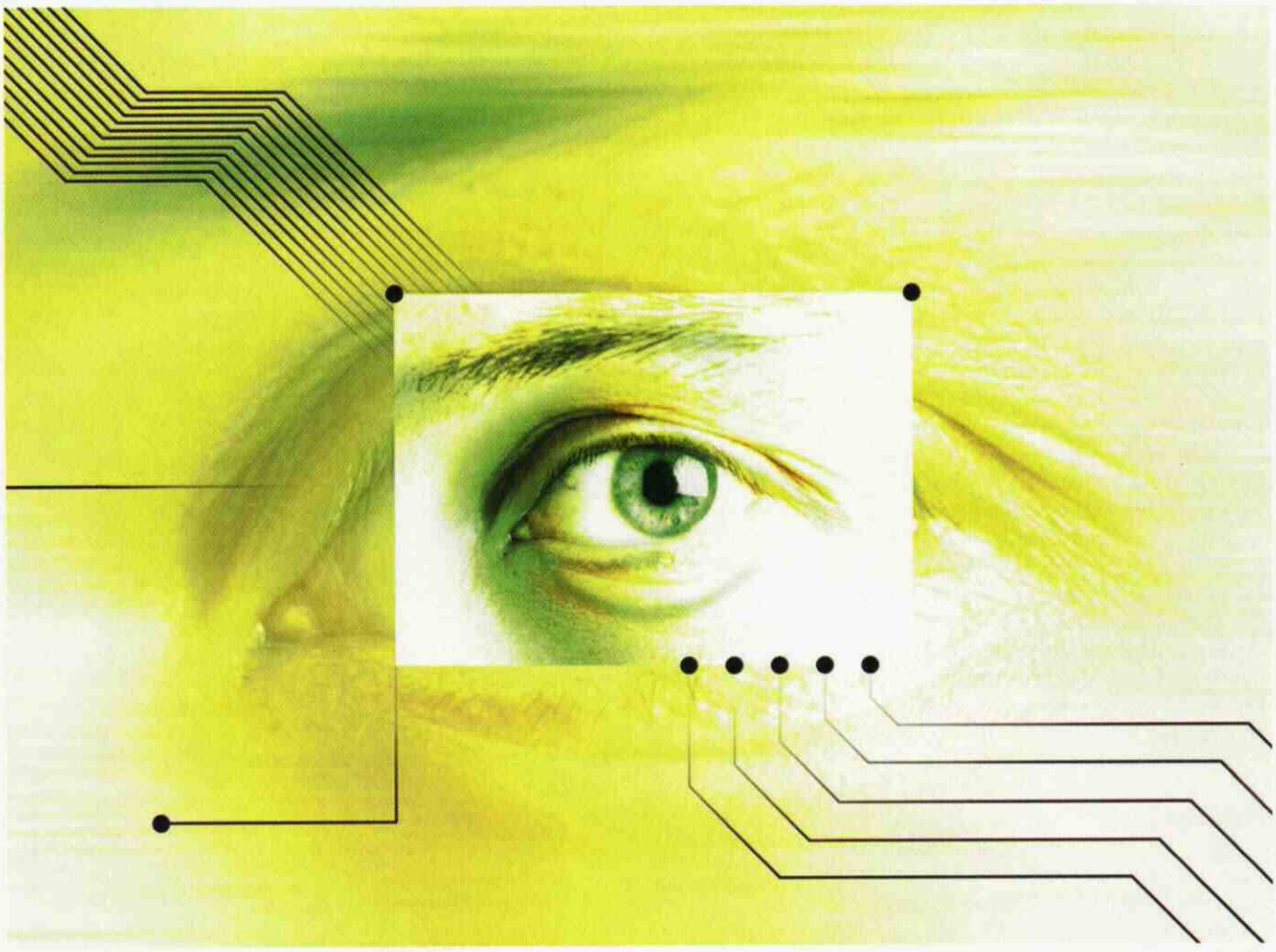

Computer Monitoring and Surveillance

Balancing Privacy with Security

Technology Issue

By Robin L. Wakefield

Information security and employee privacy are important issues facing all organizations. E-mail monitoring software will grow significantly in the next five years, from $139 million in sales (2001) to $662 million (2006), according to International Data Corp. (IDC). Federal legislation mandates that companies actively safeguard personal information. Standards established by the Federal Trade Commission (FTC) focus on maintaining the security and confidentiality of personal records and information, protecting against internal and external threats to the security or integrity of such records, and protecting against unauthorized access or use of personal records.

Whereas past information security efforts centered on protecting systems from external threats (e.g., computer hackers), the risk of internal threats to personal information has spawned both new legislation and new market opportunities. Content and information security services is a burgeoning market that IDC predicts will exceed $23.5 billion by 2007, with a yearly growth rate of 20.9%. This represents a huge opportunity for CPA firms that offer systems consulting, fraud consulting, or assurance

services. Moreover, CPA firms must also determine the extent of their own compliance with information protection laws.

Content Security

Content security involves using electronic means to monitor the transmission and storage of data over a company's network. Content-filtering software can stop spam, scan attachments for inappropriate language, block dangerous attachments, stop intellectual property breaches, quarantine questionable messages or embedded images, and notify systems managers when policies are violated. The potential costs of litigation from adverse network practices underscore the importance of content security. Thomas Shumaker II, an expert in labor and employment law, believes that "CPAs have a duty to take reasonable steps to protect both their employees and their clients. Don't be afraid to monitor the workplace." Shumaker thinks it is critical for companies to realize that they are legally liable for all transmissions within their networks. In one recent incident, reported by *The New York Times*, a sexual harassment suit cost Chevron $2.2 million because an employee sent coarse messages over the company e-mail system.

Employee monitoring is one component of BDO Seidman, LLP's critical anti-fraud procedures (CAP) program. Carl Pergola, national director of BDO's CAP, states that "it is essential for organizations to monitor employees" in order to comply with federal mandates such as the Gramm-Leach-Bliley Act. The content security approach of their CAP program recommends monitoring servers, back-ups, e-mail, and Internet activity, as well as conducting random computer forensics on employee computers. Pergola acknowledges that employee surveillance and monitoring is only one part of a comprehensive program that may also include background investigations, interviews, and fraud education.

