Privacy in The Office

Craft procedures for a reasonable privacy regimen

I always wanted to be a screenwriter, and one of my favorite shows is "The Office." My recent idea was an episode where Jim Halpert and Pam Beesly (known to play practical jokes) tell Dwight Schrute that corporate has been monitoring the Internet and e-mail activity of its employees. Dwight suddenly becomes afraid that people will discover his obsession with fantasy role-playing games and his relationship with Angela Kinsey (a co-worker).

Expert Advice

Ronald Raether

When Dwight begins sneaking around and making inquiries to his boss, Michael Scott, I can just picture the chaos and laughter that follows.

For real businesses, the above scenario could turn into a human resources nightmare and possibly a lawsuit. While the Fair Credit Reporting Act, Health Insurance Portability and Accountability Act, Ohio Revised Code 1349.19 (breach notification act), and other privacy rules and regulations may not be familiar to many companies, these laws likely apply.

Let's take the above as a hypothetical and assume that corporate was monitoring the web usage of its employees (a growing practice). Dwight has signed up to access his medical records online, and these records are accessed and reviewed by a monitoring tool. The monitoring tool stores and logs the data. Who has access to all this information? Is the Electronic Communications Privacy Act, the Computer Fraud and Abuse Act or the Stored Communication Act implicated? What about HIPPA? Forget about the pure legal questions and imagine the CEO or union leader being informed that their health records (you can be creative here) were just stolen by a criminal and thus could be available to millions of people on the Internet.

The above questions may seem theoretical, but indeed the law is already being tested in this area and the results raise serious questions. For example, a Federal appellate court has held that a party can be liable for unauthorized access to employee's private email messeges. Tbeofel v. Farey-Jones, (U.S. App., 9th Cir., Aug. 28, 2003). Two weeks ago, the same court found that an employer can be held liable under the Stored Communication Act for acquiring transcripts of private messages sent to a pager issued to the employee by his employer. Although the employer paid for the pager and up to 25,000 characters' worth of messages a month, the employer (a police department) did not have the right to view the content of the messages when evaluating whether to change the 25,000 character limit. Quon v. Arch Wireless Operating Co. Inc., (U.S. App., 9th Cir., June 18, 2008).

The above may seem too high-tech for many companies. However, employee privacy also extends to physical theft. The recent burglary at Colt Express Outsourcing Services provides a perfect example. Burglars stole computer systems from the company, which administers benefit plans for CNET and other clients. The computers contained the names, birth dates, Social Security numbers and beneficiary information for 6,500 employees enrolled in CNET's health insurance plans. Colt Express was going out of business and as a result CNET had to notify its employees of the breach and provide credit monitoring services.

So the issue has been identified, and the next step is to figure out where to start. The answers will depend on the nature and circumstances of the business and what information is being maintained and monitored. I suggest analyzing 10 areas to begin this analysis. Here they are:

1. Governance and policy: Does privacy governance include Human Resources as a key stakeholder?
2. What data do you have: Do you know all the types of HR data, where it is located, and who has access to the data?
3. Outsourcing and vendors: What do you outsource and what are the privacy practices of the vendors?
4. Security and access control: What measures are in place? For example, when at rest, is HR data encrypted? Encrypted in transit?
5. Record retention: When was the last time the policies were reviewed? Do the retention policies address privacy?
6. Mergers and acquisitions: Do the teams consider privacy, especially as to employee records?
7. Globalization: How do you track virtual employees, and what are the privacy concerns for such employees? Do you have any global workforce and are you tracking the laws of those countries?
8. Incident response: Do you have a documented and tested plan for responding to an HR privacy incident?
9. Training and awareness: Do you have a consistent, ongoing privacy training regimen, and where does HR fit into this program?
10. Review and assessment: Do your review programs and internal auditing include HR privacy issues?

The above covers much ground. For companies that have not even begun to consider privacy as an issue to their businesses, the above can seem overwhelming. However, with the right personnel and the proper tools, companies can begin to respond to these questions and craft a set of process and procedures that provides a reasonable workplace privacy regimen.

With a little preventative action, employers can protect themselves against avoidable exposure and provide a work environment that reassures its employees that their privacy is being protected. When the inevitable workplace privacy breach occurs, you will be prepared to answer the questions around what have you done to prevent protect your employees' personal information.

Ronald Raether *is a partner in the Dayton law firm Faruki Ireland and Cox P.L.L. Reach him at rraether@ficlaw.com.*