

Article

Data Security—What To Do When An Employee Leaves

Unfortunately for employers, unconditional trust in an employee's honesty is not a luxury any employer can afford. The Computer Security Institute's "2003 Computer Crime and Security Survey" indicates that "theft of proprietary information caused the greatest financial loss" and, additionally, 62 percent of those who responded to the survey reported that an insider was involved in a security incident. That statistic alone should provide the impetus for companies to take precautionary steps when employees leave the company, either voluntarily or involuntarily. To prevent incidents of deliberate sabotage to company data (i.e. destruction, alteration or removal of proprietary information), businesses should make a best practice of following certain key steps to ensure the company information is safe.

Disable Employee Access—PROMPTLY

Employees who leave should have their passwords revoked immediately upon their departure—preferably on their last day of employment. Taking a longer time to secure this step could become a costly mistake if the employee leaves only to access the company's information to destroy or steal from a remote site. Studies have shown that it is quite common for employees to share passwords, which could possibly lead to illegal access. Disabling the password could prevent other unauthorized personnel (who could still be working for the company but may not originally have access to certain sensitive information) from getting into confidential data. Because of the prevalence of password sharing in corporate America, it may also make sense to force a companywide password change on a regular interval, including the day access is revoked from an employee.

Maintain Information On Employee Access

With information stored in a variety of security levels and locations across the network, access rights are numerous. To leave the margin for error as close to nil as possible, it is advisable for a company to maintain a document that lists each employee's access to the company's information systems. The company is then in a position to disable all of the access rights, limiting the error of leaving any access

codes untouched. Having a manager make sure that all access rights are disabled with a checklist that has to be signed for confirmation is another measure to take to guarantee safekeeping of proprietary information.

Conduct Exit Interviews

Businesses that did not possess the foresight to have employees sign a non-compete or non-disclosure agreement in the initial employment stages should conduct exit interviews to remind the employees that company information is confidential and should not be revealed to an outsider. Of course, this practice should be facilitated by a company policy already in place about the prohibition of disclosing company information to outsiders or competitors.

Safekeeping or Imaging Hard Drives

Continued use of the computer includes risk of changing file dates of creation, alteration, access or deletion. Also, any of the following actions could alter evidence of an employee's fraudulent activities or theft of corporate electronic property: turning computer on/off, entering new data, loading new software, compressing data, defragmenting disk and moving data from one system to another.

Based on the above information, it may be good measure for businesses to keep the hard drive(s) of any employee who has access to sensitive information when they leave. This practice will ensure that activities on the computer are not inadvertently erased and should there be a need to investigate a suspect's hard drive for questionable activities, the evidence would not have been tampered with by anyone else.

Another alternative is to image the employee's hard drive. Computer forensics experts can obtain a "mirror-image" of a hard drive and businesses can keep a copy of the imaged drive for a period of time. This recourse will allow continued usage of the original hard drive and still afford employers a copy of the original. If there is a need for electronic evidence discovery in the future, a computer forensics expert can perform the investigation on the imaged drive. As Scott Jones, a computer forensics expert at Forensicon, a Chicago-based computer forensics and electronic discovery firm, says, "Imaging a computer just on the off-chance that a company may someday need the copy of the hard drive may seem like a laborious step, but it is a relatively cheap insurance for any company that has proprietary information that, when leaked out or tampered with, could possibly cost the business great financial loss."

When An Employee Is Suspected of Foul Play...

When an employee who has left the company is suspected of foul play, (i.e. stealing company data, deleting files, sharing information with outsiders), the first thing to do is to turn off the suspect's computer. Activities that occurred on the computer can be traced but the chances of finding evidence could be limited by continued usage of the computer. Companies should hire computer forensics experts to discover evidence on the computer that could prove that the employee did indeed perform illegal activities on the computer.

It is essential to hire third-party experts rather than using the internal IT department personnel because that way they can ensure that the evidence is handled appropriately. Computer forensics experts can maintain a proper chain of custody, avoid data spoliation and authenticate the evidence. Additionally, an important factor to consider is that, unlike internal IT staff, third-party experts do not usually know the suspect personally, reducing the risk of them sabotaging the hard drive to help or to incriminate the suspect.

Computer forensics experts not only extricate electronic evidence, they can work with counsel to ensure that proper steps are taken in compliance with electronic discovery regulations and should the need arise, they are also able to offer expert witness testimony to elucidate the court in the more technical aspects of electronic discovery. The cost of hiring a computer forensics expert could be a factor in the decision, but just contemplate it from this perspective: what would it cost your company if proprietary information lands on the wrong hands?