

Securing Confidential and Trade Secret Information: Battening Down the Hatches

By Brett Creasy*

Companies, large and small, lose millions of dollars every year when employees take confidential and trade secret information. When an employee leaves and joins a competitor and the competitor suddenly signs a deal with a client, not only do eyebrows get raised, but litigation is likely to follow, particularly if the former employee used confidential company information to lure the client away. Many companies overlook some of the easiest and cost-effective ways to prevent the loss of their proprietary and confidential information. In fact, most companies already have the required tools; they just need to use them. Below are some steps that nearly all companies can implement that will help secure their confidential information.

need access to the confidential information to perform his or her day-to-day functions, then such access should be restricted. Convenience is not an acceptable reason to fail to secure what is valuable to the company. Most businesses already have the tools to restrict access to confidential information because these tools are built in to modern operating systems, including Microsoft Windows and Linux derivatives. It is simply a matter of enabling the built-in access control features to assign individual usernames and passwords, and to create security roles such as “administrator” that would have access to everything or “accounting user” which has access to only accounting records. By assigning a “role” to each user, access to data or document repositories may be re-

“Do employees use their home personal computers to access trade secret information? Is the most critical company information maintained on company secured network shares?”

Determine Where Confidential Information Is Located: One of the first steps in securing proprietary and confidential electronic information is to identify all of the potential electronic repositories where employees maintain and access the company’s confidential electronic information. For example, are confidential electronic documents kept on everyone’s personal computers? Are employees permitted to take copies of confidential documents home on portable media (such as a thumb drive or CD)? Do employees use their personal home computers to access trade secret information? Is the most critical company information maintained on company secured network shares? Does the central company repository that contains sales and marketing materials also contain the information relating to patent issues for the product? Once a company knows where its confidential information is located, then it can take the steps described below.

Restrict Access to Confidential and Proprietary Information: Simply stated, if an employee does not

stricted to only the documents or data relevant for a user’s job function. Restrictions as to what a user can do with a document may also be applied. For example, employees in the human resources department probably do not require access to accounting records, and should be assigned a role that prevents them from accessing the accounting records. In addition, some employees within human resources may need to read information from an employee file, but may not need to add or modify the information. A special role can be created to grant the access required, while restricting the ability to modify the information. Assigning user roles provides other useful security benefits including centralized management of network access, limiting the spread of viruses and preventing accidental deletion of information.

This issue of qubit and past issues are available on our website at:
www.bit-x-bit.com

Securing Confidential and Trade Secret Information: Battening Down the Hatches*from p. 1)*

Communicate the Confidential Nature of the Information: Confidential company information should be identified and when appropriate “branded” as such. This can be easily accomplished through appropriate labeling such as “water marks” (available in Microsoft Word), login prompts (configurable through the operating system) and employee training. All of these steps can help fight the “I didn’t know” response, and help establish that the company trade secrets were marked appropriately, which is important for court enforcement of trade secret protection. It also will help to educate employees against misusing company information for things such as responding to “innocent” requests for confidential information, employees helping themselves to customer lists or peeking at the accounting records to see what the person in the next office is earning.

Encryption: Encryption tools, which effectively scramble data until it is unlocked with the correct encryption “key,” can help keep confidential data safe. Similar to access control tools, encryption tools are part of modern operating systems and many common applications. BitLocker, which is built into the “Ultimate Editions” of newer Windows operating systems is one such tool for encrypting data at rest on a hard drive. Encrypting confidential data while it is in transit is equally important and can be accomplished by leveraging the encryption technologies available in popular applications such as Microsoft Exchange email server and Outlook clients, Microsoft IIS, or Apache web servers and Adobe Acrobat.

Enforce a Clean Desk Policy: Important papers, CDs, USB drives, and other items left on an employee’s desk can be easily removed or copied by cleaning crews, company visitors, or even other employees. While a marketing manager may not have electronic access to research and development data, or the company’s financial reports, if these items are left on a desk unattended, they are suddenly accessible without any “logs” to show when and how they were taken. Similarly, failing to log off a company network or exit from a desktop when an employee is away from his or her desk may expose confidential information to the risk of loss or theft by someone simply sitting down at the terminal of someone who has already logged in.

Monitor and Audit Access: Establish regular auditing of data repositories containing confidential information and

access to those repositories to ensure that the company’s information security policy is being enforced. Knowing that such company auditing practices exist may in fact deter employees from the risks associated with taking confidential information.

Preserve Departing Employee Information: When an employee leaves to go to a competitor, be sure to preserve anything that he or she worked on for the company, as well as any email and cell phone communications. Desktop and laptop computers, company issued cell phones, PDAs and the employee’s email are just a few examples of the valuable sources of information that may be critical to any potential legal action against the employee. The manner in which the information and digital evidence is preserved is extremely important as well. If trade secret theft is a possibility, company managers and IT staff should resist the temptation to take even the slightest peek at the departing employee’s computer or cell phone until the information can be properly preserved. Ideally, a forensic image should be made of the key systems by an expert with the proper training, experience and forensic tools. If the matter ends up in litigation, and sound preservation procedures were not used resulting in the loss of critical evidence, then a solid case may be jeopardized.



**Brett Creasy recently joined bit-x-bit, LLC
as a Forensic & E-Discovery Analyst.*

Prior to joining bit-x-bit, Mr. Creasy was an Information Security Analyst with UPMC’s Information Security Group.

For questions or comments regarding this issue of qubit, please contact Susan Ardisson at Susan.Ardisson@bit-x-bit.com.

qubit \ˈkyü -bit\ n. a quantum bit, the counterpart in quantum computing to the binary digit or bit of classical computing. Just as a bit is the basic unit of information in a classical computer, a qubit is the basic unit of information in a quantum computer. *whatis.com*

This publication is for informational purposes only and is not meant to be, nor should it be, construed as legal advice.

© 2010 bit-x-bit, LLC. All rights reserved.