Lost iPhone just one headache for Apple security

September 18 2011, By MARCUS WOHLSEN , Associated Press

(AP) -- Wanted: experienced security professional. Must have plan to thwart Chinese counterfeiters, protect secret blueprints from spies and keep workers from leaving super-secret unreleased smartphones behind in bars.

A day after a recent report surfaced that an Apple employee had lost a prototype for a new but unreleased iPhone at a Northern California watering hole, two job listings appeared on Apple's website for managers of "new product security."

Such workers would join a team at the $350 billion company that has included ex-FBI agents and other highly trained pros with backgrounds in intelligence and law enforcement.

While a private security force might not seem in keeping with its user-friendly image, Apple and other companies in its league need the best protection they can buy, corporate security experts say. And lost iPhones likely don't come near the top of the list of anxieties.

"Corporate espionage, that's big money. Billion-dollar money. The paranoia is justified," said Jim Stickley, co-founder of corporate security consulting firm TraceSecurity "Whatever they're trying to do, their competitors want to know. Everybody wants to know."

Apple declined to discuss its security operations in detail with The Associated Press, in keeping with the company's longstanding reputation

for secrecy. Nor has the company confirmed the existence of the iPhone 5, the rumored latest model, much less a lost prototype.

But San Francisco police have said that four officers recently went to a home in the city's Bernal Heights neighborhood with two Apple employees, who met with the resident and searched the home for an iPhone prototype.

Apple watchers say the company is known for creating many test versions of its new devices before they're released to see how they work in the real world. The reportedly lost iPhone likely would have been far from the only one in circulation.

Losing just one such device is perhaps more of a marketing headache than a serious security breach, as was the case for Apple last year when the tech blog Gizmodo posted photos of what turned out to be the then-unreleased iPhone 4 lost by an employee at a San Francisco Bay area beer garden.

Once a new device has reached the point where employees are field-testing it, a competitor who obtained one wouldn't have enough time to analyze it and do anything to take advantage of that insider knowledge, Stickley said.

Even so, sheriff's deputies seized Gizmodo blogger Jason Chen's computers as part of an investigation into whether the blog's $5,000 payment to acquire the lost phone amounted to a crime. No charges were filed.

Such tactics might seem heavy-handed. But for Apple and other tech companies the issue amounts not just to a publicity problem but a fiduciary obligation to shareholders to secure the company's valuable assets, said longtime Apple analyst Tim Bajarin.

Companies also have an obligation to try to prevent such a loss from happening again, he said: "If they fail, it's the system that failed as much as the individual."

Despite the blogosphere frenzy surrounding the lost iPhone prototypes, experts say the security threats to tech companies are far more serious in China, where thousands of workers labor to manufacture Apple's products.

According to a 2008 diplomatic cable released by Wikileaks, Apple had only a modest security presence in China until March of that year, when the company hired a team from Pfizer that led a crusade against fake Viagra.

Under the leadership of Donald Shruhan, whose LinkedIn profile lists him as a Hong Kong-based senior regional director for Apple in security and investigations, the company began taking steps to reign in the country's trade in counterfeit iPhones, iPods and MacBooks.

"Early evidence suggests nearly 100 percent of Apple products in unauthorized mainland markets are knockoffs," according to the unclassified cable from the U.S. Embassy in Beijing.

The job of keeping such counterfeits off the shelves, to keep blueprints for new products from leaking and to otherwise secure vital trade secrets falls under the field of information assurance.

For information assurance professionals, securing computer networks is only part of the job. They also make sure companies remember to lock their actual doors.

"Social engineering" also remains a constant threat in the tech industry, said Gary Kessler, director of the information assurance program at

Norwich University, a private military college in Vermont that has trained security personnel at Apple and other high-profile companies. From e-mail scams seeking sensitive personal information to Cold War-style cloak-and-dagger subterfuge, human weakness can be easier to exploit and harder to protect against than digital vulnerabilities.

"This stuff has been going on for decades, just in a different guise," Kessler said. "The Internet has just given us a new vector for attack."

And in the end, he said, even the best-trained security team in the world can only do so much to protect against someone in a bar who may have been drinking and may have been showing off the most sought-after secret product in the world.

Said Kessler: "I'm guessing that Apple probably did everything that anybody could do, and they probably did it right."