

Disgruntled Employees in Your Law Firm: The Enemy Within

By Sharon D. Nelson, Esq. and John W. Simek

© 2005 Sensei Enterprises, Inc.

“I can take these guys out of business anytime I want”
- a law firm system administrator

If that doesn't chill your bone marrow, you need to lower your dosage of Xanax! The truth is, most law firms give the keys to their kingdom (their data) to their IT employees and pay very little attention to the inherent dangers in trusting them. Hackers and other external intruders surely remain a legitimate threat, but the greatest threat invariably comes from within.

Why do employees become disaffected? Perhaps they didn't get a raise, or feel they are not treated with sufficient respect. Perhaps they want to prove their machismo or illustrate how stupid their high paid bosses are. Some are not disgruntled but greedy, and seek to win the lottery by lifting their employer's data. The worst threat of all is the fired employee. This employee is always unhappy, and sometimes vengeful. What better way to seek revenge than to bring the law firm's technology to its knees? Without its networks, the average law firm today is virtually paralyzed.

So what can happen? Here is an example that we once had to cope with. The head of a local lawyer referral office resigned under pressure. Angry at her bar association, she performed wholesale deletions on the server, wiping out agency forms, procedures, correspondence, and historical records. Fortunately, she was not technically adroit and, with a little technical wizardry, all the deleted material was recovered despite the inexplicable absence of backup tapes. Not every employer is that lucky.

What law firms tend to worry about are power failures, system crashes, hackers, spyware and viruses. To be sure, those are all things that can and should be worried over, but the greatest danger is often close to home. It is much easier to create all manner of mayhem from within given an insider's knowledge.

Real Life Nightmares

- *An AOL software engineer stole the personal information of 92 million (million!) customers in May, 2003 and sold the data to various and sundry spammers. He originally sold the data for the less than princely sum of \$28,000 but got smarter along the way and began charging \$100,000 per sale. By the time this article is published, Mr. Jason Smathers is expected to be a guest of federal authorities for an anticipated 18-24 months.*

- *Apple filed two lawsuits in December 2004 accusing insiders and partners of leaking proprietary information.*
- *A Forbes computer technician, angered at his termination, brought down five of eight network servers. All the data in those servers was deleted and none of it was recoverable. Forbes was compelled to shut down its New York Office for two days and sustained losses of more than \$100,000.00.*
- *A Lockheed Martin employee crashed its e-mail system by sending 60,000 colleagues a personal e-mail message requesting an electronic receipt. Lockheed Martin had to fly in a Microsoft emergency response team to repair the damage.*
- *Prudential Insurance Co. had an employee merely frustrated with his sense that he was underpaid. His revenge consisted of purloining electronic personnel files for more than 60,000 Prudential employees. He not only sold the information over the Internet, but incriminated his former supervisor in the theft.*
- *Omega Engineering suffered \$10 million in losses when a network engineer, agitated about his termination, detonated a software time bomb that he had planted in the network he helped to build. The bomb paralyzed Omega, which manufactures high tech measurement and control devices used by the Navy and NASA. When the bomb went off in the central file server, which housed more than 1,000 programs as well as the specifications for molds and templates, the server crashed, erasing and purging all programs. The incident resulted in 80 layoffs and the loss of several clients.*

As horrific as these stories are, they are only the tip of the iceberg. If you want the hair on the back of your neck to stand up still further, check out the stories at <http://www.cybercrime.gov/cccases.html>.

Don't assume that disgruntled employees are all you have to worry about! There are other, often overlooked, "insiders" such as independent contractors, vendors and clients - and yes, those cleaning folks who come in late at night. If you left everything up and running, you have no idea what your computer may be doing at midnight.

