Venture Capital and Early-Stage Security Start-ups

THE CYBERWIRE (Thursday, August 11, 2016) — Jeff Moss, Black Hat's founder, characterized this year's conference as being about speed (last year's was about complexity). Speed plays into the sector in many ways: speed to market, speed to produce products, and speed to counter threats. Speed, Moss noted, matters to boards and C-suites, and speed should matter to companies as they try to sell into the current market.

That's consistent with some of the lessons we drew from our conversations with venture capitalists. Don't make the mistake, if you're a start-up, of trying to sell a solution that's labor-intensive and takes a long development cycle for its implementation in a customer's environment. The shortage of skilled security labor is the biggest single source of marketplace drag. Your solutions should, above all, not exacerbate labor market drag. Ideally, it should alleviate it.

Casey Corcoran of FourV Systems agreed on the need for speed. "There are a number of companies with shelfware because they've never been able to get it to the place where it produces results for them." An eighteen-month implementation cycle is likely to never be completed. This is true, he thought, of many artificial intelligence tools as well—these tools have to be trained, and you often have to build an infrastructure around them.

We spoke with Allegis Capital's Bob Ackerman, who's long had a particular interest in the cyber security start-up ecosystem. He offered his perspective about some of the things early-stage companies should bear in mind. First, while the venture capital market has cooled a bit (generally, not just for cyber security) as investors have come to worry that the market may be overcapitalized, funding is still available. People are growing a bit suspicious of the unicorns, and they've taken note of the slow IPO market. Investment is still available, but cybersecurity companies who wish to attract it must show clear differentiation. They've got to prove their value in the marketplace.

There are some reasons for optimism, in Ackerman's view. Cybersecurity is no longer regarded as a speculative investment. And enterprises no longer regard expenditures on cybersecurity as discretionary.

But to attract investors, Ackerman noted, you must be differentiated from the others in the sector. There are a lot of point solutions on offer that might be nice as a feature, but that won't sustain a company. Don't be one of those offering a point solution. Go for disruption, and be clear about your value proposition.

We also spoke with **Alberto Yépez,** managing partner at Trident Capital, who leads a sector-focused venture capital fund investing only in cybersecurity. Like Ackerman, Yépez sees cyber investment as affected by a general slowdown in the venture industry, but he stresses that the amount of capital available for investment in cybersecurity remains very large. But the bar to getting funded has been raised. You've got to show sound fundamentals. Yépez summarized the VC's criteria for investment as follows. All five areas should align:

1. Market—should be large and growing,
2. Technology—how hard is it to replicate what you do? High barriers to entry are a must.
3. Go-to-market—how are you going to deploy your solution? Will you do it yourself, or will you work with a partner ecosystem? We look for the latter: strategic relationships will make you grow.
4. Team—we look for someone who can assemble a team (with appropriate domain expertise) that can go to market.
5. Investment community—do you have the right interest from investors?

Both Ackerman and Yépez agree that the shortage of skilled professional labor and the high cost of integrating point solutions define the gaps that are crying to be filled by innovative companies.