Questions

1. Define the relationship between ethics and the Sarbanes-Oxley Act.
2. Why is records management an area of concern for the entire organization?
3. What are two policies an organization can implement to achieve Sarbanes-Oxley compliance? Be sure to elaborate on how these policies can achieve compliance.
4. Identify the biggest roadblock for organizations that are attempting to achieve Sarbanes-Oxley compliance.
5. What types of information systems might facilitate SOX compliance?
6. How will electronic monitoring affect the morale and performance of employees in the workplace?
7. What do you think an unethical accountant or manager at Enron thought were the rewards and responsibilities associated with his or her job?

* CLOSING CASE TWO

Invading Your Privacy

Can your employer invade your privacy through monitoring technologies? Numerous lawsuits have been filed by employees who believed their employer was wrong to invade their privacy with monitoring technologies. Below are a few cases highlighting lawsuits over employee privacy and employer rights to monitor.

Smyth versus Pillsbury Company

An employee was terminated for sending inappropriate and unprofessional messages over the company's email system. The company had repeatedly assured its employees that email was confidential, that it would not be intercepted, and that it would not be used as a basis for discipline or discharge. Michael Smyth retrieved, from his home computer, email sent from his supervisor over Pillsbury's email system. Smyth allegedly responded with several comments concerning the sales management staff, including a threat to "kill the backstabbing bastards" and a reference to an upcoming holiday party as "the Jim Jones Kool-aid affair." Pillsbury intercepted the email and terminated Smyth, who then sued the company for wrongful discharge and invasion of privacy.

The court dismissed the case in 1996, finding that Smyth did not have a reasonable expectation of privacy in the contents of his email messages, despite Pillsbury's assurances, because the messages had been voluntarily communicated over the company's computer system to a second person. The court went on to find that, even if some reasonable expectation of privacy existed, that expectation was outweighed by Pillsbury's legitimate interest in preventing inappropriate or unprofessional communications over its email system.

Bourke versus Nissan Motor Corporation

While training new employees on the email system, a message sent by Bonita Bourke was randomly selected and reviewed by the company. The message turned out to be a personal email of a sexual nature. Once Bourke's email was discovered, the company decided to review the emails of the rest of Bourke's workgroup. As a result of this investigation, several other personal emails were discovered. Nissan gave the employees who had sent the personal messages written warnings for violating the company's email policy.

The disciplined employees sued Nissan for invasion of privacy. The employees argued that although they signed a form acknowledging the company's policy that company-owned hardware and software was restricted for company business use only, their expectation of privacy was reasonable because the company gave the plaintiffs passwords to access the computer system and told them to guard their passwords. However, a California court in 1993 held that this was not an objectively reasonable expectation of privacy because the plaintiffs knew that email messages "were read from time to time by individuals other than the intended recipient."

McLaren versus Microsoft Corporation

The Texas Court of Appeals in 1999 dismissed an employee's claim that his employer's review and dissemination of email stored in the employee's workplace personal computer constituted an invasion of privacy. The employee argued that he had a reasonable expectation of privacy because the email was kept in a personal computer folder protected by a password. The court found this argument unconvincing because the email was transmitted over his employer's network.

However, according to a news account of one case, a court held that an employer's use of a supervisor's password to review an employee's email may have violated a Massachusetts state statute against interference with privacy. In that case, Burk Technology allowed employees to use the company's email system to send personal messages, but prohibited "excessive chatting." To use the email system, each employee used a password. The employer never informed employees that their messages would or could be monitored by supervisors or the company president. The president of the company reviewed the emails of two employees who had referred to him by various nicknames and discussed his extramarital affair. The two employees were fired by the company president, who claimed the terminations were for their excessive email use and not because of the messages' content. The court denied the company's attempt to dismiss the suit and allowed the matter to be set for trial on the merits. The court focused on the fact that the employees were never informed that their email could be monitored.

This case illustrates the importance of informing employees that their use of company equipment to send email and to surf the Internet is subject to monitoring to prevent subsequent confusion, and a possible future defense, on the part of employees.[7]

Questions

1. Pick one of the preceding cases and create an argument on behalf of the employee.
2. Pick one of the preceding cases and create an argument against the employee.
3. Pick one of the preceding cases and create an argument on behalf of the employer's use of monitoring technologies.
4. Pick one of the preceding cases and create an argument against the employer's use of monitoring technologies.

* MAKING BUSINESS DECISIONS

1. Information Privacy

A study by the Annenberg Public Policy Center at the University of Pennsylvania shows that 95 percent of people who use the Internet at home think they should have a legal right to know everything about the information that websites collect from them. Research also shows that 57 percent of home Internet users incorrectly believe that when a website has an information privacy policy it will not share personal information with other websites or companies. In fact, the research found that after showing the users how companies track, extract, and share website information to make money, 85 percent found the methods unacceptable, even for a highly valued site. Write a short paper arguing for or against an organization's right to use and distribute personal information gathered from its website.

2. Acting Ethically

Describe how you would react to the following scenarios:

- A senior marketing manager informs you that one of her employees is looking for another job and she wants you to give her access to look through her email.
- A vice president of sales informs you that he has made a deal to provide customer information to a strategic partner and he wants you to burn all of the customer information onto a CD.
- You start monitoring one of your employees' email and discover that he is having an affair with one of the other employees in the office.
- You install a video surveillance system in your office and discover that employees are taking office supplies home with them.

3. Spying on Email

Technology advances now allow individuals to monitor computers that they do not even have physical access to. New types of software can capture an individual's incoming and outgoing email and then immediately forward that email to another person. For example, if you are at work and your child is home from school and she receives an email from John at 3:00 p.m., at 3:01 p.m. you will receive a copy of that email sent to your email address. A few minutes later, if she replies to John's email, within seconds you will again receive a copy of what she sent to John. Describe two scenarios (other than the above) for the use of this type of software: (1) where the use would be ethical, (2) where the use would be unethical.

4. Stealing Software

The issue of pirated software is one that the software industry fights on a daily basis. The major centers of software piracy are in places like Russia and China where salaries and disposable income are comparatively low. People in developing and economically depressed countries will fall behind the industrialized world technologically if they cannot afford access to new generations of software. Considering this, is it reasonable to blame someone for using pirated software when it could potentially cost him or her two months' salary to purchase a legal copy? Create an argument for or against the following statement: "Individuals who are economically less fortunate should be allowed access to software free of charge in order to ensure that they are provided with an equal technological advantage."