CXO INSIGHT

Five Strategies for Better Cyber Protection and Defense

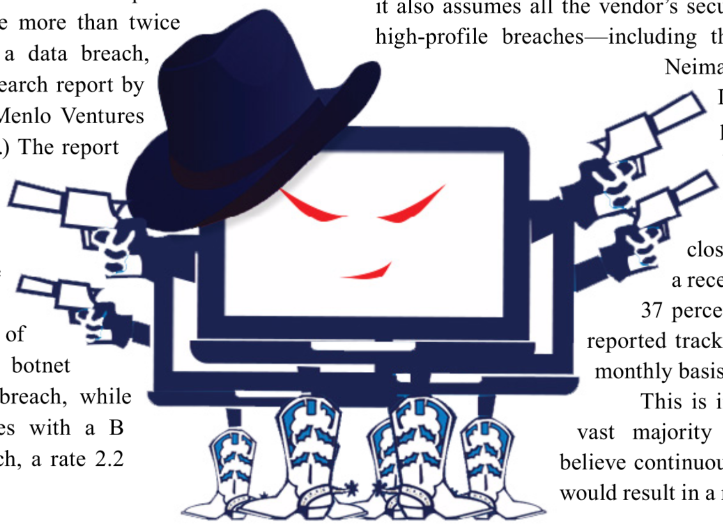
By Venky Ganesan, Managing Director, Menlo Ventures

Cyberattacks are intensifying at a shocking rate. The latest Internet Security Threat report from Symantec reveals the sobering numbers. Five out of every six large companies (those with more than 2,500 employees) were hit in 2014. There were 45 times more ransomware attacks IN 2014 than in 2013. There were nearly a million new pieces of malware released onto the Internet every day in 2014.

Why the dramatic increase? Like the Maginot Line, many of today's defenses are facing the wrong direction: backward, in this case. A lot of companies are using outdated, ineffective methods to keep them safe, building fortifications against the threat that was, not the threat that is and will be. They are looking at the rearview mirror instead of the windshield.

Here are five ways organizations can update and improve their cybersecurity:

1. Protect against botnets. Companies with weak botnet defenses are more than twice as likely to experience a data breach, according to a recent research report by BitSight Technologies. (Menlo Ventures is an investor in BitSight.) The report examined 6,273 large companies, of which 199 (3.3 percent) had experienced at least one recent publicly disclosed breach. Just 1.7 percent of companies with A-grade botnet defenses experienced a breach, while 3.7 percent of companies with a B or lower suffered a breach, a rate 2.2 times higher.



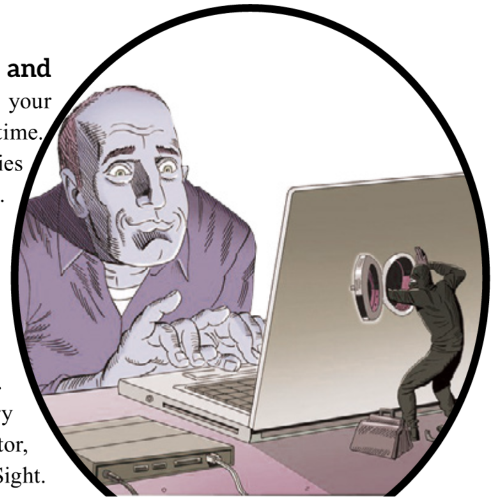
> "A lot of companies are using outdated, ineffective methods to keep them safe, building fortifications against the threat that was, not the threat that is and will be

2. Monitor security in the supply chain. When a company assumes a relationship with a third-party vendor, it also assumes all the vendor's security flaws. A number of high-profile breaches—including those at retailers Target, Neiman Marcus and Home Depot—were made possible by third-party vulnerabilities. Yet few organizations watch third-party security closely enough, according to a recent Forrester survey. Only 37 percent of survey respondents reported tracking vendor security on a monthly basis.

This is in spite of the fact that a vast majority of IT decision-makers believe continuous third-party monitoring would result in a major improvement of their security effectiveness in key areas, including identification time, event-remediation time and response time to high-profile incidents. It's clear that organizations, especially retail organizations, need to match their execution to their aspiration and do more work monitoring security in their supply chain.

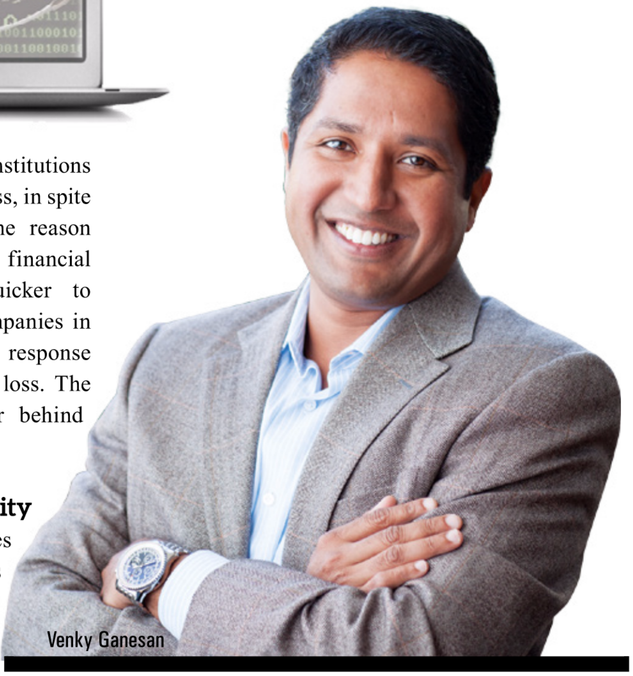
3. Generate a daily security rating. Credit bureaus have successfully used rating scales to score consumers and measure risk. This is something that that CIOs and CISOs should be doing as well. Personally, I'm very interested in platforms that are able to produce daily security ratings for individual organizations by gathering data on security outcomes—such as infected machines and improper configurations—from sensors deployed around the globe. Such a platform can analyze terabytes of data and then map it to a company's known networks to create an overall rating of its security strength. These ratings, based on externally accessible data, provide real-time visibility into a company's security posture and help it improve. They can also help reduce your cyberinsurance expenses as major insurance companies are using these scores to underwrite their policies.

4. Focus on detection and recovery. You can't protect your network from every hacker all the time. Hackers will get in and companies need to admit that unhappy fact. Don't spend all your resources on erecting an impenetrable wall—it can't be done. Focus sufficient attention on detecting the bad guys and quickly recovering from the incident when they do get in. The financial services industry does this better than any other sector, according to a report by BitSight.



The report rated financial institutions highest in security effectiveness, in spite of frequent cyberattacks. One reason for the high rating is that financial services companies are quicker to respond to breaches than companies in other industries. And faster response time means less damage and loss. The technology industry lags far behind financial services in this area.

5. Benchmark cybersecurity performance. Companies benchmark other business functions like customer service, sales and marketing, and human resources—so why not cybersecurity? While other corporate departments have embraced benchmarking, security teams are still working without a yardstick. But there are now tools on the market that enable security teams to compare their performance against industry averages on a continuing basis. These tools can also provide a quantified and comparative view of cybersecurity performance over time. With this kind of actionable benchmarking data, organizations can measure the effectiveness of risk-mitigation programs, communicate key indicators to the board and continuously improve their security posture.



Venky Ganesan

In spite of their increasing awareness, the cybersecurity problem is still much bigger than most organizations realize. That must change. We need to win battles now or risk losing the war later. Fortunately, the cybersecurity sector is poised for huge innovation and Menlo Ventures is investing more than $80M of our current $400M fund XII in cybersecurity.CR