



DAMAGE

From Within

What Happens When IT Goes Wrong?

by Rod Scher

KEY POINTS

▲ Companies are really just people—and most people fear being labeled “the bad guy.” That fear puts the company at risk.

▲ No one person should have enough power to completely destroy company assets or infrastructure.

▲ Regular security audits are a key to protecting the company.

▲ Security audits should include simulations that cover dealing with disgruntled or terminated employees.

Larry was an experienced system administrator who had been promoted through the ranks and was now director of IT for a Midwest business management and consulting firm. A longtime employee, Larry knew better than to violate the company’s rule against moonlighting. But moonlight he did, and management decided it had no choice but to terminate his employment. The termination meeting went well, as those things go: Instead of tears and recriminations, there were smiles and handshakes and sheepish admissions

that he’d made a mistake and a heartfelt apology for having caused this uncomfortable situation.

The managers, relieved that things had gone so smoothly, told Larry (not his real name, of course) that he was welcome to retrieve his personal gear from his office and his computer, and hand in his keys and ID on his way out, so Larry went into his office and packed up his belongings. Then, using his high-level admin passwords, he connected to every one of the company’s 11 servers and formatted every drive on every server. For good measure, he trashed

the onsite backups. Then he grabbed his cardboard box of books and posters and family pictures, handed his keys to the receptionist, and walked out the door with a smile.

It took the company months to recover, and the final cost was estimated at \$13 million.

Problems Aren't Uncommon

Security expert Chris Hadnagy, author of *Social Engineering: The Art of Human Hacking*, says that scenes like this play out regularly, mainly because companies fail to manage their employees. "Too many times companies compromise on the rules and standards they know they should have in place, because they are difficult to implement and not always the most comfortable."

This is not an isolated problem, says Hadnagy. "According to a recent industry report, there was a 27% increase in employee theft over the last year, with losses now totaling some \$994 billion." Theft, fraud, and damage by employees is one aspect of owning a company that most people do not want to think about. "But," says Hadnagy, "the unfortunate fact is that if companies do not think about it, it can end up costing them dearly."

No one wants to be the bad guy, but even something as simple as setting and following procedures for hiring and firing can make a huge difference. Rigorous policies would help companies avoid most of these kinds of problems, say experts.

Protect Your Company

What Larry's managers should have done, says Hadnagy, is disabled his mail, network, and admin accounts *during* the meeting, and then had security supervise the cleaning out of his office. Yes, that could make people uncomfortable, but it's part of managing employees and running a business; being thought a nice guy is not worth \$13 million.

Companies need policies in place to limit potential damage, including policies that detail how to handle the hiring and firing of employees. And at the root of those policies should lie the safety and security of the company and its employees, not the comfort and convenience of either the firing manager or the terminated employee.

One excellent step, say security experts, is the establishment of regular and rigorous security audits—including audits that simulate terminations and disgruntled employees.

A security expert we'll call "Martha" told us about going "undercover" in a financial services company that was worried about the stability and intentions of its lead system administrator. "The sys admin apparently had some performance issues," she says. "But

every time they tried to talk to him about those issues, he would freak out—childish stuff. The company wanted to address his problems, but the managers were afraid that he would blow the company away."

Martha went in pretending to do a HIPAA (Health Insurance Portability and Accountability Act) audit, but her real goal was to check out the administrator. In the end, says Martha, "My take was that he was a tech nerd who'd been left unsupervised for too long and who used the company as a playground simply because he could get away with it." The employee was buying toys and implementing the "latest and greatest" all the time, but not getting the more foundational, boring things done at all. "Also," notes Martha, "he was on straight salary and was paid very well, so he really had no incentive to meet various goals, because he was paid the same no matter what."

The solution? "Have the other IT people step up and take on more responsibility. Make this guy be a real manager and give him clear, measurable goals that he can be held to." And, says Martha, "if there's no one else on staff with a comparable technical background—as was the case here—bring in quarterly oversight to review the budget and documentation."

In this instance, notes Martha, there was plenty of blame to go around. Sure, the employee was immature and self-indulgent, but the company was also at fault. Employees need to be managed, and someone in this situation had abdicated a basic managerial responsibility.

It's Your Policy, So It's Your Responsibility

Employees have and need power, access to sensitive data and valuable equipment, and enough autonomy to encourage them to make the most of that power and access. But they also need oversight.

Consider Martha's comment about the company worrying that a rogue employee might "blow the company away." An early security audit would have uncovered that risk and raised alarms: No company should ever confer on one person enough power to destroy an entire company. Allowing such a situation to exist in the first place is simply bad risk management—and bad risk management usually boils down to bad management in general, say the security experts.

In the end, there's no getting around the fact that people in positions of power require access to powerful tools; limiting that access would limit their ability to do their jobs. That means that nothing short of sensible policies, regular security audits, and intelligent, active oversight will protect a company from the misuse of that power. ▲

The Ultimate Rogue IT Scenario

TERRY CHILDS HOLDS
SAN FRANCISCO
HOSTAGE

Municipalities are, in effect, businesses—and they can be just as vulnerable as any other business. When the City of San Francisco decided to fire its senior IT guru in July of 2008, it learned just *how* vulnerable: During a confrontational termination meeting, the city's chief IT staffer, Terry Childs, was ordered to hand over passwords to the city's network. He did so, but it turned out that the passwords he had given them were bogus. Days later, Childs handed over the real passwords to San Francisco mayor Gavin Newsom, the only person he felt was competent to handle them. It turned out that the city didn't actually have in place procedures that outlined how (or to whom) to hand over passwords, which is the issue on which Childs based his defense. In April of 2010, Childs was found guilty of network tampering. ▲

