The Examiner

Prudent Portfolio: Cybersecurity is a Brave and Critical New World for Investors

July 18, 2017 By Examiner Media

By Peter Chieco

Last fall, Connecticut Gov. Daniel Malloy named an ex-military intelligence officer to a newly created post, one that 20 or 30 years ago would have sounded like science fiction: chief cybersecurity risk officer.

The appointment, however, came in response to an all-too-real scourge – cyber threats affecting the state.

Anyone reading the headlines knows that cyberattacks are not unique to one state; indeed, malware, viruses, phishing and spam are a menace throughout the nation. Often, hackers infiltrate targeted computer networks to corrupt crucial data files or steal personal, proprietary or financial information.

In fact, a recent Morgan Stanley poll of high net worth investors showed that data security was a leading concern, with some 72 percent saying that identity theft eclipsed other worries such as terrorism (65 percent) and illness (56 percent).

The costs associated with data breaches are astounding. Last year, some $81.6 billion was spent worldwide on cybersecurity products and services. In the U.S. alone, the 2017 budget proposes a $19 billion cybersecurity strategy, a 35 percent increase over the 2016 budget.

In response to the growing threat, an entire industry has developed, and for the savvy investor, it may be an industry worth careful research and investigation.

From large movers and shakers with household names to newborn startups with ground-breaking, inventive new methodologies, investors have a range of options to consider, some of which may prove to be solid additions to a well-diversified portfolio.

As with other industries, investors can gain exposure to investing in the cybersecurity sector through various channels, ranging from diversified baskets of technology investments that place some of the assets in cybersecurity holdings, to portfolios of companies that provide security hardware, software and solutions to individual equities.

The imperative to protect data in the face of often well-funded hackers has birthed an array of new ventures. Many computer users are familiar with firewalls and the companies that manufacture them, but the industry now devoted to enhancing system reliability and protecting sensitive data seems to be evolving each day. Advanced software tools can analyze activity and "listen" to a computer network to detect unusual behavior.

Globally, many companies offer regular assessments of their clients' security risks, from poor user protocols to exploitable vulnerabilities in code writing. With billions in assets, research, intellectual property, infrastructure and reputations at stake, these companies send dedicated teams to help their client organizations establish effective cultures of online security. Client education is a growing field.

Now, too, cybersecurity companies are specializing in the sectors they protect. The recent large-scale security breaches of major health insurers has led at least one major company to focus on helping health care organizations – hospitals, health plans, medical practices, health care startups and service providers – improve their information risk management.

Other companies strive to defend global financial institutions or military and national security.

Government websites often are popular prey to cyberattack. Of the four million e-mails that arrive each month on Connecticut's state network, at least a quarter are blocked as suspicious, and several thousand more are identified as malware. Increasingly, small- and medium-sized businesses are hacked. They now are the target of 65 percent of cyberattacks, according to some analysts.

Besides the companies that provide cybersecurity per se, or those that evaluate vulnerability and offer risk management, others have blossomed in response to the needs of cyberattack victims and may also be worthy of investor consideration. Those include disaster recovery experts, insurers that provide coverage against the costs associated with responding to an attack, forensic experts and others. Cloud, mobility, IoT (Internet of Things, or devices such as your insulin pump or your smart refrigerator) and cloud-based e-mail managers also are on the rise.

Of course, all of this is aside from the branches of law, regulatory compliance and law enforcement that also deal with cybercrime and fraud.

The caveat: past performance never is an indicator of future success. Monstrous breaches like that in 2015 of the U.S. Office of Personnel Management, or the recent global cyberattack involving ransomware, may lead to spiked attention to cybersecurity, followed by a wane in interest.

While cyberattacks may plague us personally or professionally, there are plenty of associated investment opportunities. Just like investors who explore pharmaceutical companies that aim to cure diseases, investors can likewise explore the cybersecurity industry that aims to cure the ills of cyberattacks.

Peter Chieco is a financial adviser with the Global Wealth Management Division of Morgan Stanley in Greenwich, Conn. He can be reached at 203-625-4897.