

Companies hope cybersecurity experts in the boardroom can counter hacks

August 26 2015, by Paresh Dave, Los Angeles Times

The board of directors at construction and engineering company Parsons Corp. needed to fill a seat two years ago.

Naturally, they wanted someone with communication and leadership skills. They also needed someone new: an expert to help them battle computer hackers, cyberthieves, electronic spies, digital vandals and anybody else out to wreak havoc in a connected world.

The privately held firm's latest board member is Suzanne Vautrinot, a retired Air Force major general who helped create the Department of Defense's U.S. Cyber Command and led the Air Force's IT and online battle group.

Parsons, based outside Los Angeles in Pasadena, is at the forefront of a fast-expanding trend in corporate governance: the elevation of [cybersecurity](#) experts to the boardroom, a perch traditionally occupied by former CEOs and specialists in marketing and finance.

In recent months, AIG, Blackberry, CMS Energy, General Motors and Wells Fargo have added a board member with computer-security knowledge. Delta Air Lines and Ecolab did the same in recent years.

The reasons are clear. Cyberattacks on large companies skyrocketed 44 percent last year from 2013. Cybercrime costs businesses more than \$400 billion a year, according to Lloyd's of London.

Boards are responsible for advising chief executives on setting goals and plans to achieve them, and to question the challenges standing in the way. Not adequately addressing a cybersecurity risk could prove costly - in money, reputation, legal bills, lost time and lost customers.

Just ask Target. Since hackers breached its payment systems two years ago, Target has spent \$256 million cleaning up the mess, with insurance expected to cover about a third. Though costing a small slice of revenue, the damage was enough to sack the chief executive and scare away many customers for several months. Government investigations and several lawsuits from affected customers and business partners are ongoing.

In other cases, cyberthieves steal sensitive corporate data, which could cause the company's competitive advantage to slip and its reputation to wane.

Data show that corporate boards have a long way to go. Just 11 percent of public-company boards queried this year reported a high-level understanding of cybersecurity, the National Association of Corporate Directors said. A review by the New York Stock Exchange and security firm Veracode found that two-thirds of board members questioned think their companies are ill-prepared for a cyberattack. Yet consulting firm PricewaterhouseCoopers reports that 30 percent of boards surveyed never talk about cybersecurity at all.

That fact raises eyebrows. "There's some liability in not taking every measure you can to protect your clients, to protect your revenue stream," said Gary Matus, managing director at the executive recruiting agency RSR Partners. "To give people confidence, you have to be getting the best advice you can."

To Parsons Chief Executive Charles Harrington, having a cyber pro on the board was a no-brainer. The nature of Parsons' business demanded it.

Along with classified government work, Parsons builds bridges, utility plants and military bases. Harrington realized that those projects' IT networks needed protection. Computer viruses were spreading that could destroy the infrastructure Parsons assembled. So he has been preparing his company for what he calls the age of "electronic battlefields."

He bought two cybersecurity companies. Pairing them with Parsons' engineers and scientists, they aimed to "bake" in security rather than "bolting" it on after.

Harrington knew the direction was right, but needed someone with a new perspective to help him strategize, and communicate that strategy to the board. He tapped Vautrinot, whom he calls a "rare individual with the deep technical set and the communication skills needed to gravitate to a board." And she's "not afraid to dig in and get her hands dirty."

She's no rubber stamp. Vautrinot visits the company's cybersecurity teams. She helps think through what will persuade a customer to pay for cybersecurity services, likening it to the challenge years ago of getting people to wear bicycle helmets. In the boardroom, she cuts through jargon, explaining opportunities to protect the technological backbone of railroads, toll roads and the like. She advises on how the 15,000-employee company should protect its own worldwide network, under constant threat because of the sensitive projects Parsons undertakes.

"You can bring the passion, you can champion, you can ask good questions," she said. "You can help other board members see 'Is it viable? Can we do this and grow as a company?'"

In February, Vautrinot joined Wells Fargo, which is heavily investing other cost-savings into information security. She's also on the boards of Ecolab and Symantec.

Demand for board members such as Vautrinot is increasing, board recruiters said.

David Burg, U.S. cybersecurity leader at PwC, said he's still receiving an "amazing" number of requests from boards for basic education. For example, PwC helps boards compare their company's security approach with competitors'.

There's a big problem with the whole trend, though: a shortage of cyber-qualified board candidates.

