

Information Security – How Prepared Is Your Organization?

Before you suggest that your organization has a solid information security practice, consider the following five true stories:

- An influential attorney, involved in a complex merger acquisition was overhead to say, “I’ll just Email the compensation agreements to you, because it’s too confidential for faxing...”
- An Excel payroll file was stored on a shared drive of a file server, so the president and CFO could both access the information. They believed this was a safe practice because the file was password protected.
- An accountant emailed a password protected “pdf” file to a client (at their request) containing their last year’s tax return.
- An executive frequently worked at home. Although he had a very secure connection to his office systems, with encryption and multiple layers of passwords, he was unaware that his daughter had installed a file-sharing program on the home computer.
- A laptop belonging to a Veteran’s Association was stolen. It contained a list with the names of thousands of Veterans, including their addresses and social security numbers.

Each of these stories emphasizes common misconceptions about security and electronic information and gives the ill-informed a false sense of security if they are not careful. However, contrary to popular belief, it is very easy to tap into electronic data and access vital information.

Email Security – Email is highly susceptible to security leaks, because email standards specify how data is contained so that various email systems can work together. In addition, email passes over a public network, making it available to a plethora of snooping eyes. In essence, an ***Email is less private than a post card!***

Password Protection – This form of protection only provides a minimal level of security. There are many tools readily available to open such files regardless of the passwords.

Stolen or Lost Computers – Data on any hard disk is accessible to anyone with a little knowledge and patience, even if the disk has a password.

Phone: 773.868.4381

Fax: 773.913.6217

www.en-terpret.com

3642 N Magnolia, Suite 2

Chicago, Illinois 60613 USA

Associated Worldwide with JHI
www.jhi.com



VPN's or other "secure" remote access tools – these can be compromised easily if the remote equipment is already compromised. File sharing software, shares and unencrypted Wireless networks...even viruses and spyware can expose company data via the "secure" VPN.

The Bottom Line

Your data is not secure and you should be concerned about this... concerned enough to develop a ***Comprehensive Information Security Plan*** for your organization. This plan should include Email policies, data encryption strategies and much more. If you are unsure where to begin or would like more information, please contact an expert to get you started.

For more information, call Dan Harris at 773-868-4381 or email him at dharris@enterpret.com.

