Technology for Spying Lures More Than Military

By JULIE CRESWELL and RON STODGHILL
Published: September 25, 2006

In the world of security sleuths and private investigators, it’s billed as one of the biggest events of the year. Some 20,000 experts in the business are gathering this week in San Diego to check out the latest in high-tech surveillance gadgets and sit in on seminars discussing undercover investigations, background checks and interrogation techniques.

One of the keynote speakers is George J. Tenet, the former director of the Central Intelligence Agency.

But many of those attending the ASIS International “Maximum Security” conference will not be there on behalf of the United States government or the military. They work for corporate America, where security is a big and sometimes controversial business, as the executives of Hewlett-Packard have found in the wake of revelations of a covert-operations spying scandal that the company conducted against its own directors and journalists.

There’s no word whether executives from Hewlett-Packard are attending the conference to take in seminars like “Rules of Engagement: The Impact of Security Services Contracts in Future Litigation” or “Trusted Insiders — Preventing Betrayal in High-Risk Times.”

But while H.P. may be in the spotlight for the spying imbroglio in its boardroom, it is far from alone in diving into the murky world of private investigators and secret surveillance.

Companies worldwide spent an estimated $95 billion on security last year, according to the Freedonia Group, a market research firm in Cleveland. While that’s a broad figure that includes spending on emergency planning in case of a terrorist attack and protecting corporate records from hackers, an increasing portion went to high-tech equipment like spyware and specialized data-mining software that was deployed in-house so companies could better see what their own employees were up to.

Outside their offices, corporations are also turning to a vast network of large consulting firms and local ex-cops-turned-detectives that can supply all sorts of personal information and run surveillance on competitors, executives and directors using techniques worthy of the C.I.A.

The problem with all this spying, however, is that technology has far outpaced its users’ knowledge of the laws and ethics regarding privacy, which vary from state to state, say experts.

“In this day and age, it’s not impossible for me to find checks that you wrote and cleared
in your bank account yesterday," said Thomas D. Thacher II, who spent years rooting out
fraud in construction projects in New York before forming the investigative firm Thacher
Associates. "It is scary the personal information that is available through obviously illegal
means."

In the case of Hewlett-Packard, the company hired private investigators who used
" pretexting" — pretending to be someone else — to gather home phone records of
directors and journalists it believed were involved with the leaking of secrets from the
boardroom. Investigators for H.P. also tried to plant software on a reporter’s computer to
track a bogus document it sent to her and considered infiltrating newsrooms with spies
masquerading as clerical workers or cleaners.

"The means here did not justify the end," said George Bradt, chief executive of
PrimeGenesis, which coaches chief executives on leadership topics. "They pulled out a
Sherman tank to attack a mouse."

The H.P. episode is not the first time a company has tried to spy on, or to manipulate,
journalists. In 1965, General Motors hired private detectives to investigate Ralph Nader
after the publication of "Unsafe at Any Speed." (Mr. Nader later won a court settlement of
$284,000 against G.M. for invasion of privacy.) In 1989, American Express admitted to
planting defamatory articles about Edmund J. Safra, a former company executive who left
to form a competing bank.

Still, corporate security experts say there are plenty of legitimate reasons companies need
to be involved in the spy game, or at least to bolster their intelligence-gathering apparatus.
Companies frequently tap investigators to unearth compromising data about individuals
who have filed lawsuits against them, to scour gray or counterfeit markets for knock-offs
of their products or, increasingly, to uncover whether short sellers are working in concert
to drive their companies’ stock down.

More remarkably, many defend the practice of pretexting as a useful way for companies to
keep track of their competition.

"Pretexting is a valuable investigative tool in its natural form," said Charles Mittelstadt, a
security consultant in Atlanta who has worked with H.P., L.B.M., and Georgia-Pacific in
criminal cases. "Company A calls Company B and impersonates a consumer to vendor to
obtain vital information about pricing, development plans, etc.," he said.

But just because a company has the capability to spy, should it? According to some
investigators, they, not their clients, are the ones drawing an ethical line in the sand.

"We are frequently asked by clients who watch far too much television whether we can do
this or do that. In our engagement letter with them, we make it clear we will not do
anything illegal and they should not expect us to," said Joseph Rosetti, who headed up
security at L.B.M. for years before joining Kroll Associates. He now runs his own firm,
called SafirRosetti.

"Investigators are going to have problems until they develop a set of national standards to
which they must conform," said Jack Lichtenstein, director of government affairs and
public policy for ASIS International (formerly the American Society for Industrial
Security), which is host of the San Diego conference.

The biggest challenge companies face when they turn to outside private investigators —
and one of the chief appeals of using them — is not knowing and controlling the
techniques to be used. That’s because security firms typically farm out parts of the
investigation to other firms or local on-the-ground investigators.

"We will pull a number of subcontractors into an investigation. There are firms out there
that have strength in the computer-forensic world or S.E.C. matters that can help out,” said Mr. Thacher. “But the further you go down the chain, the more removed the client is from the investigation and their ability to judge or know how the information is being obtained.”

That may have been the case with Hewlett-Packard, experts say.

Hewlett-Packard’s chairwoman, Patricia C. Dunn, has acknowledged that she authorized the investigation, and documents show that its senior counsel and director of ethics, Kevin T. Hunsaker, directed the operation, which involved Hewlett-Packard investigators and several layers of outside detectives and subcontractors.

Already, some companies are trying to cover their tracks in the wake of the Hewlett-Packard spy scandal.

“We just received a retention agreement from a large Wall Street firm in which the specific language was laid out that the consultant agreed not to do things that are illegal,” said Mr. Thacher. “It made us all smile. One would think that goes without saying. But it’s in there now.”

Next Article in Technology (2 of 32) »

Don’t have TimesSelect? What are you waiting for? Try it free for 14 days.