Disgruntled Employees: Today’s Biggest IT Threat

It’s late on a Friday afternoon before an expected busy holiday weekend, and an employee at a ski area was let go due to performance issues. No one in HR or building security was around to collect building keys. So later that night, the fired employee entered the building and poured 5 gallons of varnish on the company servers. Needless to say, the company’s entire operations were seriously compromised the next day.

When the economy sours, some of the biggest threats to IT security are not rapidly spreading viruses, but the rapidly expanding number of disgruntled or fired employees. Predators to a company’s IT system can be internal as well as external, and companies must be vigilant in taking steps to protect themselves from employees upset over lack of raises or a pink slip. There are several ways you can encourage your technology clients to step up their efforts:

1. Beef up the physical security of the server

A company must ensure that the server is physically protected. Who has access to the room? Who controls the administration of access to the room? Is the server itself appropriately protected? While many companies have the good sense to keep servers in highly protected rooms protected from floods, earthquakes, and other damages, other companies keep servers sitting right under a conference table or desk, where it is just a coffee spill away from disaster. Moving servers into a locked room, or from an easily accessible basement to a security floor can limit or reduce physical harm to the server.

2. Establish procedures for discontinuing computer access

When an employee has been terminated, it is important to cut off network access to the company’s system within a matter of hours, not days. Who would notify IT that an employee has been terminated and how long would that take? Do you know how quickly IT could turn off their access after they are notified? How quickly could they get any company computers returned? Could they get cell phones, pagers and blackberry’s back before an angry ex-employee acts inappropriately with company tools and resources? This issue is becoming more complicated as many workers operate out of their homes or in remote offices where IT staff is not located.

3. Obtain access to a terminated employees’ records and files

If the person running the payroll department is terminated and is angry about it, all they would need do is put a password on the payroll records and no one, not even the overall system administrator, could open that file. All the company payroll records would be sealed. A company doesn’t want to suddenly find that they need to spend a day or two figuring out how to get access to their invoice system, after the person in charge was let go. It’s malicious behavior like this that makes it critical to obtain a terminated employees’ digital records and files as soon as possible before they are permanently locked up or destroyed.

Formal, effective IT security policies are important in good economic times and in bad. But in poor business environments, preventing a breach to IT security often means taking a closer look at the policies and procedures in place for potential devious current or departing employees.

Quote of the day:
“Nothing is so fatiguing as the eternal hanging on of an uncompleted task.” William James

For more information, please contact:
Workers Comp & Employee Safety: Helen Richards at 800.528.7730 or helen_richards@wellsfargois.com
Employee Benefits: Nancy Taylor-Babcock at 800.876.0505 or nancy_taylorbabcock@wellsfargois.com

This publication is intended to be a general discussion of the matters contained herein and the information should not be used in making a decision concerning the subject matter without consulting with your attorney, accountant, or insurance professional. Wells Fargo Special Risks assumes no responsibility whatsoever in connection with its use.