

# The Hidden Security Threat- When Ex-Employees Represent a Security Risk

**From the laid-off to the disgruntled, ex-employees with an axe to grind can make companies vulnerable to data theft. Kaspersky Lab security evangelist Ryan Naraine discusses the threat and offers practical advice to prevent data loss.**

## By Ryan Naraine

Security Evangelist  
Kaspersky Lab Americas

When you think about securing your computer systems, whether it's on the desktop or the network, you always visualize your primary enemy as the evil hacker looking for vulnerabilities to exploit and steal your valuable data.

While that enemy remains formidable, it's important to understand – and prepare for – another dangerous adversary: that ex-staffer with access to system accounts (and default settings) that remain active after he/she has left your company.

Whenever the risks from the insider threat are discussed, it's usually about the disgruntled/malicious employee within the firewall abusing permissions to steal data or plant malware in sensitive parts of the network. But that orphaned account -- the ex-employee who still enjoys e-mail access and who knows the default passwords to the sensitive parts of your network -- is a bigger risk and, frighteningly, is often forgotten.

As the economic troubles take root and businesses implement reductions in workforce, the risk is heightened and the news headlines confirm the worst.

The story of Viktor Savtyrev, who worked as a systems administrator at a New York-based mutual fund company, is an eye-opener. In April 2009, Savtyrev pleaded guilty<sup>1</sup> in a federal court to charges that he tried to extort an undisclosed amount of money and even forcibly secure good job references from the company that had just laid him off.

According to court documents<sup>2</sup>, a day after he and 13 other employees were laid off, Savtyrev sent the firm's general counsel an email that threatened to unleash devastating attacks on the network unless his demands were met for additional severance pay and health insurance.

"My comrades for a small fee are able to help me out with bridging firewall security and carry out data destruction and virus outbreak," Savtyrev wrote in the email dated November 6. "And lucky me to find out that [the company's firewall] is the cheapest firewall to crack." He went on to threaten a barrage of

## Getting Your House in Order

**42%** of businesses do not know how many orphaned accounts exist within their organization.

**30%** of businesses said they have no procedure in place to locate orphaned accounts.

Approximately **27%** of respondents said that more than 20 orphaned accounts currently exist within their organization.

More than **30%** of respondents said it takes longer than three days to terminate an account after an employee or contractor leaves the company, while 12% said it takes longer than one month.

More than **38%** of respondents said that they have no way of determining whether a current or former employee used an orphaned account to access information, while 15% said that this has occurred at least once.

Source: Symark 2008 Survey

nasty press if the managers did not comply.

The mutual fund company facing Savtyrev's threat was lucky. It was able to contact law enforcement authorities early to avoid any damage, but without a formal policy in place to deal with this threat, the Savtyrev story could have had a terrible ending.

I'd wager a bet that more than 75 percent of small businesses have no idea how many orphaned accounts exist within their organization. Quickly, do you have a procedure, or the resources, in place to automatically nuke every user credential for exiting employees? Didn't think so. Do you have a coherent strategy for locating orphaned accounts and mitigating that risk? Probably not. And it is scary.

When that laid-off employee walks out the door, sensitive information may already be gone. When layoffs happen, there is usually rumor and buzz within affected departments. Employees who believe they are at risk of being cut can start moving critical company data to USB drives or emailing the data to personal web addresses.

In this economic environment, some employees receiving pink slips are experienced personnel whose responsibilities gave them widespread access to things like customer lists, financial information, trade secrets, roadmap plans and the overall strategic direction of the company.

Do you, as the small business owner, even know where all your IT assets are and who has access to them? In these tough economic times you have to be prudent about expending resources, but in your IT security budget you need to spare some room to create formal policies to deal with ex-employee accounts that are never disabled. It's crucial that companies get serious about keeping detailed inventory of essential data, knowing where it's stored and who has access to it, and staying alert for unusual data traffic.

A May 2008 survey of more than 800 IT professionals found that 42 percent of those surveyed didn't know how many orphaned accounts existed within their business. The survey, commissioned by Symark<sup>3</sup>, also found that 30 percent had no procedure to locate the orphaned accounts, and more than 48 percent had no way to determine whether an orphaned account had been used to access information.

Follow this practical advice to avoid the risks associated with orphaned accounts within your organization, and take the first steps in securing your network from ex-employees.

1. Be rigid about maintaining an inventory of critical data, where it is located, who has access to it, and how well it is protected.
2. Monitor access to data and keep logs of all activity on the email system.
3. Establish a formal procedure for reducing staff. Put together a checklist involving access to data and passwords for sensitive parts of the network.

4. Terminate access immediately. Avoid the temptation to get a few more days of work out of an employee who will be laid off. Once the decision is made, shut off access to the company computer and remove that person's access to everything. In some cases where really sensitive company data can be at risk, escort the employee out the door and do not allow a final log-on to the network.
5. Monitor log events. Current employees might be tempted to log in through an orphaned account to cause mischief so it's important to use technology to log keystrokes or prevent the erasure of logs. Set this up to receive an alert when someone attempts to access an unauthorized area.
6. Implement solid password management procedures. Make sure default passwords are changed the first time they are used and avoid a single password for multiple IT staffers at all costs.

[1] <http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9132280>

[2] [http://www.theregister.co.uk/2009/04/27/bofh\\_cops\\_plea/](http://www.theregister.co.uk/2009/04/27/bofh_cops_plea/)

[3] <http://blogs.zdnet.com/security/?p=1132>