Investigating I.P. Theft

By: Dennis P. Farley and Jack Mattera

TheIntelligenceGroup®
RESEARCH ▾ INVESTIGATIONS ▾ FORENSICS

While most legal professionals think of external hackers when they hear about information theft, that's often not the case. The more common culprit: someone with legitimate access to the information - i.e., insiders.

Common insider methods include:

- Internal theft of technology or business plans.
- Employee theft of customer lists.
- Leaking of non-public financial data.
- Vandalism of information systems.
- Infiltration by competitors.
- Tricking employees into providing information by misrepresentation, e.g., pretending to be I.T. staff. Identity theft.

Responding to a Loss

Investigating I.P. theft uses classic investigative techniques, but with different tools. Like any crime, the factors of need, opportunity and rationalization must be evaluated. But the key focus - opportunity - is where the techniques of the investigator must be appropriate and up-to-date. Forensic computer investigation, e-mail screening, and network/workstation monitoring, can be critical to find evidence of wrongdoing.

Forensic computer investigation is the most valuable of these techniques. Evidence of wrongdoing - the "fingerprints" and "footprints" of fraud or theft recorded on electronic media - are very difficult to erase or hide. A well executed forensic computer investigation can recover all data recorded on a computer hard drive (or other media), including anything deleted by the user.

Commercially available (and proprietary) software tools can help investigators evaluate electronic media on a bit-by-bit basis, and reconstruct key strings of information, if not entire documents. Time frames can be determined such as dates of document creation, alteration or destruction. Caveats exist, obviously, as documents can be partially, if not entirely, overwritten the longer a machine has been in use.

Basic Steps

To conduct a successful investigation, basic steps must be followed:

1. *Don't turn on the machine.* If the media to be evaluated is a computer hard drive, don't turn on the machine. In most Windows-based platforms, starting the machine writes to the hard-drive, and you've just introduced doubt into the integrity of the evidence. Don't give opposing counsel extra opportunity to challenge the results of the investigation.
2. *Preserve the chain of evidence.* If litigation has not yet been started, assume it will be. Documenting a chain-of-custody is consistent with sound evidentiary procedures and will help resist challenges from opposing counsel.
3. *It's (probably) not a job for your I.T. staff.* Forensic computer investigation is a highly specialized field, with skill requirements not typically met by network administrators or information security specialists. Certification in this field, other than software specific training, is primarily limited to law enforcement professionals through the International Association of Computer Investigative Specialists.

E-mail Screening

E-mail screening techniques can catch a perpetrator in the act of a theft, stop the unauthorized transmission of information, and/or monitor communications with other individuals.

Many e-mail screening products are available commercially, which are typically housed on a firm's email server to monitor outbound and inbound traffic. These products can be set to monitor message content for key words, phrases, names or characters of interest to the investigation, and provide options for blocking, quarantining, or flagging of messages matching the set criteria.

In the absence of such technology, evaluation of past e-mail is often a component of an investigation into an alleged theft.

Even in instances where a suspect's machine is not available for forensic evaluation, e-mails are often archived on firm servers. Forensic tools can facilitate key word searching and other techniques.

Networks and Workstations

Commercially available software can capture keystrokes, and that data can be evaluated as part of your investigation.

These tools have become quite sophisticated, and can be used to monitor activity (document preparation, communications, Internet activity, etc.) in real time.

Making it Stick

While technological advances in the workplace have made the theft of intellectual assets easier to perpetrate, it has also made the theft easier to document and ultimately resolve.

It's possible to develop proof and prosecute offenders in intellectual asset thefts, because the use of electronic media in committing the act can provide investigators with an accurate record of the transgressions.

The key to taking advantage of this technology is having the appropriate policy and procedures in place beforehand, which facilitates the investigation and sidesteps potential "expectation of privacy" defenses.

Dennis Farley *is president of The Intelligence Group, a security consulting and investigations firm, based in Bedminster, N.J.*
E-mail: DFarley@intell-group.com
New Jersey Office. Web: www.intell-group.com

Reprinted from Law Tecnology News