Security firm learns limits of security tech

April 6 2011, By JORDAN ROBERTSON , AP Technology Writer

(AP) -- Top-level data breaches often start at the bottom of the ladder. That's a lesson RSA, one of the world's premier computer security firms, learned the hard way.

The company is best known for its small security "tokens" that generate secondary passwords for accessing sensitive networks. Three weeks ago, the company disclosed that hackers had infiltrated RSA's own network in an "extremely sophisticated" attack, and made off with data that RSA still has yet to specify.

The break-in was alarming because of the breadth of RSA's business, and because it's rare to hear of a severe breach at a key security firm.

Speculation is mounting about what was stolen. One possibility is that the attackers made off with the codes for how the tokens' passwords are generated, which would be serious for the military and banks and other institutions that use them.

Meanwhile, RSA has revealed a few details about how the attack happened.

The explanation is a reminder of how vulnerable a company can be when workers are hoodwinked, never mind that they're surrounded by cutting-edge hacking protections.

RSA, a division of data-storage leader EMC Corp., says the intruders got in by exploiting a flaw in the ubiquitous Adobe Flash software, and the

gullibility of a worker who opened an infected spreadsheet inside an e-mail that carried the subject line "2011 Recruitment plan."

The Flash vulnerability was a so-called "zero day" flaw that hackers found before the software maker, so it had no chance to fix it with an update. RSA says the flaw is now fixed.

"In our case the attacker sent two different phishing emails over a two-day period," RSA said in a blog post. "These emails were sent to two small groups of employees. When you look at the list of users that were targeted, you don't see any glaring insights; nothing that spells high profile or high value targets."

Once the worker's computer was infected, the attackers used it as a launching pad to hunt through the corporate network for users with more access to sensitive data. RSA would only say that even though the company caught the attack in progress, "there was time for the attacker to identify and gain access to more strategic users."

Many sophisticated breaches happen just as RSA's did. The fact that a company that makes some of the most widely used anti-hacking technology could itself be hacked should serve as a reminder of the limits of security technology in the face of previously unknown software bugs and expertly crafted scam e-mails. EMC, however, said it's rare to catch such an attack in progress, which it suggested speaks to the capabilities of the protections it has in place.

Apart from the hackers, there was another winner in the ordeal.

This week, EMC announced that it was buying Virginia-based NetWitness Corp., a network security firm that helped RSA detect the breach. It's led by Amit Yoran, the former director of the U.S. Department of Homeland Security's cybersecurity division.