

## 10 Ways to Protect Your Company From Computer-Savvy Employees

By John B. Gamble, Jr., Esq. and Gregory L. Fordham,  
Certified Computer Examiner

*(This article first appeared on July 27, 2005 in,  
Counsel to Counsel Labor & Employment Law Alert,  
Martindale-Hubbell)*

In the not so distant past, employers could protect themselves when terminating employees by changing locks, monitoring the removal of personal items from desks and lockers, and, if potential violence were a concern, escorting the employee from the premises with security at hand. Today, however, a disgruntled, malevolently ambitious, or resentful employee who is also computer savvy can hurt your company in far more damaging and lasting ways than by simply taking or damaging physical property. Protection of your electronic data when you discharge employees, or when you otherwise lose employees in sensitive positions, has become an essential feature of security in today's world and must be coordinated with conventional defenses against employee sabotage and retaliation.

In addition, when litigation ensues between employees and companies, whether over the validity of the discharge, or over the culpability of an employee for breaching confidentiality, purloining trade secret information or breaching a non-compete agreement, the Company's preservation of electronic evidence is nearly always crucial. Too often employers who become embroiled in such litigation find that the electronic evidence they thought they could rely upon simply no longer exists and cannot be recovered. Or such employers find that the integrity of the evidence has not been preserved, so that it cannot be used effectively in litigation.

In this article, we suggest 10 ways in which employers can protect their electronic information from computer-savvy employees and former employees and preserve critical evidence in the unfortunate event that litigation with such employees become necessary.

**1. Preserve computer hard drives after an employee is terminated or resigns.** When an employee is terminated, many employers reassign the terminated employee's computer to another employee. Indeed, some companies even reformat the employee's hard drive and reinstall application software. Frequently, the result of this serious mistake is either a total loss of electronic evidence of the employee's improper activities, or evidence so badly compromised that its usefulness in litigation is questionable.

Thus, whenever employees are terminated in situations in which litigation (or any other forensic dispute) is possible, the employee's old hard drive should be removed and retained in a secure location with restricted access. Obviously, saving an old hard drive requires some storage space, and disk drives can be susceptible to degradation during long storage periods. If a long storage period is anticipated, or if storage space is at a premium, the hard drive should be imaged and retained in a more durable medium such as a DVD.

## **10 Ways to Protect Your Company From Computer-Savvy Employees**

---

Correctly imaging a hard drive, however, is easier said than done: care must be taken to image the complete drive contents, including free and slack space. Many company IT departments do not realize that such imaging requires the use of forensic grade software instead of the software typically used for replicating workstations. Critically, all forensic imaging, and any and all forensic examinations of the evidence, must be done in such a way as not to change *any* of the *active or deleted* data on the drive, when making images or performing other examinations. Such imaging is best done with the use of *write protection devices* (which prevent the altering of electronic information when imaging is done) by experts who are familiar with forensic procedures.

2. **Preserve server based e-mails.** Just as important as preserving hard drives is the preservation of any and all *active and deleted* e-mails (including e-mails on which the employee is copied) to or from the employee. Such data should be stored in an easily accessible format such as Microsoft Outlook.

The employee's electronic mailbox should, of course, be preserved in its entirety. This should be done separately from the recovery of deleted e-mails, so that recovered e-mail which had been deleted by the employee is clearly distinguishable from e-mails which were still in the employee's mailbox upon termination of employment. (Very often the fact that the employee deleted the e-mail, and the timing of the deletion itself, may be critical in the forensic context.) Some employers will use what is known as an *e-mail migration package* to extract the employee's mailbox from the hard drive data and convert it to a different format. If such a package is used, it should be one which does not alter properties of electronic data such as date stamps, which show the timing of the employee's creation and modification of the data.

3. **Carefully inspect for documents of interest.** The employee's hard drive and e-mails will need to be examined for documents of interest, of course, but this process should never be begun until after both the hard drive and the employee's e-mails had been properly preserved intact, as described above.

Beyond the obvious search for e-mails which are of operational use (e.g., to supervisors and replacement employees), the examiner may need to look for file system remnants, and determine when important files were deleted, or whether the computer was ever *cleaned* or *defragmented* by the employee, possibly to hide evidence of improper use.

