



Dow Jones Reprints: This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers, use the Order Reprints tool at the bottom of any article or visit [www.djreprints.com](http://www.djreprints.com)

[See a sample reprint in PDF format.](#)

[Order a reprint of this article now](#)

## THE WALL STREET JOURNAL

WSJ.com

TECHNOLOGY | JUNE 7, 2011

# Security 'Tokens' Take Hit

*RSA Offers to Replace Its SecurIDs or Provide Monitoring for Nearly All Customers*

By SIOBHAN GORMAN And SHARA TIBKEN

RSA Security is offering to provide security monitoring or replace its well-known SecurID tokens—devices used by millions of corporate workers to securely log on to their computers—"for virtually every customer we have," the company's Chairman Art Coviello said in an interview.



Joe Schram/The Wall Street Journal

RSA SecurID

In a letter to customers Monday, the [EMC Corp.](#) unit openly acknowledged for the first time that intruders had breached its security systems at defense contractor [Lockheed Martin Corp.](#) using data stolen from RSA.

SecurID tokens have become a fixture of office life at thousands of corporations, used when employees log onto computers or sensitive software systems. The token is an essential piece of security, acting as an ever-changing password that flashes a series of six digits that should be virtually impossible to duplicate.

Mr. Coviello didn't specify what happened to the tokens at Lockheed. The intruders didn't take any Lockheed customer or employee data. But as a precaution, he said RSA will offer to replace nearly all tokens—millions of them used by government agencies and businesses ranging from Rolls Royce Motor Cars Ltd. to [PokerStars.com](#).

### Related

[Hackers Say They Hit a Sony Unit Network](#)

[Hackers Attack Nintendo](#)

[Sony Pictures Confirms Hacker Attack](#)

[For Some Hackers, Goal Is Pranks Hackers Broaden Their Attacks](#)

Some customers may not need to replace them because of their specific security needs, he said. "We believe and still believe that the customers are protected."

Mr. Coviello said RSA will provide transaction monitoring and other detection capabilities for customers, particularly for financial institutions.

In March EMC disclosed it had been hit by a sophisticated

[Video: White House Targeted in Gmail Hack 6/3/2011](#)

[Video: 3rd Hacks into School Admin Accounts](#)

cyberattack on its SecurID products. It advised customers to beef up their own security, such as making sure no rogue programs had been installed on servers running RSA software. It also suggested users increase the length of employee "PIN" numbers used in tandem with the digits spit out by the RSA token.

As the company did a forensic analysis of the attack, it began to suspect the attacker was focused on defense contractors based on the sophistication of the attack and the profile of the hacker.

"Their modus operandi led us to believe this perpetrator was likely to attack defense secrets and related intellectual property," Mr. Coviello said, of the intruders. The Lockheed infiltration received high-level attention in Washington, including from President Barack Obama, who was briefed on the incident.

Shortly after concluding defense customers were likely targets, RSA began working with its government and military-contractor customers, and offered to replace all their SecurID tokens, which Mr. Coviello said was key to preventing further attacks.

Some analysts said RSA's token replacement program is a smart move but that the breach will still hurt its reputation.

"It would have been better if RSA was more forthright from the beginning. They unnecessarily damaged their reputation by holding back," said Gartner analyst Mark Diodati.

Mr. Coviello said his company has provided the right amount of information to its customers. Providing any further information, he said, would give the hackers a blueprint for how to mount further attacks.

Companies have been hit by a wide range of attacks in recent weeks. Sony Corp., PBS and users of Google Inc.'s Gmail are among recent examples. The RSA incident raised the most alarms given the company's core competence—computer security—and the central role it plays in guarding the systems of major U.S. corporations.

Lockheed became the first confirmed breach related to the RSA issue, with the U.S. weapons manufacturer saying an investigation into last month's cyber attack on the company "concluded that the RSA breach was a direct contributing factor."

"RSA has been with us every step of the way since our breach, and we're replacing all of our SecurID tokens," Lockheed spokeswoman Jennifer Whitlow said. "They did review our investigation details and have offered to help out as they could."

The Lockheed attack showed that it was technologically feasible to hack a third-party using data taken from RSA, and the defense contractor may not be the last example. Mr. Coviello said that "I'm not suggesting we won't see some other attacks in the interim given the scale of the Lockheed attack, but it is the only confirmed attack we have using the [stolen] information."

He added that RSA is working with other companies rumored to have experienced attacks due to the RSA breach, but declined to identify the customers.

"Because of these attacks and the changing threat landscape there has been and incredible heightening of

public awareness," Mr. Coviello said.

"The whole thing has reached a crescendo where customers don't want to tolerate any level of risk, whether it's real or perceived."

**Write to** Siobhan Gorman at [siobhan.gorman@wsj.com](mailto:siobhan.gorman@wsj.com) and Shara Tibken at [shara.tibken@dowjones.com](mailto:shara.tibken@dowjones.com)

Copyright 2011 Dow Jones & Company, Inc. All Rights Reserved  
This copy is for your personal, non-commercial use only. Distribution  
and use of this material are governed by our [Subscriber Agreement](#) and  
by copyright law. For non-personal use or to order multiple copies,  
please contact Dow Jones Reprints at 1-800-843-0008 or visit  
[www.djreprints.com](http://www.djreprints.com)