ForensicsConsulting Solutions, LLC™

Best Practices when Employee Intellectual Property Theft is Suspected

Let's be honest! The "Best Practice" for Intellectual Property is not to lose it in the first place. Ensure proper security controls or countermeasures are in place to avoid, detect, and minimize theft of Intellectual Property. Prevent employees from copying or emailing sensitive company data, maintain logs of file access, and watch for suspicious activity. But if you suspect that IP theft has been committed in your company, follow these simple guidelines:

1. **Preserve the evidence** – Be sure you have collected all of the suspected employee's electronic devices, including laptops, desktops, cell phones and USB devices prior to their departure.
    a. **Do Not** allow the suspected employee's devices to be re-issued to a new user until you have verified that no data has been taken or you have the drive imaged by a Computer Forensic Expert.
    b. **Do Not** allow the suspected employee to take these devices home and return them at a later date. Doing so may result in the loss of data and could compromise an investigation.
    c. **Do Not** allow anyone to turn on or access the devices as this could compromise the defensibility of the investigation or damage the evidence in it's as-is state.

2. **Hire a professional** – Sleuthing by non-professionals can damage evidence. Jim the IT manager may be very intelligent, but he's not a Forensic Examiner. And Jim may also be best buddies with the IP thief, effectively "helping" him remove telltale evidence from the devices. An outside investigator can provide a clear, untainted opinion of the case, and may well be important when it comes time to testify.

3. **Find the Smoking Gun** – A digital Forensic Examiner can identify a great many things pertaining to data theft. You can assist him by providing a clear timeline of events such as hire date, fire (or departure) date, and how long suspicious activity was noticed. Be prepared to provide the forensic expert with login information, passwords and any other user account details that may be relevant. If the employee went to work for a competing company, provide that information to the expert so he can search for evidence of communication with that company or the people who work there.

4. **Take Action** – If IP theft is confirmed, be prepared to take the appropriate legal action that you and your legal advisor deem necessary. This may include prosecution or other legal action.

2600 N. Central Avenue, Suite 700 • Phoenix, Arizona 85004 • 602.354.2799 • Fax 602.54.2754
www.discoverfcs.com