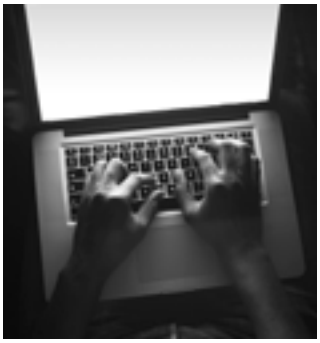
AVALONCyber

Case Study: IP Theft – Former Employee Steals Company Data For New Employer



Avalon was requested to perform a forensic analysis of a laptop that was utilized by a former employee of a telecom provider and who had resigned to take employment with a direct competitor. As with all of these types of non-compete labor prosecutions, it is extremely valuable to obtain independent forensic evidence of actual exfiltration of corporate data that can assist in determining actual damages or value of the claims of the former employer. This evidence is also extremely valuable in obtaining the temporary or permanent relief such as court-imposed injunctions or restraining orders.

The files that were accessed contained highly valuable pricing models, client contracts with values, and confidential supplier data.

The Challenge

Avalon had to prove, with a high degree of forensic certainty, that specific corporate data, intellectual property, and/or competitive business intelligence data were exfiltrated from the company systems by the former user.

The Strategy

The laptop, desktop, and corporate file server authentication log data from the former employer were forensically collected and preserved by Avalon. Avalon used a forensic analysis of the laptop to recover evidence indicating that, in the evening prior to providing notice of his resignation, the user was logged onto the network after hours and was accessing numerous proprietary corporate files. This was very unusual based on the user's normal work history. The network files that were accessed contained highly valuable pricing models, client configuration files, client contracts with values and expiration dates, and confidential supplier data files. Further analysis revealed that the user was logged into his Yahoo! e-mail account at the time he was accessing the files. Avalon was able to confirm that several e-mails were sent from his Yahoo! account with numerous attachments containing the corporate data.

The Results

There were three significant outcomes of the forensic investigation.

1. Counsel obtained a court order that compelled the former employee to produce his Yahoo! credentials for forensic collection and analysis. Upon review of the collected e-mail data, Avalon determined that after the user received the e-mails with attachments containing data from the former employer, the user subsequently forwarded those e-mails to the new e-mail address. Evidence revealed that the user also forwarded some of the e-mails and attachments to other principals of the new employer.

2. Counsel obtained a court order that compelled the former employee and an additional employee of the new employer company to produce their current employer-issued computers for forensic collection and analysis.

After Avalon forensically collected and preserved the digital devices and began the forensic investigation, it was apparent that prior to providing them to Avalon, both employees had taken significant steps to erase numerous files and e-mails relevant to litigation from their systems. Avalon successfully recovered the majority of the deleted data and produced to counsel for review. Another expert affidavit was prepared and a Spoliation Motion was prepared.

3. Based upon the expert affidavit and a Spoliation Motion brought by plaintiff counsel, the court struck the Answer of the Defendants establishing complete liability. The case for damages is still pending.

AVALON Cyber

QUESTIONS?

For more information on any of our services, please contact:

Ian Gattie
Director of Marketing
716.995.7777
ian.gattie@teamavalon.com