LABRADOR VENTURES

WWW.LABRADOR.COM

Look for 'Micro-Dots' of White Space

by: Sean Foote, Labrador Ventures – April, 2005

Sometimes, market opportunities are as obvious as billboards. Other times, they're more like street signs. And then, in crowded markets where technologies have matured and VCs have already placed their bets, market opportunities are more like micro-dots of white space on already well-worn canvases.

Sean Foote

As seen in the...

VCJ

Venture Capital Journal

LABRADOR VENTURES

101 UNIVERSITY AVENUE

FOURTH FLOOR

PALO ALTO, CA 94301

TEL: 650-366-6000

FAX: 650-366-6430

In fact, one pass through the RSA Conference in San Francisco in February confirmed just how hidden certain market opportunities can be.

In the once wide open market for security technology, suddenly everything looks the same. Anti-spam. Anti-spyware. Anti-virus. Anti-phishing. Anti, anti, anti-everything. In markets like that, it's easy for investors to cut and run. Many fellow early stage investors already have. Though capital spending on security technology is now estimated at roughly 4% of total cap-ex spent on technology, that expanding commitment within IT budgets has been offset by multiple well-funded early, mid- and later-stage security companies offering products and services as far as the eye can see. Moreover, product differentiation between such companies has grown so thin it's become difficult to find market opportunities large enough to justify several rounds of investment, let alone a single Series A round of funding.

As Peter Christy, Principal with NetsEdge Research Group notes, "Even great mathematicians are having difficulties getting their voices heard or convincing others to wrap business models around their innovations." Indeed, with over 250 companies presenting their wares at the RSA show, one has to wonder just what solution hasn't yet been invented? Yet, for better or worse, network, desktop and application security threats are growing faster than they can be addressed – even with all of the startups and venture capital that's been thrown at them. "CEOs who five years ago would have said they spent zero dollars on security technology now cite it as one of their greatest concerns," says Christy.

Most in the industry agree that the perimeter around the enterprise – the moat, the gates, the walls defending its most precious assets – is disappearing. Now, the edge of the enterprise is wherever the end user happens to be. And end-users are no longer simply employees, but now include vendors, contractors, consultants, or customers who must interact with a company's data and processes. If the great promise of technology was a fully automated supply chain that spits out endless amounts of data to be analyzed and integrated into ever larger and more complex systems, we got our wish.

For early stage investors this doesn't just mean more due diligence prior to making another security investment. Rather, it's about finding those micro-dot sized white spaces of opportunity that allow us to cut through the clutter and noise within the industry, and then place significant and intelligent bets on the technologies and entrepreneurs capable of capitalizing within those unique areas.

Proactive Approach

In March 2001 we invested in GreenBorder Technologies, which had a simple yet elegant technology for making Internet Explorer and Outlook safe to use. As with other firms, we had started off looking at all of the "anti" companies at just about the time when all of those anti-everything startups were getting a bit over-fished.

Everybody was, and still is, looking for better, faster, cheaper solutions in big fast growing markets. But fancy technologies that don't address true business security problems are relatively useless. And companies targeting markets where three to four startups have already been funded seemed like an equally silly proposition. GreenBorder addressed both: It had differentiated technology that took a proactive approach to security-related business pain. The basic problem was that end users needed more access to do more things within the enterprise. Users could no longer be virtually imprisoned in an environment where IT departments were on a "patch management treadmill," as GreenBorder CEO Drew Hoffman puts it. "There are only so many fingers you can keep putting in the dike before that doesn't work any more," Hoffman says.

GreenBorder thus created a virtual desktop where a user could open any attachment, read any email, or go to any website all within a metaphorical invisible force field of safety. "We aren't trying to be all things to all people," says Hoffman, delineating his own sliver of white space with the simple proposition of making IE and Outlook safe to use. Because connectivity to the Internet has largely become equally ubiquitous and business critical, the fortress around the enterprise had become more difficult to defend; the fortress walls were challenged because the user had

cont.

now become more active and was traveling far beyond the original security boundaries any IT person had foreseen.

