News & Analysis
Amid Arrests In HP Case, Time To Shore Up Corporate Probes

Sharon Gaudin (sgaudin@cmp.com) and K.C. Jones
621 words
9 October 2006
InformationWeek
30
1109
English

With Hewlett-Packard insiders and contractors facing fraud and conspiracy charges, a spotlight is being shone on the shady world of corporate intelligence.

A month after HP principals admitted to conducting a boardroom leak investigation that involved spying, accessing phone and fax records using false pretenses, and running a sting operation on a reporter, former HP chairwoman Patricia Dunn and four others were charged last week with fraud and conspiracy. The California attorney general's office arranged for Dunn and former HP ethics chief Kevin Hunsaker to surrender. Dunn is to be arraigned on Nov. 17, Hunsaker on Dec. 6.

Also charged with felonies were security contractor Ron DeLia and investigators Matthew DePante and Bryan Wagner. DeLia and Wagner were expected to turn themselves in last week. At press time, Attorney General Bill Lockyer's office had not made contact with DePante. All five face charges for allegedly engaging in fraudulent wire communications, wrongful use of computer data, identity theft, and conspiracy to commit those three crimes. No charges have been brought against HP CEO Mark Hurd, named chairman on Sept. 22 when Dunn stepped down.

A federal investigation of HP's practices continues out of the U.S. Attorney's Office, as do probes by the FBI, FCC, Federal Trade Commission, and Securities and Exchange Commission.

FORBIDDEN FRUIT

Security and intelligence experts say the temptation can be great for executives to authorize the use of Web bugs, miniscule eavesdropping devices, and other newfangled technologies. They give companies a sense of distance and anonymity. Using tracking software seems less cloak-and-dagger than breaking into someone's office and tearing through desk drawers.

"It amounts to an extraordinary amount of change in our industry," says **Michael Hershman**, president of the Fairfax Group, an investigative firm that largely deals in theft of proprietary information, embezzlement, and computer sabotage. Most investigators aren't sifting through reams of legal papers crammed in the back rooms of courthouses. Instead, they're searching online databases from around the world. And they employ computer forensics, accounting, legal, and insurance experts as part of what have become information consultancies.

To track employees, some companies rely on GPS technology installed in company cars and on company-issued cell phones, says Howard Schmidt, a former White House security adviser and now CEO of R&H Security Consulting. And "phone home" software installed on laptops will send out a notification of a machine's location every time it's booted up.

Legal investigative tactics? Most of the time. Ethical? That gets a little murkier, but as long as it's company-owned equipment and networks, employees can expect their communications to be monitored.

HP's investigators went a couple of steps over the line, concocting the persona of a disgruntled HP senior manager e-mailing insider information to a reporter. Attached were tracers, otherwise known as Web bots. If the reporter forwarded the messages to her secret contact on the company's board, the tracer was set up to send his IP address back to investigators.

Ken Springer, a 12-year FBI veteran and now president of Corporate Resolutions, an investigative firm, calls these kinds of tactics "forbidden fruit." "It's there, but you can't take it," he says. "You have to make sure that what you do stands up to scrutiny."

Ever since news of the HP scandal broke, clients have called Springer to make sure their investigations are legal, even asking for written assurances. "Before, people assumed you were doing it legally," he says, "but now they're double-checking."

http://informationweek.com/

Document IWK0000020061009e2a90000q