Developing an information security strategy that involves employee monitoring requires that the information risks and system controls of an entity are understood. Any strategy requires the implementation of surveillance tools and the development of a monitoring policy that effectively reduces risk and demonstrates compliance with federal laws. A comprehensive content security policy focuses on four areas tailored to the needs, resources, and goals of individual organizations: prevention, detection, investigation, and reporting.

Prevention

Prevention is the main component of an information security strategy. It includes a clearly written and readily available corporate policy that defines information security principles, establishes acceptable and unacceptable practices, outlines criminal offenses, and describes disciplinary actions.

Monitoring is an effective deterrent and detection technique within an overall content security strategy. Prior court rulings suggest that reasonableness is an important standard of acceptable monitoring activities. Electronic monitoring is reasonable when there is a business purpose, when policies exist to set the privacy expectations of employees, and when employees are informed of the rules and understand the means used to monitor the workplace.

One important component of prevention is establishing the business purposes of monitoring, which may include the following:

- Preventing misuse of resources. Companies can discourage unproductive personal activities such as online shopping or web surfing on company time. Monitoring employee performance is one way to reduce unnecessary network traffic and reduce the consumption of network bandwidth.
- Promoting adherence to policies. Online surveillance is one means of verifying employee observance of company networking policies.
- Preventing lawsuits. Firms can be held liable for discrimination or employee harassment in the workplace. Organizations can also be involved in infringement suits through employees that distribute copyrighted material over corporate networks.
- Safeguarding records. Federal legislation requires organizations to protect personal information. Monitoring can determine the extent of compliance with company policies and programs overseeing information security. Monitoring may also deter unlawful appropriation of personal information, and potential spam or viruses.
- Safeguarding company assets. The protection of intellectual property, trade secrets, and business strategies is a major concern. The ease of information transmission and storage makes it imperative to monitor employee actions as part of a broader policy.

