Tech titans see opportunity in cybersecurity

September 19 2013, by Steve Johnson

With its PC sales slowing, Hewlett-Packard Co. is grappling for a piece of the exploding cybersecurity market as a key part of CEO Meg Whitman's plan to turn around the struggling company.

The Palo Alto, Calif., corporate colossus is one of many Silicon Valley technology powerhouses - including Apple Inc., Google Inc., Intel Corp. and Cisco Systems Inc. - that have snapped up security companies in recent years to gain a foothold in the industry, which already boasts worldwide annual sales of more than $67 billion, according to the research firm Gartner. That's more than twice the $25 billion forecast to be spent this year globally on tablet and smartphone applications, and the total for security is expected to hit $94 billion in 2017, thanks to the burgeoning menace posed by computer hackers.

"This is the issue of the day," Whitman said of the growing threat, during a recent CNBC interview. "I contrast it back to when I started at eBay. I was worried about a teenager in Red Deer, Mont., hacking into our systems. This is now organized crime." As a result, "we are really making a big push in security."

HP is elbowing its way into a crowded field.

The San Francisco Bay Area and the region around the nation's capital are widely considered the hottest spots in the world for the industry. More than 100 companies here are involved in monitoring and fending off hackers, several cybersecurity experts estimated. Many of the firms are recent startups like 4-year-old HyTrust of Mountain View, Calif.,

which helps secure data accessed over the Internet.

"We're seeing our sales quadruple this year compared to last year," said co-founder Eric Chiu.

He and other experts partly attributed the business boom to the increased security concerns of companies placing data on Web-based services and the enormous popularity of mobile devices, which often aren't as well protected as PCs and are frequently targeted by malware.

But the main reason is the increasing sophistication of computer crooks, who are pilfering corporate secrets, extorting money, hijacking identities and reaping huge profits.

"It's a multibillion-dollar business in and of itself," John Grady, a security specialist with International Data Corp., said of the criminal enterprises. "So the industry, to keep up on the defensive side, has just skyrocketed."

Although HP doesn't reveal how much money it gets from its cybersecurity products, which are designed to discourage attacks and minimize losses when breaches occur, the amount is a tiny portion of its revenue. But the company hopes to change that. Even as the company is cutting its workforce by 29,000, its website lists more than 150 security-related job openings, from engineers and content developers to incident analysts and project managers.

It's the same story at other companies, according to a report this year by Burning Glass International, which tracks employment. It found that in the past five years, demand for cybersecurity positions has grown three and a half times faster than for computer jobs generally and 12 times faster than the overall labor market.

Moreover, businesses of all types are boosting their cybersecurity budgets. Of nearly 2,000 executives surveyed this year by corporate consulting firm Deloitte, 79 percent expressed concern about their vulnerability to hackers and 58 percent planned to raise spending on cybersecurity in the next 12 months.

That's largely due to a spate of publicized cyberattacks against companies ranging from Wells Fargo, Citigroup and PNC Financial Services to Facebook, LinkedIn and Microsoft, according to Robert W. Baird & Co. analysts. As a result, they concluded in a recent note to their clients, "government officials and boards of directors are taking cyber threats more seriously than ever."

Security firms confront the threat in different ways. Some spot vulnerabilities on corporate networks and block hackers from getting in, while others sniff out malware on Internet sites and clean infected devices. But incorporating all these offerings from different sources can be hard, said Pat Calhoun, senior vice president of McAfee's network security division, because "these products were never designed to work together."

McAfee hopes to grab a larger chunk of the market by providing a compatible package of protections. If it succeeds, it would be a bonus for Intel, which bought McAfee in 2010 for a staggering $7.7 billion, the biggest deal in the Santa Clara, Calif., chipmaker's history. Like HP, Intel's sales have been hurt by the declining consumer interest in PCs, so it is counting on the McAfee purchase to help shore up its bottom line.

Similarly, HP, which gets about 29 percent of its revenue from PC sales, in 2010 bought ArcSight for $1.5 billion as well as Fortify Software for an undisclosed sum.

Other Silicon Valley tech giants also are making security purchases.

This summer, San Jose, Calif., networking giant Cisco Systems announced a $2.7 billion deal to buy Maryland-based Sourcefire, whose technology government agencies and top corporations use to fight off advanced cyberattacks. Last year, Google bought VirusTotal, which detects infected files and websites; Juniper Networks Inc. bought Mykonos Software, which blocks attacks on websites and applications; Apple bought AuthenTec, which protects mobile gadgets; and Twitter Inc. bought Dasient, which scans websites for malware.

Oracle Corp. and VMware Inc. also have gobbled up security companies in recent years and more such deals are likely, according to FBR Capital Markets & Co. analysts.

Predicting a "surge" of such acquisitions, they concluded in a recent report, "we believe the network security competitive environment will heat up in 2013 as the threat environment continues to evolve, leading to massive potential for growth and a battle for market share among the industry's well-known players."

©2013 San Jose Mercury News (San Jose, Calif.)
Distributed by MCT Information Services