
JOB SECURITY ALSO DEPENDS ON INFORMATION SECURITY

(Sunday, 01 May 2005) - Contributed by Richard Jones - Last Updated (Friday, 03 February 2006)

10 ways every employee can help secure the information that keeps their company running, competitive, and profitable

Ira Winkler, a former corporate spy now employed as a global security expert, recently reminded businesses that data thieves are interested in information, not just the computers that many companies bolt to desks or hide behind locked doors.

Information about the companies themselves. Information about their customers. Information about their marketing plans. Information that someone can use to steal, corrupt, and destroy corporate information. All this information is what corporate spies and other data thieves are really after.

Therefore, companies must be as diligent about information security as they are about computer security, which, says Winkler, are not the same thing. "You can protect a computer perfectly," said Winkler to ComputerWorld.com, "but if someone throws out a classified printout, you are out of luck."

That means a company's security measures must extend beyond its buildings, equipment, hardware, and managers' offices to most of its information and all its information workers. All employees need to be trained to also assist with preserving and protecting critical and confidential information because corruption or theft of such corporate data can adversely affect each and every one of them.

Every employee can assist with information security by adhering to simple guidelines such as the following.

First, take full possession of your login credentials. Do not allow other people to logon to anything as you. Whatever happens under your user ID is your responsibility, so do not risk your job by allowing others to access corporate information as you. If someone needs access to particular data, instruct them to take up the matter with their manager.

Second, do not give your passwords to anyone, including IT staff members, because they do not need your passwords. For example, while help desk workers may need to confirm your identity, your username, or that you have been granted a particular security clearance, they never need your password to reset it or for testing or troubleshooting purposes. If they need to, they can change your password without knowing your current or old one, issue you a new temporary password, or ask an account administrator to do so. Neither should you give your passwords to your managers, who also should not access company information and network resources as anyone except themselves.

Third, use strong passwords. Simple passwords are weak passwords that only strengthen the possibility of someone guessing or cracking them. Do not use words like the names of people, places, or things. Do not use just numbers or any dictionary word. Use your imagination to create complex passwords that you can remember, but which are difficult for others to guess. Use six characters or more, including at least two numbers, a special character, and no more than two repeating characters.

Fourth, do not write down your login credentials or other confidential information and leave this information where others might find it. Many employees jot their usernames and passwords on sticky notes and leave this information on their desks, computer monitors, or inside unlocked desk drawers. These are very bad practices. Keep your login credentials in your head or some other very secure location.

Fifth, when you no longer need papers with passwords or other confidential information on them, shred these papers rather than discard them like regular trash. No thanks to employees filling garbage containers with intact documents containing passwords and other sensitive information, the trash has become a veritable goldmine of information sought by corporate spies, hackers, and other ill-intentioned information hounds. Destroy and do not simply discard login credentials and sensitive corporate data.

Sixth, practice sanctioned as well as safe computing. For instance, do not visit a Web site or do anything with a company computer or email account unless you have a legitimate business reason. Whenever you are prompted to save a password, do not do so. Also, lock your computer screen before stepping away for any reason. If you access company data from home or another remote location, work with the IT department to ensure that the computer and access method you use are properly secured. Take extra precaution not to give others unauthorized access to a computer that you logon to or to password-protected resources you access via a computer.

Seventh, store all company data in secured locations. When using a computer, store business files in secured locations on the network or the computer's hard drive. Store paper documents in locked desk drawers, compartments, file cabinets, or designated filing areas. Avoid making confidential information available to the wrong people simply by putting it in the wrong place on your computer or somewhere else it does not belong.

Eighth, do not share any more information about the company than what management has authorized you to share. Moreover, before telling anyone anything about the company, make sure they are who they say they are, that they are

entitled to the information, and that the information is not classified. Also, when someone asks you anything about the company's network or its servers, instruct them to contact the IT department. Be careful not to tell the wrong person all the "right" things.

Ninth, hold private conversations about private matters. Be aware of who is around you and near you when talk about business matters, especially if your company or department does not adhere to the practice of security conscious seating. Credible research consistently shows that "insiders" – for example, disgruntled employees and so-called script kiddies with any level of network access – pose one of the greatest threats to information security and data integrity. Avoid being overheard by those who should not know what you are talking about.

Tenth and finally, if you are a manager, immediately notify the IT department whenever one of your employees leaves the company. This will permit the IT staff to disable that former employee's login credentials before these are put to misuse. Remember, too, that it constitutes a security breach to give a former employee's login credentials to their replacement. Request that a former employee's login credentials be revoked and, when necessary, that new login credentials be given to a new employee. In addition, you should encourage and enable employees to report those who may be abusing their access privileges or violating these basic security guidelines.

This is not an exhaustive list of measures that companies should take to secure sensitive information. Rather these are some things all employees must do to help keep sensitive information out of the wrong hands, eyes, and ears. Management, the IT department, and those responsible for securing premises and other company property must work together to develop and deploy a comprehensive security strategy that incorporates these security guidelines; for it only takes one employee being careless with information to expose a company to unnecessary risks and financial woes that could negatively impact all of its employees.

Richard Jones (www.iamrj.com) is a systems administrator and freelance writer living in Detroit, Michigan USA. He can be reached by email at rjones@email.com.