Institutional Investor

The Ongoing Battle of Cybersecurity

12 JUL 2016 - DAVID MARTIN

Cybersecurity is not a technical issue. It's a managerial problem that requires a new approach to risk management.

Imagine going down a river in a rowboat. Water seeps in, and you cannot see below the waterline — or, as it's called in cyberese, the attack surface. While on the river, you bail the water out, and upon arriving back onshore you patch the most obvious holes. The very next day, you purchase a new product that ensures the bottom of your boat is absolutely water resistant. Now, feeling highly confident that you solved yesterday's problem, you take the rowboat out on the river again. This time, you go over a waterfall and wreck the boat.

In cybersecurity, it's simply not a question of what could go wrong today but, rather, what if such things happen tomorrow. That's why companies need to become intelligence-driven organizations. In the simple case of the rowboat, researching the river's path might have caused you to change the course of the boat or, knowing that you had to travel over a waterfall, you might have lightened the load or strengthened

the boat. Gathering intelligence is the only practical way to become proactive in a cyberthreat environment that is constantly changing.

It's no longer a question of whether a company will be attacked but more a question of when — and what that company is going to do about it. Many IT organizations today cannot visualize and manage the attack surface of a company's entire cyberinfrastructure. According to research firm Gartner, the average lag time before a breach is detected is a shocking 205 days. Companies will not only have to demonstrate that they have controlled and reduced the attack space, but they will also need to have a data breach response plan in place and have the ability to manage a significant incident.

A cost-benefit approach can be a manageable way to approach risk mitigation. When serial bank robber Willie Sutton was asked why he felt compelled to heist financial institutions, he replied, "That's where the money is." The same goes for cybercriminals. That means a company has to decide what assets are the most valuable and then spend accordingly to protect them. In the asset management business, confidential client information may be the most critical for protection and should receive a disproportionate share of the cybersecurity budget.

The key to effective risk management of cybersecurity is the ability to assess, measure, monitor and control the risk. Companies now focus on breaches, which is really only the assessment aspect. They need to broaden their focus, develop new measures like cyberrisk tolerances and such innovative monitoring techniques as key performance indicators, and implement better cyberrelated controls that are incorporated in updated policies and procedures.

Companies also need to factor cybersecurity into their strategic decision making. In the world of the Internet of Things, there are few competitive advantages more critical than trust, and excellence in cybersecurity will become a distinguishing factor.
It is no longer acceptable to hire one individual with a strong technical and government regulatory background to manage cybersecurity. It will become

incumbent upon the board and CEO to ensure that cybersecurity is not a technical problem to be solved but, rather, an ongoing risk to be managed.

David X. Martin is a special counselor for the Center for Financial Stability, a nonprofit think tank in New York focused on financial markets.