John Pironti, a risk and security advisor for the professional group ISACA, is urging his members to ask for more responsibilities during this "big hump of sensitivity," so they'll be primed for larger advisory roles in the future - including on boards of directors.

Harrington is open to that idea. Three years ago, Parsons' board decided to allow employees to join boards of other companies, though it hasn't yet fielded any requests.

"Depending on how critical their IT network is to them, absolutely, having someone on the board can shift the dialogue," Harrington said of other companies. "Cyber finds a way onto our agendas one way or another."

Help is wanted in the cybersecurity field - and not just on the board of directors.

As computer hacking grows more pervasive, so does the demand at all levels for workers skilled in the field. And where there's a demand, there's a startup looking to meet it.

Cybrary is an online cybersecurity training website that launched in January, and already, the company said, 150,000 people have participated.

Like many startups, Cybrary aims to fill a market gap with a better, quicker and cheaper service. For now, its courses are free to individuals. Businesses pay a few thousand dollars a month for access to specialized courses. About two dozen businesses and schools have subscribed.

One is N2grate, a data center management firm in Washington, D.C. Using Cybrary is expected to drop the small firm's training costs to \$15,000 this year from \$50,000, according to N2grate President and Chief Operating Officer Steve Halligan.

"It's a fascinating transformation of the corporate training market," he said.

Classroom training was inconvenient and expensive, he said. Now classes can be taken on the fly. Recently, on-demand materials proved valuable when his team quickly had to learn about mobile security issues for a Department of Justice project. Niche courses from a provider such as the SANS Institute might be held only a few times a year and only in certain regions.

Ryan Corey, a Cybrary co-founder, taught cybersecurity in classrooms for 13 years and was unimpressed with the cost and quality of alternative online offerings. He had no doubt there was a market for his idea if he could pull it off.

Heavily hacked industries - retail, finance and health care among them - doubled cybersecurity hiring over the last five years. Security gigs stay unfilled for 8 percent longer than other technology jobs and pay \$6,500 more annually, according to job-market data firm Burning Glass

Technologies.

Corey saw an opportunity to both sharpen cybersecurity workers' skills and train new workers with Cybrary, which is based in Maryland.

"We're going to empower the entire world to learn cybersecurity and prepare themselves for the threats that are out there," Corey said with an entrepreneur's enthusiasm. "For beginning professionals, for high-end professionals."

Someone who starts with a basic course on how computers work could confidently apply to a beginner-level job after taking about six courses and spending up to 40 hours on each, Corey said.

After giving the site a try, Paco Hope, principal consultant at software security firm Cigital, said the courses can also be used to prep for certification tests.

He likes the price. Except at the highest levels, cybersecurity techniques are "largely understood and agreed across the industry, so if someone wants to make it available free, that's fine," he said.

-Paresh Dave

EXPERTS TACKLE CYBERSECURITY FROM THE INSIDE

A few of the companies adding board members with cybersecurity expertise:

CONVERSA HEALTH

The company hired Peter Levin, who overhauled the Department of Veterans Affairs' online health records system and now runs a data security company. "Health care tends to be at the front of the spear for attackers," Conversa Health CEO West Shell III said. Companies "need to have smart, technical [board members](#). If not, they are going to wish they had."

XOOM CORP.

The online money transfer service added Tom Killalea, Amazon's first chief information officer. "Data hacking and data loss ... are being scrutinized at higher and higher levels," Xoom CEO John Kunze said. "All boards have to be prepared to take accountability and oversight of information security."

GENERAL MOTORS

Linda Gooden, who ran the Lockheed Martin division that builds and manages computer systems for the Department of Defense and other large customers, was tapped to help GM. Listed among her oversight responsibilities is "vehicle cybersecurity," a hot topic given the recent news about hackers remotely taking control of Jeeps and Teslas.

AMERICAN INTERNATIONAL GROUP INC.

The insurance giant known as AIG added former Northrop Grumman executive Linda Mills. With degrees in math and computer science, she climbed the defense contractor's ranks over 12 years, most recently overseeing nearly all complex projects and their security components.

©2015 Los Angeles Times

Distributed by Tribune Content Agency, LLC.

Citation: Companies hope cybersecurity experts in the boardroom can counter hacks (2015, August 26) retrieved 23 April 2024 from <https://phys.org/news/2015-08-companies-cybersecurity-experts-boardroom-counter.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.