

[Industry View](#)

Employee Monitoring Good for the Employee

'Big Brother' headlines or no - ArcSight CEO Tom Reilly argues that employee monitoring protects everyone from the negative impact of malicious insiders

By Tom Reilly, president and CEO, ArcSight

January 14, 2009 — [CSO](#) — Ever since the advent of the first business, trusted employees have stolen from their employers. Occasionally they stole for revenge or even excitement, but for the most part, they stole for money. Traditionally, perpetrators have been found in the stock room, maybe working a register, or handling accounting. However, with the advent of corporate IT networks that provide hundreds and thousands of employees with easy access to highly valuable information, the most dangerous of perpetrators are now sitting in a cubicle row or in a corner office.

A quick scan of headlines reveals that these perpetrators are of both genders and are found in all geographies and industries.

- A [DuPont](#) scientist stole \$400 million in intellectual property from his employer in the form of 16,706 documents and over 22,000 scientific abstracts
- An employee working in a Texas physicians office that was contracted to treat [FBI agents](#) attempted to sell an agent's health records to drug traffickers for \$500

A [Federal Emergency Management Agency](#) (FEMA) employee stole the identity information of 200 persons and opened \$150,000 in credit accounts

Whether it's for a little money or a lot, malicious employees have been fleecing their employers for years. Unfortunately, with the recent economic downturn, more white-collar workers might feel that the reward, or the vengeance of stealing from their employer, may outweigh the risk of being caught. Job losses, plummeting 401[K]s, foreclosures, and fire-sale mergers are taking a financial toll on the best of workers, who feel they have no control over their destiny. Combine increasing financial stress with easy access to highly valuable corporate data and a multitude of [on-line black market outlets that turn information into cash](#), and you have the perfect recipe for insider cybercrime.

Employees can commit cybercrimes such as fraud, identity theft and [theft of intellectual property](#) much faster and easier than un-trusted outsiders. Never before have so many had so much access to such a wealth of data. For example, an employee with access to sensitive information doesn't

have to be a world-class hacker to print it, copy it to an MP3 player, or e-mail it to a friend. Knowing this, many organizations have already increased their vigilance by monitoring activities that may signal insider threats:

- What applications employees are using and how are they being used
- What data is being accessed and how much
- What information is being downloaded, printed, or emailed, and at what time of day

When we work as security advisors to our customers, we are increasingly asked for tools and processes to better monitor how trusted users such as employees, consultants, partners, and others are operating on the network. Our clients have clearly shifted from worrying mostly about external hackers, worms, or phishing attacks to worrying about the insider threat, which now appears to be their number-one concern. Based upon what we're seeing globally, there will be a greater onus on monitoring for insider activity and determining the "who" when an incident occurs. Questions such as who did it; should they be doing it, and if not, what else are they doing; how long has it been happening; and who else is involved, need to be addressed efficiently and effectively. At the end of the day, you can't arrest a laptop.

Some people might see this as "Big Brother." Perhaps surprisingly, however, not only are organizations pushing for this type of monitoring, but so are many employees. In these hard times, an attack on a company could have a direct impact on employees; the company could even go out of business and employees could be out of a job. This is exactly what happened to Ellery Systems in Colorado when an employee gave intellectual property to a competitor. This case helped lead to the Economic Espionage Act of 1996, which makes the theft or misappropriation of a trade secret a federal crime. Since the damage caused by an insider can be substantially higher than that caused by an outsider, prudence dictates that insider monitoring be put in place for everyone's protection. Much like a store owner keeps an eye on his inventory and registers, corporations are keeping an eye on their most important asset, information.

Monitoring for malicious insiders isn't "Big Brother." It's smart business, and it helps protect employers as well as their employees. ##

Tom Reilly has served as [ArcSight](#) Chief Executive Officer since September 2008 and as ArcSight President since August 2007. Mr. Reilly served as ArcSight Chief Operating Officer from November 2006 to September 2007. He holds a B.S. in mechanical engineering from the [University of California, Berkeley](#).