In this example, GreenBorder's micro-dot of opportunity wasn't just within its technology solution, but within its differentiated approach to how one looks at security. Most companies remain reactive – a new worm, virus, or Trojan horse requires first figuring out the threat, then creating a signature for it, then distributing that signature. In a proactive approach, the security solution relies not on detection but on protection. With a safe zone – a virtual courtyard for safe user interactions with the Internet – T managers no longer have to be on the threat detection/patch management treadmill. If GreenBorder could free up those resources, it could give users a far greater range of access without changing their behavior, allowing technology and business problems to each be solved simultaneously.

The next area of white space that's piqued our interest lies within the evolving micro-economies being formed by the maturing security technology industry itself.

We already know that technology, with all its latest bells and whistles, had overwhelmed even the most experienced IT staff. For example, though large scale customers, and/or their security technology providers, now have huge numbers of IT employees to monitor break-in attempts, alerts, permits and denials, they are literally drowning in that flow of information. The business of security information management systems (SIMS) and outsourced service providers was born to address this pain and quickly became heavily invested with multiple competitors between them, but therein lies a "picks and shovels" solution of its very own.

Though SIMS give enterprises control over all the data overwhelming IT managers – allowing them to simplify and normalize information from disparate security and network devices – those SIMS are often hampered by several gating factors. First, though a SIM system can pick apart 10,000 events and analyze which ones really matter, the degree to which the rules for that parsing project can be sliced into even greater detail is critical. The more detailed the rules, the more accurate the slicing. Second, as businesses have now begun operating in "real time," they are quickly moving away from "iterative reporting" – the process of logging events just once or twice a day.

If a SIM system can sit on a platform that allows it to be fed, and thus sift through data in real time rather than iteratively, the value of that software goes up exponentially. If the real time data can further be screened for even tinier details, the parsing rules become that much more valuable. If a SIM system developer can concentrate on rules and reporting instead of the underlying platform speed and architecture, the product is more profitable and quicker to market still.

EventGnosis, a very early stage startup, created its own platform to manage and monitor thousands and thousands of 'events' in real time while helping accomplish all three of these activities – data analysis, sifting and parsing. It's a "picks and shovels" solution for the industry's larger SIMS players to use and pass through to their own customers. A market opportunity that's also an offshoot – a "tool set" really – for the much bigger-picture security problems facing some of the world's largest corporations. As EventGnosis and others now realize, if the first-tier customers can use the tool sets to build better products and services, their own customers will beat a path to their door.

Seeing Into the Future

A third micro-dot of security technology involves evaluating not merely where the market is or where it's going, but in figuring out where future security threats may ultimately lie. It's not just about solving the next problem in security, it's about investing in a company that will be one of the first, if not *the* first, to know what that problem is and from which source it will emerge.

Kelkea, a San Jose, CA-based company, has roots that go back to 1996 with the formation of Mail Abuse Prevention Services LLC, (the first anti-spam company). It addresses this problem by attempting to stop spam at its source. Built over the past 8 years, Kelkea's reputation database is the largest in the world, with ratings for more than 1.5 billion IP addresses. As a result, some of the largest ISPs, including AOL, RoadRunner, BT, and Telstra, use its services to fight spam. And much like EventGnosis, Kelkea is filling out that second tier of emerging companies selling the picks and shovels necessary for others to fight emerging security threats.

But that's only part of the market opportunity. Because Kelkea's reputation database is so vast and deep, it can go one step further into the future. By analyzing an entity's behavior over time, allowing it to know who it is dealing with and what that source's actions have been, Kelkea can help customers make informed decisions about a source's future behavior. Carried one step further, threat patterns from various sources can be analyzed to accurately predict the greatest security problems for IT managers tomorrow. Few startups have the data necessary to make such predictions accurately; Kelkea could be one of the first.

These three micro-dots of white space listed above are, of course, only a fraction of the opportunities that can emerge within the security industry for early stage investors. And, indeed, analysts such as Peter Christy claim that the real opportunities are only now beginning as technologists finally address real-world business problems. Yet, by looking below the surface, as far below as those micro-dots of white space, VCs will surely find some of the most interesting and exciting opportunities the security industry has ever seen as we recognize that the search is growing harder every day.

This is one in a series of monthly columns on seed and early stage investing that Labrador Ventures was selected to contribute to the *Venture Capital Journal*.

Sean Foote is a partner at Labrador Ventures, a Silicon Valley seed-stage venture fund. He may be reached at sfoote@labrador.com