Employee Monitoring and Surveillance—The Growing Trend

By Robin L. Wakefield, Ph.D., CPA

One natural consequence of recent data security legislation (e.g., the US Gramm-Leach-Bliley Act) is that everyone is now a potential threat to client information. That means individuals both inside and outside the organization. The Safeguards Rule of the US Federal Trade Commission (FTC) establishes standards for the administrative, technical and physical safety of customer records. The objectives of the standards are threefold:

- Maintain the security and confidentiality of client records.
- Protect against internal and external threats to the security or integrity of such records.
- Protect against unauthorized access or use of client records or information that could result in substantial harm or inconvenience to the client.

Consequently, organizations are monitoring their networks in increasing numbers not only to comply with federal statutes, but also to reduce other employee risks.

Can no one be trusted?

Trust is not the issue—client information privacy and security are. Data security laws have effectively elevated the privacy and safety of client information above the privacy expectations of employees. Furthermore, legal experts advise that firms should remove all expectations of privacy in the workplace. They have to, or they risk being found noncompliant with security laws and exposed to other costly litigation. Legal compliance and liability are two of the top three reasons why managers are monitoring employees.[1]

Workplace monitoring and surveillance is a sensible means to comply with federal data security statutes. It also provides additional liability protection for the firm. Monitoring promotes the personal protection of employees by reducing or eliminating instances of workplace harassment. Balancing monitoring and employee privacy is achievable with minimal stress when organizations inform employees of the purpose of monitoring activities, set privacy expectations and create reasonable monitoring policies. Firms that use electronic monitoring and surveillance to comply with the Gramm-Leach-Bliley Act may find that the added benefits (i.e., protecting organizational assets, preventing misuse of company resources and protecting the firm from legal liability) are worth it.

Who Does It?

The American Management Association's (AMA) 2001 Workplace Monitoring and Surveillance Report indicates that 82 percent of responding managers use some type of electronic monitoring in the workplace. As many as 14 million employees in the US (one-third of all employees) are under surveillance in the workplace (*www.privacyfoundation.org*). According to the AMA, monitoring Internet connections remains the predominant surveillance activity (63 percent), followed by storage and review of e-mail (47 percent) or computer files (36 percent), video recording job performance (15 percent), and the storage and review of voice-mail messages (8 percent). The top three reasons for employee monitoring are legal liability (68 percent), security concerns (60 percent) and legal compliance (50 percent). Although electronic monitoring is also implemented for employee productivity and performance reviews, this is a less important motivation. Managers realize that the need to protect the organization from employee activities over firm networks outweighs employee claims for privacy in the workplace.

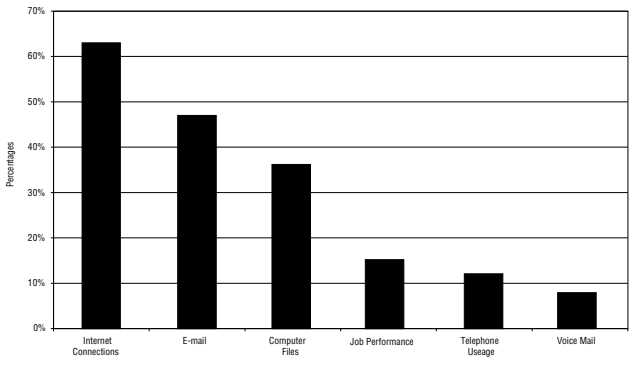
Types of Monitoring

Network Surveillance

Internet activity over corporate networks is the predominant surveillance activity occurring in organizations. Managers find that employer-owned computers and Internet services are being used by employees to facilitate online shopping and to access pornography or other questionable sites. The surveillance of corporate networks can moderate the temptations to use employer resources for personal use and encourage employees to adhere to company policies.

Network surveillance is accomplished by a variety of methods. Software is available that allows supervisors to randomly access employee computer screens or send an employee's monitor display to the supervisor for inspection. Surveillance software can also record every employee keystroke,

Figure 1



including deletions and revisions. Other less intrusive aspects of network monitoring include blocking spam and viruses detrimental to employee productivity and client records.

E-mail Monitoring

A large number of managers indicate that they also consistently monitor e-mail communications. The dynamic qualities of e-mail that have propelled it to record use in business are also some of its vulnerabilities. For one, e-mail is less formal and may be more personal and impulsive. Employees may be sending confidential, sensitive or offensive information across a corporate network with the sincere belief that their communications are private. In reality, e-mail can be easily distributed, copied and read by numerous others without the sender's knowledge. E-mail distributed within a network is stored on the system even though receivers and senders may have deleted the messages. Stored e-mail provides records of communications that can be legally retrieved and printed for review. E-mail is also admissible in court.

Organizations are legally liable for all communications originating from their networks. This puts the firm at risk for lawsuits if employees engage in harassing, profane, discriminatory or illegal communications.

E-mail monitoring software scans employee communications and/or computer files for key words and phrases that may signal unacceptable or illegal messages. In one recent incident, the *New York Times* relates that a sexual harassment suit at Chevron cost the company US $2.2 million when an employee sent coarse messages over the company e-mail system.