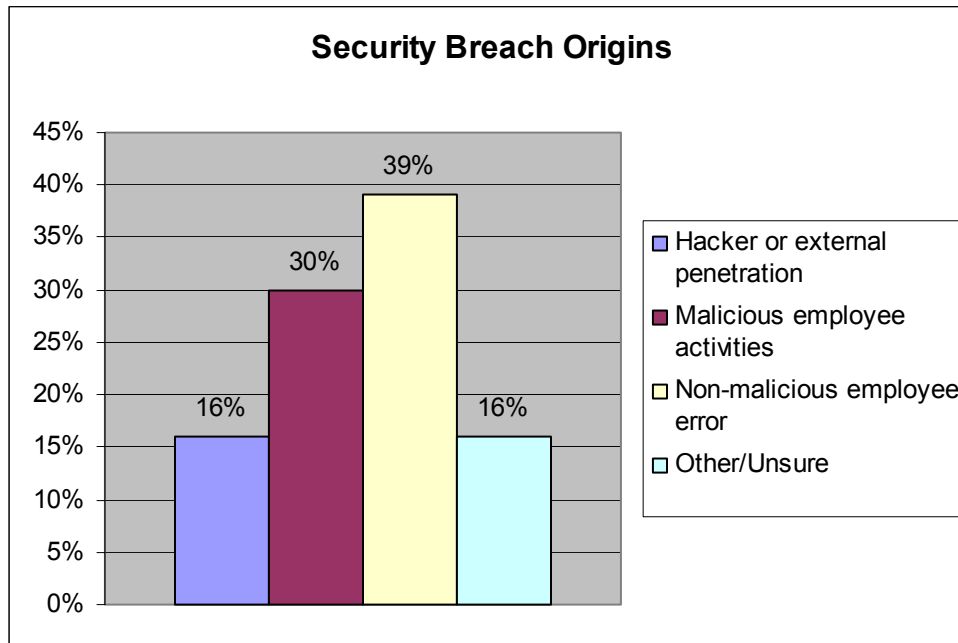
Statistics

The Gartner Group reports that 84% of high-cost security incidents occur when insiders send confidential information outside the company. It's easy to see why. Hacks have to figure out how to break into the network, then locate, obtain and distribute the target data, all without being detected by increasingly sophisticated security systems. People within the firm have authorized access to data AND access to the Internet – a deadly combination from a security standpoint.

The Computer Security Institute/FBI 2003 Computer Crime and Security Survey found that of 488 companies surveyed, 77% suspected a disgruntled employee as the source of a

security breach. Vontu, a company which makes software designed to prevent confidential data loss, conducted assessment studies which showed that one out of every 500 outbound e-mails contains confidential data.

A 2004 study by the Ponemon Institute clearly indicates that the great threat to law firm security comes from within, whether the employee action is malicious or merely inadvertent.



The Dark Side of Security

All law firms have come to recognize glumly that some level of security is necessary. With further reluctance, they acknowledge that they will have to spend serious sums on security. But they usually underestimate their needs, especially if they have not yet been burned by a security breach. It's no joke to say that security comes at a price, both literally and figuratively.

Security done right can be doggone expensive. Without question, it is always an extensive burden, and the aggravation factor doesn't decrease over time. Implementing security can slow systems down and impair productivity. There is almost always a tradeoff between security, system access and productivity. Yet the absence of security is always sorely lamented - after the fact. Tracing security breaches, remedying their effects and preventing recurrences - all of this costs a great deal more than careful preventive measures.

How to Achieve Security and Sleep at Night

- Have strong, enforced policies about computer, e-mail and Internet usage.

- Have computer security training for new employees, particularly emphasizing the dangers of social engineering.
- Check references, and run background checks on system administrators!
- Use firewalls and specialized software designed to prevent your data from leaving your firm, such as products from Vontu, Vericept, Authentica, Liquid Machines and Websense. Modern software can do such things as look for contextual clues in messages to see if they are ok to send or be coded such that particularly sensitive files can be identified and blocked from transmission. Software has evolved to the point where it can analyze a range of variables, from content patterns and relationship to sender and recipient attributes, as well as network protocols and gateway locations. Of course, this doesn't prevent a miscreant from putting the data on a thumb drive and walking out the door.
- Back up your data and do test restorations religiously.
- Use off-site "cold" storage as well as "warm" storage onsite.
- Run virus/spyware protection software that self-updates on a regular basis.
- Restrict employee access to confidential information.
- Require the use of strong passwords and regular password changes.
- Physically secure your servers and make sure all workstations are turned off when employees leave for the day.
- Monitor/filter employee activity and announce your intention to do so, making that notice a part of the dialog box when employees log-on to the network.
- Terminate employees carefully, without notice and requiring the immediate return of any company property, including laptops, PDAs, cell phones, loose media, etc. Do not allow the employee access to a computer while packing personal belongings (or have those items pre-packed) and make sure their ID is disabled so remote access is no longer possible. If misconduct is suspected, take the computer out of service until the machine can be forensically imaged and analyzed.
- Check out cyberinsurance (which we will cover in another "*Hot Buttons*" column) and make sure you have coverage appropriate for your firm.

In the end, the best prophylactic is using the suggestions above and constant vigilance. Disgruntled employees are a constant, but their ability to inflict severe financial damage has increased exponentially with the technological juggernaut. Only eternal vigilance really works - and even that only buys you a better shot at avoiding or surviving technological assaults.

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology and computer forensics firm based in Fairfax, VA. 703-359-0700 (phone)
www.senseient.com