Global Information Assurance Certification Paper

Employee Right to Privacy, Perceived or Real?

Fred Berryman
22 Oct. 2000

Rising costs related to employee misuse of company facilities has led to increased monitoring activities that may or may not be beneficial to the organization. The Federal government has performed extensive studies that suggest that dissatisfied employees are the biggest abusers of company facilities. According to an article by Compupol, in order to minimize the loss due to misuse of company e-mail systems, playing computer games, shopping, personal relationships, investments, job searches and pornography, employers should develop a computer misuse policy, publicize the policy and get employee's signatures acknowledging the policy. [1]

The Compupol article goes on to say that employers may spend more on litigation than the cost of computer misuse if a written policy is not in place. Even if there is a written policy, the company often pays, even if they win the litigation. Some examples should prove this point. Compaq, for example, fired over a dozen employees for inappropriate web browsing, but they paid for their actions through bad publicity surrounding the issue. Another company fired an employee, supposedly due to financial needs of the company, but a lawyer uncovered e-mail from the supervisor in the case that quoted her saying "fire the bitch, whatever it takes". This written evidence cost the company $250,000.

Fear of litigation should not stop efforts to detect and minimize computer abuse. Omega Engineering in Bridgeport suffered $10 million in productivity losses due to a logic bomb that was unleashed in their system. Employers are responsible for insuring their resources are not used in violations of the law. Managers in higher positions are held responsible for, or were aware of illegal activities in which company facilities were used to commit a crime. [1]

It seems hard for an employer to imagine, but some employees feel they have the right to use company facilities for their own gain or pleasure. One such employee published a web site that teaches others to surf the web while appearing to be working. Since some modern day workers see this as "workers' rights", employers are compelled to fight back by monitoring such activities and following up with disciplinary actions.

What does the law say about employee rights? The Computer Security ACT of 1987 was the result of extensive research into the misuse of government facilities by employees.[2] The ACT takes such abuse seriously due to the potential impact on the security of the nation. Private business should take a similar stance and crack down on computer misuse. They should write policies that detail the acceptable and non-acceptable uses of company facilities and have their employees sign the policy.

It is not enough to write a policy or even have employees sign it. There should be

a security-training program to teach employees in the acceptable use of computer systems. Training gives the employer more legal grounds for disciplinary action, but it also eliminates the need for litigation in many cases. An educated employee, who realizes the importance of misuse, will think twice before making a bad choice. The Federal government spends approximately $15 million annually for training employees in computer security and they estimate a savings compared to the perceived financial loses due to misuse of its systems.

Another set of laws that aid in setting computer use policy is the Wiretap laws, originally written to protect the privacy of individuals using telephones and later extended to include computer messages sent via e-mail and files stored on computers. Brent Johnson discusses wiretap laws in his article "Technological Surveillance in the Workplace". Johnson says 22% of all private companies and 30% of companies with more than 1,000 employees monitor employee actions by searching e-mail, voice mail, computer files and other electronic communications. His article states that illegal interception of live communications may result in criminal and punitive damages, but illegal monitoring of stored data will not result in punitive damages being assessed. E-mail messages captured in transit are covered under the live traffic laws, while computer files are covered under the stored data chapter, unless they are sent as attachments to e-mail. These distinctions in the laws make it necessary are why computer security and use policies need to be specific in what is allowed or disallowed. Company lawyers should be consulted to insure compliance with these and other laws.

State and Federal constitutions provide for a reasonable right of privacy to government employees, but they do not apply directly to private organizations. Therefore, private employers have more freedom to monitor e-mail or search employee's work areas without consequences, but it is still highly recommended that written acknowledgment of such activity should be obtained.

California has written laws, which give employees a certain expectation of the right to privacy in the work place, much like those for government employees, and Colorado has laws concerning common law invasion of privacy. These laws include the unreasonable disclosure of personal information, the unreasonable intrusion into the personal life of another, publicity that places an employee in a false light and outrageous conduct by an employer, which causes an employee stress or harm. Union activities are also covered exclusions of illegal monitoring activities.

Johnson feels it is clear that the further an employer goes with monitoring of employees, the more likely he is to face and lose litigation. If monitoring is to take place, the employer should consider the following. He should define the purpose for monitoring and stick to these activities. Avoid monitoring private communications if at all possible. Obtain written permission from all monitored employees. Inform employees that a password to a computer login does not relay any rights of privacy concerning that computer. Be judicious in the dissemination of any information gained by monitoring activities.

The following is an example computer use policy found in the Compupol article referenced above.

> Many people think data stored on computers, transfers of data between individuals on dial-up modem lines, communications on the Internet, and e-mail are private, and in most cases they are. However, the company reserves the right, without prior notice, to access, disclose, use, or remove both business and personal computer communications and information and will do so for legitimate business purposes.
> Random audits to verify that company computers are clear of viruses and used in accordance with company policy may be performed. Complaints about inappropriate images on computers, inappropriate e-mail or other inappropriate conduct will be investigated. The company may monitor Internet activity to see what sites are frequented, duration of time spent, files downloaded and information exchanged. Computer systems and information are company property and should be used principally for business purposes.
> It is not the company's intention to be "Big Brother." However, it is the company's fiduciary responsibility to establish and enforce policy to help prevent illegal acts, to reduce the risk of liability and business interruption to the company; and to maintain a professional work environment where computer misuse will not be tolerated.

This written policy is a good start, but all employees should sign the policy. Furthermore, a training session should be established in which the policy is explained along with other pertinent computer security issues. The training should be repeated annually and could be incorporated with the annual review of the Equal Opportunity and Corporate Code of Conduct.

[1] CompuPol. "Computer Misuse Well Known Organizations are Experiencing." User Policies Made Easy. URL: http://www.compupol.com/new/misuse.html (22 Oct. 2000).

[2] Aenigma inc. "Computer Security Act of 1987." 8 Mar. 1998
URL: http://www.aenigma.net/resources/csa_87.htm (22 Oct. 2000).

[3] Johnson, Brent T. "Technical Surveillance in the Workplace." 1995.
URL: http://www.fwlaw.com/techsurv.html (22 Oct. 2000).