An examination for *computer cleaning* can include a determination of whether a software program such as Windows' Clean Manager was run and whether any other artifacts remain of file *wiping software* that may have been used. Another sign of *drive cleaning* by the departed employee could be large volumes of files being created or copied onto the computer, as the process of copying large quantities of new files can overwrite previously deleted files and make them unrecoverable.

If large quantities of files have been deleted, there is reason to suspect that the former employee may have run the *Windows disk defragmenter* to overwrite deletions, thus hiding them and making them harder to recover. Normally, electronic files are stored in contiguous segments

## **10 Ways to Protect Your Company From Computer-Savvy Employees**

---

on a hard drive. Because operation of the computer can result in those files being stored in non-contiguous segments, the *defragmentation* process re-organizes a file's storage locations so that they are once again in contiguous segments. Defragmentation software may also copy files to other areas on the drive before moving them to their final location. As a result, the use of a defragmentation program by an employee trying to hide nefarious conduct can be very effective in making deleted files unrecoverable. Determining whether a defragmentation program has been run should be part of most forensic examinations of the hard drives of departed employees.

There should also be a review of *LNK files*. *LNK files* are Windows shortcuts (links, hence "LNK" files) such as those most users keep on Windows desktops, or on their Start Menus, pointing to specific locations on the hard drive for the convenience of the user. In the case of the terminated employee, detection and review of *LNK files* often help the examiner determine whether suspect documents have been copied or downloaded to storage devices such as floppy disks, zip disks, or home networks.

4. **Practice and monitor good computer security procedures.** The value of good security practices should never be underestimated. Computer security must start with the basics: unique passwords, restricted permissions, frequent changing of passwords, activity and access logging, and logging off when leaving a workstation. Beyond this, a forensic examiner's analysis is significantly facilitated by using information captured in security logs, adding to other evidence found on hard drives and in *active and deleted* e-mails. Security and access logs should be regularly backed up and retained (see discussion below of adequate retention horizons).

The knowledge that good security practices have been followed consistently will enable the examiner to have higher confidence that the improper activity was actually performed by the former employee. For example, if employees are automatically required to change their passwords at frequent intervals (e.g., every 90 days), it is far less likely that improper use of the computer can be attributed to someone other than the employee to whom the computer was assigned. On the other hand, if an employee used the same password for many years of employment, the possibility that others knew the password (and used the computer without the employee's knowledge) increases significantly. And if the improper use becomes the subject of litigation, the employee will very likely argue that someone else had access to and used the computer in question.

5. **Clearly communicate (and verify receipt by employees of all computer-related policies and procedures).** Employee manuals, receipt of which should be acknowledged (in writing or electronically) by all employees, should communicate plainly that company computers are company property, that they are for business purposes only and that the employees should have no expectation of privacy in their use. Employers should also adopt and communicate rules prohibiting the installation of unapproved software, and prohibiting the cleaning or deletion of electronic data before returning a computer to the employer. Employees should be put on notice that employer may monitor and inspect computers at any time, and that exit interviews will include a final computer inspection and review. Employers should specifically reserve the right, and notify employees of their intention, to monitor all computer activities using company equipment and to use *spyware* when deemed appropriate.

6. **Use spyware to monitor and control employee computer use.** As computer

## **10 Ways to Protect Your Company From Computer-Savvy Employees**

usage has increased in the workplace, so have the number of employee distractions with e-mail, internet surfing and computerized games. To counter these problems, software makers have developed employee monitoring programs (commonly referred to as *spyware*) that can be installed on employee machines remotely from a central location. Spyware packages provide a plethora of useful monitoring capabilities: restricting employee access to certain internet sites, preventing installation of other software, logging employee activity and application usage (including video capture of screen activity and even logging every key pressed by the employee during computer operation) and recording all e-mails and attachments that are sent or received by the computer user.

