Privacy Liability

Companies Bleed Data as Workers Move It Offsite

THE MORE employees are working from home, the greater the risk that their employers' sensitive data is also being stored on their poorly secured devices and laptops.

A new study by Symantec Corp. found many workers are sharing, moving and exposing sensitive company data as part of carrying out the requirements of their jobs, and they may not realize they could be compromising the information or that what they are doing is wrong.

More worrisome, the study found that half of all employees surveyed who left or lost their jobs in the prior 12 months had kept confidential company data. When that happens, the departing worker, your company and the new employer are all put at risk.

How Data Leaks from Your Firm

- Workers move it to their personal devices, both mobile and at home,
- Employees transfer the data or save it on cloud services or personal hard drives, or
- Employees take data with them to their new jobs.

Worse still, the majority of employees put these files at further risk because they don't take steps to delete the data after transferring it.

"In most cases, the employee is not a malicious insider," writes Symantec, "but merely negligent or careless about securing IP. However, the consequences remain. The IP theft occurs when an employee takes any confidential information from a former employer."

Why Data Leaks from Your Business

- 47% of employees say their organization doesn't take action when employees take sensitive information offsite.
- 68% say their employer does not take steps to ensure staff do not use confidential competitive information from third parties.
- 56% do not believe it is a crime to use a competitor's trade secrets.

What you can do

Symantec suggests attacking the problem from multiple angles:

- **Educate employees** – You should take steps to ensure that IP migration and theft awareness is a regular and integral part of security-awareness training. Create and enforce policies dictating how they can and cannot use company data in the workplace and when working remotely.

Help employees understand that sensitive information should remain on corporate-owned devices and databases. Also, new employees must be told that they are not to bring data from a former employer to your company.

- **Enforce non-disclosure agreements** – If you have not done so already, you need to craft new employment agreements to ensure they include specific language on company data.

They should include language that the employee is responsible for safeguarding sensitive and confidential information (and define what that is).

For employees that are leaving your employ, conduct focused conversations during exit interviews and make sure they review the original IP agreement. Include and describe, in checklist form, descriptions of data that may and may not transfer with a departing employee.

- **Track your data** – You need to know where your data is going and how you can find out by using monitoring technology. One option is to install data-loss-prevention software that notifies managers and employees in real time when sensitive information is inappropriately sent, copied or otherwise improperly exposed.

Also introduce a data-protection policy that monitors inappropriate access or use of company data and notifies the employee and you of violations.

This increases security awareness and deters theft. When you know how data is leaving your company, you can then take steps to prevent it from seeping out. ❖