SUMMER 2014 E-NEWSLETTER

At Digital Mountain we assist our clients with their computer forensics, e-discovery and cyber security needs. With data security breaches continuing to make headlines and an organization's intellectual property at risk, we chose to theme our Spring 2014 E-Newsletter on intellectual property protection.

THE TEN COMMANDMENTS FOR PROTECTING YOUR ORGANIZATION'S DATA

Data security is of the utmost importance, but can be an overwhelming mission for a company. Even if you strive for perfection, it's not a question of if, but rather when, a data security breach may happen. Unlike the earlier days of the World Wide Web, mission critical data is now connected and the community of thieves has expanded globally, spawning different laws and regulations that are not all under the jurisdiction of the United States. While this article may not solve each organization's specific data security needs and desire to be bulletproof, the following steps are musts for your organization to improve its employees' data security posture:

1. Employees must watch out for phishing emails asking for additional personal information or IDs based on incomplete information presented to them. Clicking on Internet links or attachments should be avoided within these emails, especially when they appear suspicious. A helpful tool: hover the mouse over the Internet link to see if it redirects to an unrelated Web site. If so, it could have malicious executables or malware.

2. Employees must avoid logging onto open networks that are not encrypted, especially when transferring sensitive data. Data is sent as clear text, so on open networks information can be easily captured by anyone motivated to steal another's information. If possible, your IT department should install endpoint firewall protection and train employees how to effectively use it.

3. For documents containing sensitive intellectual property such as product roadmaps, strategic plans, product demos, etc., employees must encrypt the relevant documents and transport communications via secure messaging systems.

4. For each device, the employee or IT personnel must ensure that automatic log-off and screen lock happens after a reasonable period of inactivity. Additionally, if the employee has to go down the hall, he must always lock his machine. A helpful tool: the easy shortcut for logging off a Windows-based computer is the symbol in your lower left hand corner of your keyboard coupled with the “L” key.

5. Employees must always create passwords with at least eight characters mixed with lowercase and uppercase, as well as alphabetic, numbers and symbols if permitted. These are much harder to crack if a hacker desires to breach an account. Some practitioners recommend a minimum of more than eight characters, but it may not be practical given more errors may be made by the employee in typing and lost productivity may occur. Additionally, employees must avoid character repetition, keyboard patterns, dictionary words, letter or number sequences, usernames, relative, pet names, romantic links (current or past) and biographical information (e.g. ID numbers, ancestors' names or dates). Employees must refrain from using sticky notes or white boards for documenting user names or passwords.

6. Employees must change their passwords within a reasonable period of time (e.g. every 90 days) and don't allow the same password to be re-used regularly (e.g. the last five consecutive times). IT should also be able to implement automated password rules for employees to follow to be able to scale these policies across your organization. For more secure systems, passphrases may ensure stronger protection than passwords with lengthier characters making brute force attacks and cracking impractical.

7. Employees must ensure all mobile devices and tablet devices have passwords. This may sound rudimentary but is not always followed and is simple to implement.

8. Train and remind employees of proper etiquette for social networking and blogs. Company intellectual property and sensitive information must not be communicated publicly.

9. For discarded devices that may contain intellectual property or other sensitive information, all data must be properly wiped prior to donating or discarding. Beyond employees, many companies forget about this simple protection when divesting divisions, discarding equipment or winding down operations.

10. For mobile devices or laptops owned by an employee that may contain company data on the hard drive locally, he or she must add a lo-jack type of tracking software installed along with remote wiping capability (assumes data is synched or backed up to another location).

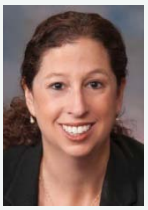
The above steps, coupled with education, are ten simple rules all employees should follow in order to help protect your company's valuable information.

UPCOMING INDUSTRY EVENTS

July 2014

Today's General Counsel Event: July 16-17
Masters Conference, Half Day EDiscovery and Social Media Conference: July 22
The 6th Annual Sedona Conference International Programme: July 23-24
The 15th Annual Sedona Conference On Antitrust Law & Litigation: July 24-25

Click here to see more upcoming events and links



Digital Mountain, Inc. Founder and CEO, Julie Lewis, will be presenting at some upcoming industry events. Please send requests for speaker or panel participation for her to marketing@digitalmountain.com.

Know someone looking for work in the e-discovery, computer forensics and cyber security industries, with entrepreneurial characteristics? If so, please share this great job opportunity with them: Seeking a Business Development Representative to join our energetic team. ***Read more...***

DIGITAL MOUNTAIN, INC.
5050 El Camino Real, Suite 205
Los Altos, CA 94022
866.DIG.DOCS

www.digitalmountain.com

Contact us today!