THE THREAT FROM INSIDE

TECHNOLOGY

Companies face serious risks from employee intellectual property theft. To protect themselves, they need strong onboarding and exiting policies, plus computer forensics expertise.

TRAVIS RATHBONE FOR *FTI JOURNAL*

Across the globe, cyber attacks from outside the company get enormous attention. But much less attention is directed toward an equally perilous — and possibly more daunting — threat: employees absconding with intellectual property and other confidential information.

Since the economic downturn, cases of intellectual property theft by employees have been increasing significantly. A recent study by the U.S. Federal Bureau of Investigation found that 44% of companies it studied had experienced internal theft of intellectual property. Fearful of losing their jobs, some employees become desperate, and one way of protecting themselves is to walk off with information that would be valuable to a competitor — for example, lists of top customers, pricing schedules, strategy documents or computer code.

Helping oneself to company information is getting easier. Whereas pilfering information once meant photocopying it and sneaking it out, today more than 80% of a company's

JAMES SCARAZZO
Director, FTI Technology, FTI Consulting
jim.scarazzo@fticonsulting.com

JASON RAY
Director, FTI Technology, FTI Consulting
jason.ray@fticonsulting.com

information is stored electronically. Some 75% is never printed. As employees bring their own mobile devices to work and make use of "the cloud" to store and exchange information, it can leave the company's control in seconds.

Employee intellectual property theft is difficult to detect. A company's workers have legitimate access to proprietary information as part of their work. For example, few would question a sales representative's copying contact lists, presentations or other material for easy access outside the office. Thus, employee theft of intellectual property often flies below the radar. Here are two examples of FTI Consulting projects:

- An industrial equipment manufacturer discovered information theft only after its suspicions were aroused by the resignation of the sales vice president and several direct reports all on the same day. They had formed another business and were using sales contacts, pricing models and other information to build it.
- Members of a financial services firm were conspiring to set up a competing business with confidential client information. They shared their plans through text messages on company-owned smartphones.

Because so much company information is used legitimately outside the office, it is practically impossible to set meaningful alarms.

No company is immune to these attacks. Because so much company information is used legitimately outside the office, it is practically impossible to set meaningful alarms. But companies can better protect themselves. Management teams should tighten employee onboarding and exiting processes, and put proper forensic computer procedures in place.

ONBOARDING AND EXITING

When companies bring on new employees, the process should thoroughly cover company policies on intellectual property and confidentiality. Ideally, these policies would be included in employment contracts and confidentiality agreements. Continually articulating these policies is crucial. It makes the company position clear and supports legal actions in which employees claim policies were vague.

The employee exit process is also an effective point for heightened scrutiny. Although it is not practical to conduct forensic computer investigations with every employee departure, management should identify key positions with potential risk. These could include sales representatives, whose contact lists often contain customer data that is protected by privacy laws, but also any employees with access to proprietary

The views expressed in this article are those of the authors and not necessarily those of FTI Consulting, Inc., or its other professionals.

or confidential information that they might use after leaving.

MAKE SURE INFORMATION WORKS AS EVIDENCE

When companies suspect employee intellectual property theft, they often move hastily: IT or HR is contacted and the staff springs into action by opening files and saving information onto CDs or portable devices. On the surface it may appear that the evidence has been obtained. But in actuality, all the company has is data. That probably isn't usable as evidence.

Evidentiary standards require detailed chronological documentation of everything that happened to the data. Opening, printing and saving files can permanently change metadata that records who did what to the file and when. Just booting up a computer can overwrite items such as caches and temporary files. Combined with altered metadata, these changes can make it difficult to prove what the employee actually did.

Opening, printing and saving files can permanently change metadata that records who did what to the file and when.

Sometimes computer experts can restore damaged evidence, but just as often they can't. The process can be costly and take valuable time. To avoid the fire drill, management should be certain that proper computer forensic skills and processes are in place.

MOVE QUICKLY TO ACTION

Stolen intellectual property can improve with age — the people who have taken it have more time to use it. Quickly understanding the facts and having reliable evidence allow management and legal teams to decide early what steps they can and should take. For example, the company could file for a temporary restraining order, pursue court orders to examine personal computers, or simply contact the employee's new employer and inform the company of what has occurred. It is also valuable to tightly integrate computer forensic activity with other forensic processes in the company, such as accounting. Evidence of fraud or other misconduct is likely to be found in computer files and electronic communications. Early, coordinated and immediate action may be necessary to discover evidence and prevent its destruction.

In times of economic distress, the incidence of employee intellectual property theft by employees can jump. Although such theft is difficult to detect, companies can take steps to protect themselves and make strong defensive moves when theft is suspected. ■