Five ways to counter insider threats

Howard
Solomon

A lot of attention is being paid to hackers who have broken into high-profile companies in the past 12 months, but CSOs shouldn't forget that insiders are a big threat.

What to do about them is the other source of worry of chief security officers. Having managers well-trained by HR on ways to avoid creating disgruntled employees is one tactic, but sometimes a staffer can't be mollified.

So here's a list of suggestions I found on CSO Online on what to do that was compiled by endpoint security solution vendor CoSoSys, after a customer survey.

1. Check what documents employees have access to: Six out of 10 employees are not aware which files are confidential. Limit permissions so employees only have access to the data necessary to get their jobs done. Users with access to sensitive or confidential data should be trained to recognize which files require stricter protection.

2. See what tools employees are using to share files: 45 per cent of insiders admit copying work files to personal computers or remotely connecting to the company network from home to continue working.

3. Create a short quiz to find out employee's knowledge regarding data security: 35 per cent of employees believe it's not their responsibility to protect data.

4. Find out if your current security tools can detect a breach caused by insiders in case it happens: Over half of employees indicate they've accidentally sent emails to the wrong person.

5. Remember how much an average cost of a data breach costs. Hint: US$3.5 million.