Data Theft Is Big Business - Are You Protected?

According to the U.S. Federal Trade Commission Internet fraud complaints soared from $206 million in 2003 to $336 million in 2005. The worst news, according to a survey performed by the Enterprise Strategy Group in 2006, is that your data is more likely to be stolen from inside your company by employees or on-site contractors than by outside hackers.

Protecting your most valuable and sensitive data must be a three-fold approach:

Assess Your Data Risk

Begin the process by asking yourself three basic questions.

- **Who would want steal from my company?** Consider the possibilities from different perspectives such as hackers, competitors, thieves, disgruntled current or former employees.
- **What data would they want to steal?** Sensitive data is any information which compromises the security of your company. Client information, product and technology information, social security numbers, bank account and financial information, credit card numbers are just a few examples of the data which could be at risk.
- **What do I need to do to plug the leaks and protect this data?** Security measures you can implement range from the very economical, such as purchasing commercial security software, to having an IT security consultant develop a custom security system appropriate to your company’s needs.

Formulate Internal Security Procedures

Creating in-house security procedures is the only sure way to prevent data leaks from occurring inside your company. Security measures should include technical features, physical safeguards and the human element. Proactive steps to remedy potential weak points include:

- **Ensuring terminated employees lose access** to not just the physical locale, but to the computer network, e-mail, and voice-mail systems as well.
- **Implementing access controls** through the creation of internal firewalls to restrict the availability of sensitive data to only those employees who need it.
- **Creating stringent password policies** to ensure employees do not share passwords. Alter passwords when employees leave or use additional passwords for sensitive data. Passwords should be strengthened by using a mixture of letters and symbols.
- **Updating your operating system regularly.** Newer systems upgrade their security software and the options relating to access control giving you better security.
- **Scrutinizing how employees use your computer system.** Prevent employees from being able to download material to CD’s or Ipods. Install security alarms to alert you when large blocks of data are deleted. Include a system to allow designated IT staff to be guard against unauthorized remote access to internal data.

Develop Systems/Internet Security

Data threats from within your physical locale can be solved by:

- **Employing encryption algorithms** to protect vital data by making it unreadable to outside eyes. This includes your order forms where sensitive information such as credit card numbers or bank account information is involved and e-mail between employees who are transmitting crucial or sensitive information should also be encrypted.
- **Basic or custom designed security software packages** which guard against viruses and worms are essential. Many companies fail to regularly update their security protection. Hackers or crackers evolve their methods and strategy of attack frequently and can be incredibly diabolical and creative.

- **Ensure you have a firewall** suitable to the needs of your company. Commercial software packages may be adequate for smaller companies, but larger companies may require custom designed systems to safeguard sensitive data.

- **Back up all of your systems on a regular basis.** Larger companies should do so daily while smaller companies could get by with weekly backups. Regardless, backups should be stored *off-site!* Should you keep backups on-site when your business experiences a natural disaster your backup system could also be destroyed. Companies need to be able to set up their system from another location with minimal delay.

- **Consider adding a virtual private network (VPN).** Vested partners must be able to access the necessary data from your company in a secure manner. A VPN will allow safe access from remote locations. Extend your security system to any hardware employees are using such as cell phones, laptops etc.