CITADEL
INFORMATION GROUP, INC.

# MEMO

To: HR Directors
Employment and Labor Attorneys
CEOs, CFOs, Other Interested Parties

From: Stan Stahl, Ph.D.

Date: July 11, 2009

Subject: *Mitigating Information Risk When Taking Disciplinary Action Against IT and Information Security Personnel*

---

**The Bottom Line:**

There is significant information and business risk in taking disciplinary action against IT and information security personnel.

By lining up its *information risk ducks* prior to taking disciplinary action, the company minimizes its information and business risk.

**Since disciplining IT and information security personnel entails an already high degree of information and business risk, any failure to get the *information risk ducks* lined up prior to taking disciplinary action may unnecessarily expose the company to significant and material consequences.**

IT personnel have the keys to kingdom. Information security personnel have both the keys to the kingdom AND a knowledge of where defenses are weak. Both have the ability to attack the IT network, potentially compromising, modifying, damaging, hijacking or even destroying the information the company needs to run its business and that it must protect to comply with laws, regulations and contracts.

As the following list illustrates—and it is by no means exhaustive—there is significant information risk in taking disciplinary action against an IT or information security employee. This risk is magnified if the employee is angry, feels he is being treated unfairly or is otherwise disgruntled. And **because of the vital importance of information to the company's business and the kind of information it stores in its systems, this information risk translates directly to significant business risk**. [1]

[1] For example, if uninsured, the company can expect to pay more than $200 for every person it is required by law to notify should the employee disclose sensitive information about the company's clients, customers or employees. (http://www.networkworld.com/news/2009/020209-data-breach.html.) Not included in this amount is

The company must expect that a motivated IT or information security employee has the means to launch a cyber-attack at the time and in the manner of his choosing. The company must assume that the employee can gain access to the network, that he can remain on the network undetected, and that, through his undetected access, he can bring harm to the company.

- The employee may have already set-up access paths into the corporate IT network from the outside
    - He might have established legitimate-looking rogue accounts which no one in IT knows about
    - He may have an illegitimate access path through a corporate firewall, either through established ports designed to allow traffic [e.g., Port 110 which is used for incoming email or the ports used for Citrix] or through ports he has purposely opened for his use [2]
    - He may have an illegitimate access path directly to a server or workstation to which he's attached a rogue modem or a wireless access point
    - He may have an illegitimate access path through a less-well-protected remote office
    - He may have an illegitimate access path through a less-well-protected vendor or other 3rd-party having access into the corporate network
- The employee may have already compromised servers, workstations, switches, password vaults, etc with Trojan horses, hard-to-detect rootkits or other hacker tools that he can remotely control
- The employee may know sensitive passwords to servers, firewalls, switches, password vaults, etc
- The employee may know the vulnerabilities in the network, in servers, workstations, switches etc and may have a treasure-trove of exploits to take advantage of these vulnerabilities
- The employee may have booby-trapped servers, workstations or other devices with *computer time bombs* or *computer logic bombs* [3]

---

the approximately 20% of customers who studies indicate may switch take their business elsewhere in the event of a breach disclosure.

[2] There are more than 64,000 ports. Few companies are going to have a detailed up-to-date accurate listing of all approved firewall ports on all the firewalls in use at the company.

[3] In a very famous case from the late-1990s, a disgruntled employee at an aerospace company in New Jersey changed the back-up program on the server so it only looked like it was backing up the server; it really wasn't doing anything. He then installed a computer program -- a *computer time bomb* – to reformat the server 6 months later. Six months later, on the given date, the program reformatted the server's hard drive and, since the backups were worthless, the company lost all its data. The ex-employee went to jail. The company went out of business.

- The employee may have the knowledge and capability to alter audit logs and fool forensic tools like EnCase so as to remain undetected on the network
- The employee may have installed his own rogue monitoring system on the network so he can detect if others are coming after him
- The employee may have colleagues, other employees, or even vendors that he can social engineer to give him network access

In mitigating its risk, the company must accept the reality that there is a high probability that motivated IT staff – even more-so, motivated information security staff – will be successful in obtaining illegitimate access to the network and have the ability to cause severe information damage; there are just too many holes to block and too many places to hide. And, **as the examples show, the advantage may likely lie with the employee.**

It is common in business to get "*one's ducks lined up*" prior to taking risky action. HR and legal are used to getting their "*employee risk ducks*" lined up with respect to employment laws, company policies and the corporate culture prior to taking disciplinary action against employees.

There are corresponding "*information risk ducks*" that need to be lined up when considering disciplinary action against IT and information security personnel.

By lining up these and other "*information risk ducks*" prior to taking action one can minimize the information risk – and consequent business risk – associated with disciplining IT or information security staff:

- Tighten defenses against a direct attack through the company's perimeter, including all firewalls, all offices, all vendors and all other 3rd-parties having access to the IT network
- Analyze workstations, servers and other devices for backdoors, planted Trojan horses, rootkits and other technology malware and strengthen defenses against these
- Review all user accounts for legitimacy
- Change administrative passwords on all servers, switches, routers, firewalls, etc; force a password change on all users
- Analyze the employee's workstation(s), both forensically and dynamically, looking for evidence that could be used to support disciplinary action but, more importantly, looking for indicators of how he might attack the network
- Increase IT network monitoring to catch an attack at an early stage before damage can be done and to gather evidence for use should an attack occur, being very cautious that increased monitoring is kept very covert
- Make sure that backup systems are correctly working and in place

- More generally, make sure that incident response, information continuity and business continuity plans are up-to-date so that the company can gracefully recover should the disciplined employee be successful in attacking the network
- Make sure IT and information security staff have the necessary forensics training to successfully preserve evidence should an attack occur
- Communicate the situation to others so as to block social engineering attacks
    - IT and information security staff
    - Other staff who may have a relationship with the staff member being disciplined
    - Outside vendors and other people who may have a relationship with the staff member being disciplined
- Review cyber-insurance to make sure it is adequate; both business interruption insurance and liability insurance covering any damages caused to clients, employees and other 3rd-parties

***Carrots and Sticks:*** One additional method for reducing risk is to make it abundantly clear to the employee that he has much to gain by not attacking the network and much to lose should he attack it.

*Carrot:* Offer the employee a sum of money to leave the company in return for which he commits to leave the company alone. Spread the payments out over time triggered by his good-behavior.

*Stick:* Make it abundantly clear that the company will take the strongest legal action if he – or someone acting on his behalf – illegitimately accesses the network or causes harm to the network. Let him know you'll be watching but be careful: you want to frighten him; you don't want to challenge him and get his competitive juices flowing.

## Citadel Information Group

**Providing *Information Peace of Mind* ® to Business and the Not-for-Profit Community**

| | | |
|---|---|---|
| Kimberly Pease, CISSP | 323.397.5752 | kpease@citadel-information.com |
| Stan Stahl, Ph.D. | 323.428.0441 | sstahl@ citadel-information.com |