When an organization is already experiencing high financial stress the last thing you want is a major data breach. Just as Countrywide was experiencing its troubles this past summer it came to light that one Rene Rebollo, working in Countrywide's subprime mortgage arm, was systematically downloading spread sheets of data to a USB thumb drive and selling the records of mortgage applicants for what eventually amounted to \$50K. He stole and distributed over two million identities. Don't let your company experience the kind of trouble that Countrywide went through in the subsequent disclosure process.

Here are Ten Best Practices for Data Protection During a Downturn. My starting point was the excellent Common Sense Guide to Prevention and Detection of Insider Threats [published by](#) Carnegie Mellon's CyLab.

1. Restate and re-publish your organization policy on confidential information. Require everyone in the company to sign it.
2. Have a strict policy regarding the usage of data storage devices including thumb drives, iPods, and USB hard drives.
3. Establish strict policies that allow, restrict or block data transfers to removable media
4. Identify and restrict access to key data such as employee records, resumes, customer lists, and financial statements.
5. Track employee access to data and retain copies of transferred files

6. Log, monitor and audit employee online actions
7. Use extra caution with system admins and privileged users.
8. Deactivate all accounts and network access of terminated employees.
9. Confiscate laptops, Blackberrys (all corporate phones) and storage devices of terminated employees.
10. Document insider threat controls

This entry was posted on Monday, November 17th, 2008 at 11:55 pm and is filed under [Data Security](#). You can follow any responses to this entry through the [RSS 2.0](#) feed. You can [leave a response](#), or [trackback](#) from your own site