WHAT'S YOURS IS MINE:

How Employees are Putting Your Intellectual Property at Risk

The Game

Employees regularly take IP outside the company and never clean it up

2 out of 5 download work files to personally owned tablet or smartphone

One-third move work files to file sharing apps without permission

Most employees think it's OK to use competitive data taken from a previous employer

Half of employees who left/lost their jobs kept confidential information

40% plan to use it in their new job

Future employers become unwitting recipients of stolen IP

Employees think they own the IP

56% of employees do not believe it is a crime to use a competitor's trade secrets

44% believe a developer who creates source code for a company has some ownership of his work

42% do not think it's a crime to reuse this code for other companies

Employees don't think their organizations care

Half say no action is taken when employees take sensitive information against policy

68% say their company does not take steps to ensure employees do not use competitive info

START OVER

Continue To RECOMMENDATIONS

A multi-pronged approach

1. Employee education:
Let your employees know that taking confidential information is wrong. Make IP theft awareness integral to security awareness training.

2. Enforce NDAs:
Make employees aware that policy violations will be enforced and theft of company information will have negative consequences to them and their future employer.

3. Monitoring technology:
Learn where IP is going and how it's leaving your network. Deploy Data Loss Prevention technology to notify managers and employees in real-time when sensitive information is inappropriately sent, copied or otherwise wrongly exposed.

Symantec. **Ponemon INSTITUTE**