THE WALL STREET JOURNAL.
WSJ

Bayshore Networks Raises $6.6M to Secure Industrial Internet

Mike Dager joined Bayshore Networks in January as chief executive. The security company plans to address the industrial Internet of Things. *PHOTO: BAYSHORE NETWORKS*

By CAT ZAKRZEWSKI May 10, 2016 7:30 a.m. ET

Bayshore Networks wants to secure the industrial Internet, protecting everything from manufacturing plants to power grids.

The Bethesda, Md., company picked up $6.6 million in Series A funding, led by Trident Capital Cybersecurity with participation from undisclosed angel investors. The company previously raised about $3 million in seed funding.

Trident Capital Cybersecurity co-founder and Managing Director Alberto Yepez said demand for companies that secure industrial networks has risen in the wake of attacks on critical infrastructure. The most well-known infrastructure attack came with Stuxnet, the worm discovered in 2010 that infiltrated Iran's nuclear centrifuges. More recently, hackers infiltrated a power grid in Ukraine in late 2015.

"I believe there's a huge market," Mr. Yepez said. "All the power companies got a wake-up call."

Mr. Yepez will join the company's board, and Trident Capital Cybersecurity Vice President Will Lin will be a board observer.

A recent study from International Data Corp. supports Mr. Yepez's predictions. The research firm predicts the world-wide IoT security products market will grow from $655.8 billion in 2014 to $1.7 trillion in 2020. IDC looks at the entire IoT sector, not just industrial IoT.

Mike Dager, who joined Bayshore Networks as chief executive in January, said this increased demand has allowed Bayshore to work with Fortune 100 companies even at an early stage. He said Bayshore is working with about 50 to 100 customers to date, though not all of them are billed yet.

"The industrial Internet and IoT space are a new frontier and a dream come true for the hackers," Mr. Dager said.

Increasingly legacy control systems that were never meant to be connected to the Internet are coming online, Mr. Dager said. As companies seek to expand visibility of their manufacturing plants, they are connecting control systems that are decades old.

Mr. Yepez said larger technology companies are seeking to embed security from the beginning, so that the Internet of Things is built with security in mind. But until older systems are replaced, there are holes that can be exploited.

Bayshore provides a product it calls the "IT/OT Gateway" to provide IT departments visibility into their company's operational environments. The company says it can inspect network flows all the way down to machine sensor values, which can be overlooked by other security products.

Mr. Dager said many companies are trying to apply security software developed for computer networks to the industrial space.

"There are shortfalls to the existing solutions," Mr. Dager said. "You have a lot of people in the IT space who just repurpose IT solutions for the industrial space, versus what we've done at Bayshore, which is designing from the beginning for the sole use case of enabling the industrial Internet of Things."

Write to Cat Zakrzewski at cat.zakrzewski@wsj.com