A second component of prevention is determining the ownership of technology resources. The ownership of the firm's networks, servers, computers, files, and e-mail should be explicitly stated. There should be a distinction between an employee's personal electronic devices, which should be limited and proscribed, and those owned by the firm.

Establishing ownership reduces employees' expectations of privacy and solidifies the employer's rights. Courts have consistently favored employers' rights to protect their interests given that the work is done at the employer's place of business, the employer owns the equipment, the employer has an interest in monitoring employee activity to ensure the quality of work, and the employer has the right to protect property from theft and fraud.

The acceptable and unacceptable uses of company networks should be clearly described. Boundaries should be set for the personal use of e-mail, the Internet, and downloads. A company should explicitly define what kinds of language, copyrighted material, or images are prohibited from being transmitted over, or accessed via, company networks.

Finally, employees should be educated about the reasons behind information security, including employer and employee protection, relevant legislation, expectations of compliance, and potential consequences. They should also be informed of the specific types of surveillance activities used and how they will affect workflow. Employees should be required to sign a statement agreeing to the specific monitoring activities related to their work and equipment.

Pergola recommends that employers tell employees that monitoring will take place throughout their employment, that it will be random, and that compliance is mandatory. Pergola says that knowledge is key to keeping employees satisfied and productive in a monitored environment. Clearly stating monitoring intentions and obtaining prior consent is essential to minimize invasion-of-privacy claims.

Shumaker also advises that employers reduce privacy expectations by posting their right to monitor the workplace in company handbooks and personnel policies. He says, "It is important for employers to demonstrate that monitoring is a routine and known activity in the organization." Companies are at greater risk when their policies are silent on the issue.

Detection

Detection is an integral part of a content security policy. It involves implementing monitoring methods that effectively reduce risk. Software tools can retrieve employee e-mail, restrict access to Internet sites, record keystrokes, and randomly access employee computer screens. Other tools can screen network transmissions for prohibited words, phrases, or images. Monitoring activities can also be outsourced to a third party.

Well-devised monitoring techniques should detect security breaches as soon as possible. Network controls, supported by company policies, protect both employees and clients and set a tone that conveys organizational responsibility and respect for others.

Investigation

The third area of a content security policy is investigation. The following are important steps in investigating a potential security violation:

- Establish an information security officer or response team to investigate security lapses.
- Develop a plan to obtain legal advice when possible criminal offenses are discovered.
- Prescribe the course of action for different kinds of security violations. Actions might include interviews, collection of evidence, formal reports, or legal conferences.
- Describe the consequences for each level of security breach.
- Determine when police intervention is necessary.
- Establish safeguards to protect employees who raise concerns in good faith.
- Use discretion when addressing anonymous allegations. Weigh the seriousness of the issue and the likelihood of confirming the allegation from credible sources.

Reporting

The final area to address in a content security policy is reporting. A designated security officer or response team should provide formal reports on security breaches, as well as on the actions taken, to the appropriate executive or committee for review. The effectiveness of disciplinary or legal consequences and of the monitoring controls should be evaluated. Information security efforts should be coordinated with the company's internal audit department.

Reducing Risk, Improving Compliance

Information security services is one of the most active areas of the IT services industry. IDC believes that the number-one issue for businesses over the next five years will be compliance with legislative requirements to protect information. Pergola predicts that "as the responsibility for fraud is more clearly defined, surveillance activities and other anti-fraud procedures will only increase." Information security strategies, including network surveillance, will be the principal focus of companies seeking to reduce risk and demonstrate compliance. ❑

Robin L. Wakefield, PhD, CPA, *is an assistant professor in MIS at Baylor University.*