
Maintaining Vigilance By Means of Secure Records Management

Without strict policies, many common scenarios can place personnel records in jeopardy. For example, the CEO and Chair of a large publicly traded company had his Social Security number stolen and used to open credit cards. The breach happened when an attorney working on the renegotiation of the CEO's contract left the CEO's personnel file on the floor by his desk. A temporary cleaning service worker photocopied the information and sold it on the street for \$75.

A chemical company that prided itself on security had a breach in one of its offices when a security guard was given a master key to the HR office that allows the guard to open any door in case of emergency. After entering the HR office, the security guard broke the lock on a worn cabinet where personnel files were stored. After taking some of the information in the file, he sold the personal information for \$50 each.

Philip Deming, an expert investigator and fixer of personnel breaches has identified what he believes are the three biggest threats to personnel records: cleaning staff, security staff and human resource information systems staff.

These groups tend to be invisible and may not even be a part of the company. Records security is more a matter of common sense than high dollar security systems such as hidden cameras. Mr. Deming suggests having a high-level employee present when cleaning crews work. Only the HR director and perhaps one other senior executive should have a key to the HR office.

He also suggests that one qualified person in HR or IT provide oversight for electronic data. The probability of a security breach would suggest going paperless, because electronic files are more secure. To maintain the tightest security of electronic files that contain personnel information, the following is recommended:

- Change computer access codes frequently
- Personnel information should never be sent over e-mail or discussed in cell phone calls
- Computers should go into "standby" mode and require a password after not being touched for a certain period of time
- Work with IT to restrict information from being downloaded onto laptop computers

The consequences of security breaches can be devastating to any organization. Without strict policies, common sense records security, and everyone maintaining vigilance, many previously assumed "safe" procedures can place personnel records in danger of unauthorized access.

What This Means For Counties

Counties need to address records management in their policies and procedures if they have not already done so. Restricted access is recommended to curtail breaches in security. Security breaches such as leaving a file unattended or bringing a non-employee into a secure area should be aggressively addressed. In addition, written policies should outline the consequences for privacy violations.

For more information, contact CTSI at 303-861-0507.