Case Study – Corporate Espionage Countermeasures & Debugging

1 THE CLIENT & REQUIREMENTS

We were contacted by a major energy firm with worldwide operations and an employee who brought possible corporate espionage to the attention of top level management. The client minimized involvement of upper management in working with us because the employee indicated upper level misconduct.

The indications were that critical and proprietary information was getting out to a single competitor employing past members of our client's management. The suspected person was an Executive Vice President, so this was a sensitive and covert countermeasures and debugging operation. Sensitive and highly valuable seismic information was getting out of the company. This included surveys, and geological and seismic studies that help energy companies to locate areas with oil and gas deposits justifying a full scale drilling operation.

The client wanted Kimmons Investigation Services, Inc. to pinpoint how information was leaking and leverage our investigative skills in getting to the root of all spying and determining the extent of the damage and all people involved. Unlike many TSCM, Technical Surveillance Countermeasures, companies, Kimmons Investigations employs trained investigators, many previously employed by the

government or police forces. This allows us to not only discover and dismantle covert surveillance, but also to investigate those involved and discover other possible threats through that investigation.

2 WHERE WE SWEPT FOR BUGS

We concentrated on the executive offices of not only the suspected person, but also all other top level management personnel. This isn't necessarily due to a suspicion that others were involved. We must determine everywhere the suspected spy may have located bugs and covert surveillance gear to monitor communications and steal vital information.

3 WHAT WE USED – EQUIPMENT

Oscor Spectrum Analyzer

This highly sophisticated analyzer is quite expensive, and many TSCM companies simply do not expend the funds to employ it. The problem is that it's one of the most effective tools available to scan spaces for radio frequency and other bugs based on their emissions and transmissions.

Using this tool, we are able to ascertain that device(s) exist, and sometimes their exact location. However, just knowing they're present, we can employ another highly effective tool to zero in on their precise locations.

Non Linear Junction Detector

A Non-Linear Junction Detector detects the presence of electronics, regardless of whether the electronic target is radiating, hard wired, or even turned off.

The ORION 2.4 locates hidden electronics in walls, floors, ceilings, fixtures, furniture, or containers. An antenna-mounted line-of-sight display lets the operator focus on the target while sweeping. The NEW ORION 2.4 transmits at 2.4GHz frequency for detecting small electronics such as SIM cards and cell phones.

4 WHAT WE FOUND – SWEEP & INVESTIGATION

In our sweep of the executive offices, we found a phone tap on the CEO's phone. This tap enabled the covert recording of any or all conversations the CEO had over the phone. We pinpointed the location of the bug and eliminated it. Most TSCM companies would be done at this point, leaving further investigation of the suspected party up to others or law enforcement.

Kimmons Investigation Services, Inc. is a full service TSCM and private investigations company. We moved forward at the request of the client with interviews of the VP as to why he was engaged in these activities and where the information was being delivered. It seems that he was funneling information to another new company formed by ex-employees of the client. They were paying handsomely for the information, but there was more.

This Executive VP, other than the money motive, was focused on helping to build up the competitor company and leaving to run it at some point in the near future. This operation was well-planned and executed covertly. Small mistakes led to another employee's suspicions, and this employee started the ball rolling with a tip to management.

If you have concerns about leaks of proprietary information in your organization, call or email us immediately for a private consultation to determine how we can help.

KIMMONS INVESTIGATION SERVICES, INC.
3033 Chimney Rock, Suite 200
Houston, TX 77056
Phone#: 713-532-5881
Fax #: 713-266-4002
State Licensed for over 30 Years

Email Rob Kimmons