BUSH LAW FIRM P.C.

Labor and employment law for business leaders.

December 4, 2012

Embezzlement Is Old School — Employee Data Theft

Data theft is a company's biggest weakness to fraud—beating out embezzlement for the top spot. That's according to the US senior executives who were surveyed for the Global Fraud Report issued by Kroll Advisory Services. You can find the report here. And employees "are far more often to blame for the loss of information than hackers."

Employees most often steal trade secret data to use it on their next job with a competitor. Everything from sensitive technical to business information can be vulnerable. Your competitor has no business learning your secret playbook by hiring away a key employee.

A federal jury recently convicted a former GM engineer and her husband of stealing technical trade secrets for possible use in China. Here's the story.

Solid HR practices help keep your secret playbook out of your competitor's hands:

- Non-compete agreements call jobs with a competitor off limits where an employee could benefit most from stealing trade secrets.
- Reasonable security measures give you the best shot at qualifying sensitive information as trade secrets.

Alan Bush
281.296.3883
abush@bush-law.com

Bush Law Firm
bush-law.com

HR Risky Business
For more insight into how solid HR practices impact your company's strategic operations, visit Alan's employment law blog at hrriskybusiness.com.

Texas Non-Compete and Non-Solicit Agreements

Business secrets

Confidential information

Non-compete agreement

Trade secret

- Exit interviews about a departing employee's next job can help spot the folks at highest risk for trade secret theft.

- Forensic IT triage can pat down a high-risk former employee's work computer for digital trade secret theft.

BUSH

LAW FIRM

P.C.