Make sure employees know you're monitoring

If some of your employees have access to sensitive information such as customer contact lists and spreadsheets of employee data, you may have been more than casually interested in recent news reports about data leaks from the vaults of the National Security Agency.

If NSA spies can't keep information secure, what chance does a private employer have?

Data breaches can compromise personal safety, cost millions of dollars and expose organizations to crippling legal liability.

Few HR pros relish the thought of playing Big Brother. However, safeguarding sensitive data relies on being able to monitor employees' use of your computer systems. In turn, you have an obligation to notify employees that you are watching what they read, write, download and upload. Just knowing that you intend to monitor may stop employees from misusing your computers.

Inform employees that the company owns and controls the equipment they use for work-related activity. Tell them you will monitor any and all of their activities while they use that equipment. You're on solid legal grounds to do so. Courts have generally upheld the rights of employers to control their equipment and limit its use.

Make sure employees understand that you may read emails, text messages and other documents that employees may create, copy, receive, send or print using your equipment.

Stopping data breaches involving employees' own phones and computers is trickier. Ask your attorney to draft a data security agreement covering what employees can and cannot do using their own devices.

If you track workers' locations or movements using GPS systems in company-owned vehicles (or smartphone apps) ask your attorney how to structure your monitoring program and notify employees about it.

7600 Leesburg Pike, Suite 300, Falls Church, VA 22043-2004 (800) 543-2002

© 2022 A *Business Management Daily*