Is Monitoring Legal?

As yet, no legislation specifically addresses e-mail privacy and electronic monitoring activities. The US Constitution's Fourth Amendment's guarantees of privacy focus on search and seizure issues that do not specifically relate to computer technology. According to recent actions, courts have not found a reasonable expectation of privacy on the part of employees, but have favored employer rights to protect their interests. Among the reasons given in the *Defense Counsel Journal*: (1) The work is done at the employer's place of business; (2) The employer owns the equipment; (3) The employer has an interest in monitoring employee activity to ensure the quality of work; and (4) The employer has the right to protect property from theft and fraud.[2] In determining the extent of electronic monitoring to undertake, organizations must rely on existing federal and state provisions. In the US, the Electronic Communications Privacy Act (ECPA) of 1986 and recent case law provide some guidance.

The ECPA governs electronic communications and extends the federal wiretap statutes to include other electronic communications. Because the ECPA focus is on conversations, exclusions from the law exist. For example, stored e-mail messages are not considered contemporaneous electronic communications under the Act, as they are not simultaneously sent and intercepted. Organizations with an acceptable business reason may intercept and review employee e-mail transmitted on the firm's networks. The "ordinary course of business exception" makes it easier for employers to prove legitimate business reasons for computer monitoring, especially in light of recent legislation to increase client information security.

Prior court rulings suggest that reasonableness is a standard applying to surveillance and monitoring activities. Electronic monitoring is reasonable when there is a business purpose, policies exist to set the privacy expectations of employees, and employees are informed of organizational rules regarding network activities and understand the means used to monitor the workplace. It is advised that organizations obtain consent from employees regarding monitoring or surveillance activities. Legal advisors suggest that it is essential for employers to demonstrate that monitoring is a routine and known activity in the firm.

Balancing Surveillance and Privacy

Balancing the legitimate need of employers to monitor the workplace with respect for individual privacy is not difficult. The best course of action is to have a monitoring policy and follow it. Legal experts state that "apathy toward e-mail and Internet policies is the biggest mistake an employer can make."[3] It is recommended that firms have a written policy clearly stating that any right to privacy is waived for documents and messages created, stored, sent or received on the firm's computer systems or over its networks.

Achieving balance may require a reasonable monitoring policy that also sets individual privacy expectations. Legal analysts advise that setting policies with clearly stated monitoring intentions is the most important action employers can take to minimize invasion of privacy claims. Clear-cut policies set boundaries, establish employees' expectations of privacy, and help set a workplace tone that conveys organizational responsibility and respect for others. At the minimum, comprehensive monitoring policies should:

- State the specific business purposes for monitoring
- Clearly state the ownership of company computers, networks, files and e-mail
- Clearly outline the forms of communication considered illegal, prohibited and unacceptable
- Clearly outline the web sites considered illegal, prohibited and unacceptable
- Define the acceptable use of company networks and e-mail
- Set clear boundaries for the personal use of company networks
- Inform employees of the specific types of monitoring activities that will be used
- Explain how monitoring activities are advantageous to employees, clients and the company
- Determine the consequences for policy violations

Conclusion

One of the most significant issues facing organizations today is employee privacy. International Data Corp. predicts that e-mail monitoring software will grow significantly, from US $139 million in sales in 2001 to US $662 million by 2006. The protection of organizational interests compels effective supervision of the workplace as firms face an increasing risk of litigation from employee misuse of computers and networks.

Recent legislation such as the Gramm-Leach-Bliley Act also increases the responsibility of firms to guard customers and clients from internal threats. Reasonable monitoring and surveillance activities protect the rights of employees, create a safe work environment, protect sensitive corporate information and assets, and demonstrate compliance with federal laws. Because technology allows employers to reach far beyond reasonable privacy expectations, balancing employee privacy and organizational needs is essential. Establishing clearly written, uniformly enforced and reasonable monitoring policies may be the best protection for firms and employees in a time of ambiguous case law and uncertain court rulings.

Endnotes

[1] Workplace Monitoring and Surveillance Report, American Management Association (AMA), 2001

[2] Adams, Hall; Suzanne M. Scheuing; Stacey A. Feeley; "E-mail Monitoring in the Workplace: The Good, the Bad and the Ugly," *Defense Counsel Journal*, vol. 67, issue 1, International Association of Defense Counsel, January 2000

[3] Ibid.

Robin L. Wakefield, Ph.D., CPA
is an assistant professor of management information systems at Baylor University (Texas, USA). She has published numerous IS-related articles in the *CPA Journal*, *Information Systems Control Journal* and the *Ohio CPA Journal*. Her current research interests include e-commerce, online trust and computer security.

Information Systems Control Journal, formerly the IS Audit & Control Journal, is published by the *Information Systems Audit and Control Association*, Inc.. Membership in the association, a voluntary organization of persons interested in information systems (IS) auditing, control and security, entitles one to receive an annual subscription to the *Information Systems Control Journal*.