### **7. Establish adequately long horizons for data retention and backup cycles.**

With the advent of electronic discovery, some employers have attempted to reduce the burden of electronic discovery in litigation by reducing the volume of their electronic data archives. Other employers may consider the sole purpose of a data bank to be disaster recovery (i.e., to retrieve data in the event of a fire or hardware malfunction), or they may believe that some kinds of legal liability can be avoided altogether if the backup cycle is kept comparatively short.

In most cases, we think this is a mistake, and we recommend longer retention and backup horizons (in our view, never less than two years, to take into account the possibility of litigation). Obviously, the longer the backup cycle, the more likely it will be that critical evidence for litigation will be retained. This is especially true when examining the hard drive of a former employee several months after his departure upon learning that he has gone to work for a competitor. If the backup cycle is only a few months, plain evidence of a breach of fiduciary duty, or a contractual commitment not to compete or solicit, may be lost forever.

When litigation is expected, and in today's world it must always be considered to be a possibility, applicable statutes of limitation must be considered—other things being equal, longer retention of data is usually better. To avoid any inference or suggestion that the backup cycle is consciously designed to aid the employer in litigation, electronic data should be destroyed (or allowed to be overwritten by other data without a backup), and the length of the backup cycle established, only in accordance with a neutral retention policy supported by sound business reasons.

### **8. Conduct surprise inspections.**

Surprise inspections of employee computers for compliance with organizational policies and procedures and safety and security of sensitive information should be a standard practice assigned to your IT department or others competent to audit compliance with such standards. On the other hand, exhaustive examinations that might interrupt important work or impair productivity are not usually necessary; in most companies, visual examinations of computer file systems, registry contents and e-mail databases will provide adequate coverage.

Two techniques common to the forensic field can be invaluable in conducting surprise audits: *signature analysis* and *hash analysis*. *Signature analysis* is a comparison of file extensions to known *byte patterns* within the file itself. (This enables the examiner to detect changes to a file extension which the user may have made to hide the importance of a file.) *Hash analysis* utilizes a known value determined by a message digest algorithm (an example is the

## **10 Ways to Protect Your Company From Computer-Savvy Employees**

---

*MD5* message digest) to determine changes to the hard drive of an employee, thus revealing prohibited conduct such as the installation of prohibited software. Several forensic tools are available which allow signature and hash analyses to be conducted relatively quickly in a live setting and without having to make an image.

Live inspections can be time consuming and disruptive, and, of course, they alert the employee to the fact that he or she is being monitored, enabling the employee to further disguise his activities; and such inspections can sometimes cause morale problems or generate conflict in the workplace. The number of live inspections needed, however, can be reduced significantly if remote employee monitoring devices (*spyware* discussed above) are used, thus enabling internal auditors to review data files remotely without disruption of the employee's work, and, when necessary or appropriate, without the employee's knowledge.

9. **Consider the risk of new technologies used by your employees.** New technologies such as *PDA*s (personal digital assistants), cell phones, *thumb drives* (tiny devices about the size of disposable cigarette lighters that connect to a computer's USB ports), *wireless networks*, and *instant messaging* are quickly making their way into today's work places. *Thumb drives* provide an easy means for anyone to remove large volumes of sensitive (and perhaps confidential and proprietary) digital data from any computer workstation with a USB port. *Wireless networks* obviously provide another open access point if not properly secured. *PDA*s and cell phones are becoming more problematic from a security standpoint as the two technologies merge and become indistinguishable. *Instant messaging*, which is fast replacing e-mail in many workplaces, typically keeps little or no logs or records of the messages sent. This technology therefore presents a very real capability for the employee who wants to send proprietary information outside the workplace without there being any evidence that the employee has done so.

For many employers the increased use of these technologies is desirable, as they have the potential to increase productivity and to allow flexibility in employee work schedules. But employers should recognize and guard against the security risks of their use; some of these may allow anyone (even a competitor) to obtain data from your employee's computer (for example, by remote access rather than by the use of a cradle device in the work place). The risk of these devices is not restricted to purloining of e-mails and contact lists. *PDA*s based on the Windows CE architecture (a smaller version of the Windows operating system designed for devices like *PDA*s, cell phones and other embedded systems) can even synchronize the contents of internal company folders and files.

