Information Security Starts at Home

A former employer had a very effective Director of Marketing who worked closely with all the principals and contacted many of the firm's current and prospective customers. One Thursday, she asked her staff to help print out the firm's customer and prospect records from the in-house databases. She apparently wanted a hard-copy of this vital information. One Monday, she and her assistant gave their notice. Apparently, the customer printouts had already been carried home over the weekend.

A few discussions later with the firm's attorneys and the paper documents were back in our hands, but the breach occurred. Indeed, if the marketing director was more technically savvy, the data may well have been copied to a CD with no outside assistance and no-one would have known about the loss at all!

Most data security breaches are not from clever hackers working through the Internet. They are from employees and coworkers. The past several months have been economically difficult, and have involved layoffs for many firms. A great deal of care and consideration must be taken when laying off or firing employees, but securing your network from tampering and data loss must be a primary goal.

A disgruntled employee may delete needed files, release a virus into your network, copy sensitive information to disk or e-mail it to an outside address.

Of course, this is not to say your employees should be treated as criminals, either.

It is vital that employee access to computer resources (including data files and e-mail) be centrally managed from the server, so that access can be changed instantly. It is equally important that employees are not introduced to the fact that they are terminated when they sit at their desk in the morning by the fact that they lack computer access. An employee's termination is a professional business decision, and should be handled with professionalism in a businesslike manner.

When an employee is called into your office for the bad news, then is the time to close their access to computer resources - no sooner or later. The procedure should be explained as a normal precaution so that it is not a surprise, and non-sensitive files for their resume should be provided by request on disk or CD.

This all assumes that you are using secure workstations and strong password authentication procedures. If you are still using Windows9x or other non-business operating system, you cannot secure your workstations. You must be using WindowsNT, 2000Pro or XPPro, Mac OSX, or a Unix or Linux type of desktop environment. You must also be using a central user directory so that changes in user permissions on the server are recognized at all workstations. Windows, UNIX, Linux, Netware and Mac OSX Server all provide capable user administration tools.

Each user must have a truly private password unknown to anyone else. If everyone knows that Anthony's password is likely to be "tony", you don't have a secure network. If you have told your personal secretary your password, you don't have a secure network. If your network administrator knows your password, you don't have a secure network. Most servers allow you to define minimum password length, whether to require numbers in the password, how often to force the user to change passwords, and whether to prevent reuse of old passwords.

A note about the needs of administrators. You may think that you want your network administrator to know your password in case you forget it. This is not the case. A network administrator can delete or reset your password without knowing the original password. How is that secure? Although your administrator could 'break in' to secure accounts, the security breach would be evident as soon as you tried to log in - because they would need to have changed the passwords. This leaves evidence of the breach.

Similarly, when a file is created, altered or deleted it is tagged with the name of the user initiating the change. This also provides a layer of evidence - a kind of a 'paper trail' - for files maliciously or accidentally altered. It's a handy way to answer the question "who deleted that file?"

Access to files and directories can be tailored for each group of users, so that access to accounting data and other sensitive files can be restricted to those people that need it.

In addition to this electronic security, you must have physical security for the server itself - where your data resides. Your server must physically be kept under lock and key to prevent unauthorized people from damaging your data. A lot of damage can be done at the server cabinet, especially if a keyboard is plugged in and an administrator account logged in (a far too frequent situation, in my experience).

Do you have any security horror stories to share? - e-mail me at mhogan@id-8.com.

Michael Hogan, AIA - head chiphead at Ideate, provides custom web solutions and provides consulting services to the AEC industry in Chicago. He welcomes comments by e-mail at mhogan@id-8.com