States scramble to attract suddenly hot cybersecurity firms

June 19 2013, by Elaine S. Povich

As data dragnets and information breaches dominate the news, states are scrambling to cash in on a rapidly expanding business sector by offering tax incentives to firms that protect sensitive information from outside attacks.

While ordinary Americans wonder if their private phone calls and emails are being monitored by their government, businesses are concerned that proprietary and sensitive business information could be stolen by competitors - at home and from overseas. State and local governments also are working to tighten safeguards to prevent outsiders from hacking into their information.

"It's the new global threat, not only to our state and nation, but to the whole world," said Mark A. Vulcan, program manager at the Maryland Department of Business and Economic Development.

Maryland is breaking new ground with a total $3 million offer of tax breaks to be distributed among cybersecurity startups already in the state or who agree to locate there. While many states include cybersecurity companies in their overall tax incentives for high-tech firms, Maryland's legislation - proposed by Gov. Martin O'Malley and signed in May - appears to be unique.

What also sets Maryland apart from other states, Vulcan said, is that this tax credit goes directly to the company, not the "angel" investor in that entity, which many other states do.

Analysts say this credit could signal a new wave of action by states trying to cash in on the cybersecurity boom. The $207 billion cybersecurity industry is expected to show "impressive growth" in the next five years, according to Entrepreneur.com.

Consultant Javier Siervo, with the Berkeley Research Group LLC in Washington, D.C., said Maryland may be the only state offering a tax credit specifically for cybersecurity, but D.C. offers incentives to companies that have an office in the District and "derive most of their revenue from technology-related activities." And nearby Arlington County in Virginia has increased technology zones to encourage tech businesses to move operations to the county.

In Virginia, a statewide program that offers capital gains tax exemptions to tech companies would cover cybersecurity companies as well as other high-tech ventures, according to Cameron Kilberg, the state's assistant secretary of technology. Under that incentive, the state doesn't tax any income already taxed by the federal government as a long-term capital gain.

The program began in 2010, Kilberg said, and will continue to 2015, past its original sunset date of 2013, because the state wanted more time to evaluate whether the program was effective.

The area around Washington is home to many government contractors and attracts a sizable cybersecurity industry, said Michael Colavito, state and local tax expert at Aronson LLC, who advises private business on how to take advantage of state tax incentives. He said security needs to be stepped up "because of all the hackers out there," and Maryland is trying to position itself to take advantage of that situation.

Some of the nation's largest defense and security companies are among the top 20 worldwide in the cybersecurity business, including Booz Allen

Hamilton Inc. (the company of Edward Snowden, who leaked the National Security Agency's data dragnet program), General Dynamics, Lockheed Martin, Northrop Grumman and Raytheon among others.

Much of the effort to incentivize the cybersecurity industry has come about because of an executive order signed by President Barack Obama on Feb. 12 that directs federal agencies to develop voluntary cybersecurity standards for private-sector industries and propose new mandates if needed. It was aimed at helping state and local governments protect critical infrastructure controlled by Web-based technology.

Widely publicized data breaches over the past couple of years fueled the government's effort. They include:

-In March 2012, NASA shut down a large database and sent warnings to its employees after a laptop stolen from a car was hacked, revealing personnel data as well as technology.

-In 2012, hackers got into the U.S. Navy system that tracks personnel moves and compromised private data on 200,000 sailors and their family members.

-In 2012 a Washington state website was hacked, revealing hundreds of thousands of Social Security and driver's license numbers of state residents.

The trade group Council for Community and Economic Research keeps track of tax incentives across the 50 states and offers businesses incentive comparisons. The group's website notes that there are more than 1,600 incentive programs across the country sponsored by different states and localities, and the cybersecurity credit is just one focus.

New York and New Jersey, for example, are competing for business -

this time in the financial sector, tax expert Colavito said. "States are being aggressive on both sides," he said.

He also pointed out that despite the tax break for investing in Maryland, the state still stands to gain if a firm is successful, because it will then pay taxes to the state. The break is a "refundable credit," however, so it applies even if the company never makes money.

O'Malley and Michigan Gov. Rick Snyder headed up the National Governors Association's Resource Center on Cybersecurity, and promoted the topic at the NGA's winter meeting in February.

Whether the return on investment for the state is profitable is an open question. According to a study in April 2012 by The Pew Charitable Trusts, states have a spotty track record on following up on the results of their economic development tax incentives. While every state has some kind of tax incentive, and many of the states have several, not all are successful at determining their outcomes.

Pew, Stateline's parent organization, rated the states and the District of Columbia on how well they are measuring the economic benefits and costs of their tax incentives. Thirteen states were rated as "leading the way," 12 got "mixed results" and 26 were "trailing behind."

©2013 Stateline.org
Distributed by MCT Information Services

Citation: States scramble to attract suddenly hot cybersecurity firms (2013, June 19) retrieved 10 April 2024 from https://phys.org/news/2013-06-states-scramble-suddenly-hot-cybersecurity.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.