These new technologies are a two-edged sword – the decision to use them should be made only after a careful weighing of the significant risks.

10. **Be sensitive to sophisticated smuggling techniques.** As electronic data continues to account for larger and larger percentages of business information, the protection of proprietary and trade secret data has also turned to digital technology. Sophisticated hackers now have access to digital *steganography* and *watermarking*. *Steganography* (literally meaning "covered writing") is the process of hiding information within other information. Digital *watermarking* is a further enhancement to digital *steganography*, which makes the hidden

## **10 Ways to Protect Your Company From Computer-Savvy Employees**

---

information in the digital document resistant to removal of the identification feature.

These digital technologies were originally developed for legitimate purposes: they enable the rightful proprietor of electronic data to hide signature data within digital data files (thus enabling the rightful owner to prove his ownership of the digital data at some future time). Unfortunately, this same technology can also be used to hide customer lists, business plans, and computer source codes in files as innocuous-looking as vacation or family photos that are e-mailed from work to home by an employee before his departure from the workplace (or even from a current employee to a departed employee). Because such hidden data within a photo file is imperceptible to the eye, as is the alteration made to the photo, a reviewer of the data cannot detect its existence without special software and/or access to the unaltered original file.

To guard against the use of these sophisticated techniques for the smuggling of proprietary data, we recommend the installation of *spyware* which that alerts the employer whenever an employee installs unapproved software that has the capability of hiding data by such means, and that can also be used to monitor an employee's improper use of *instant messaging*, *thumb drives*, and *wireless networks*.

### ***In conclusion.***

Although computers and related electronic equipment are the very tools on which organizations must rely in order to keep pace and stay competitive in today's business world, employee misuse of electronic equipment is an increasing threat to company security and survivability. According to the 2004 CSI/FBI Computer Crime and Security Survey, 52% of the responding organizations (which included employers of all sizes) experienced at least one computer security incident from inside the organization, as compared with only 37% of respondents who reported such incidents in the 1999 Survey, a 40% increase. In addition, 269 of the Survey's respondents reported out-of-pocket loss estimates from computer security breaches totaling over \$141 million, more than \$500,000 per respondent. When the Survey's results are viewed by type of incident, those most likely the result of improper employee activities like sabotage (\$870,000), financial fraud (\$7.6 million), insider net abuse (\$10.6 million), and theft of proprietary information (\$11.4 million) account for about one-fourth of the total losses. Clearly, there is more at stake for employers in monitoring and controlling employee computer activity than lost productivity from web surfing and computer games.

The day is past when trade secrets and company competitiveness can be adequately protected merely by requiring employees to execute non-compete, non-solicitation and non-disclosure agreements. Such traditional contractual protections can be of critical importance as a deterrent and in litigation, but now employers must also deploy an arsenal of modern electronic weapons to protect their secrets and retain their competitiveness. In today's electronic world, effective protection against hi-tech fraud, sabotage, or theft must include such proactive weapons as spyware, surprise inspections, and consistently enforced computer security procedures, as well as reactive weapons such as forensic imaging and adequate retention horizons. The importance of deploying such weapons in today's workplace cannot be overstated. Without them, an

## **10 Ways to Protect Your Company From Computer-Savvy Employees**

---

employer's recourse against a computer-savvy former employee may be little more than saber rattling.



John Gamble is a partner in the management labor and employment law firm of Fisher & Phillips LLP. Mr. Gamble received his J.D. degree from Duke University in 1974 and his A.B. with honors from the University of North Carolina-Chapel Hill in 1971. He has practiced labor and employment law representing management interests for over 24 years, and has extensive experience in employment litigation involving the use of electronic evidence. He can be reached via e-mail at [jgamble@laborlawyers.com](mailto:jgamble@laborlawyers.com).



Greg Fordham is the founder of K&F Consulting. He is a Certified Computer Examiner as well as a Certified Internal Auditor and a Certified Public Accountant and has over 20 years of experience in providing litigation support services. Mr. Fordham testifies regularly as an expert witness in the field of computer forensics. He can be reached via e-mail at [greg@knfcon.com](mailto:greg@knfcon.com).