

# Boston Business Journal

Volume 24, Number 5

## Hub becomes hotbed for network security talent

BY ALEXANDER SOULE  
JOURNAL STAFF

**T**ime was, an information technologist had to make a pilgrimage to the RSA Conference in San Francisco to find critical mass of security-minded IT industry types. No more.

While many area software executives attended the annual RSA show last week, the Boston area has nurtured its own bloc of computer and network security companies that is breeding new talent — both for code-level software security startups, as well as for companies needing to lock down their networks from intruders.

The area has long been home to a few security industry icons: the Laboratory of Computer Science at the Massachusetts Institute of Technology, networking pioneer BBN Technologies Inc., and RSA Security Inc., the Burlington firm whose public key infrastructure technology enables data to pass unmolested through networks.

But a growing phalanx of security firms have emerged locally that are winning attention in their own right, and forming the roots of a significant industry cluster.

There are a few reasons for the cluster's formation, say area executives. While the presence of RSA, BBN and MIT help, equal weight is given to the region's existing cluster of firms with collaboration software and networking expertise.

Only a few local security technology companies are publicly held, making it difficult to estimate employment levels in the sector. RSA had long been the largest, with 1,000 people today, but has since been eclipsed by Enterasys Networks Inc. with 1,500 employees. Enterasys retooled its product line a few years ago to emphasize security applications, while moving its headquarters from New Hampshire to Andover.

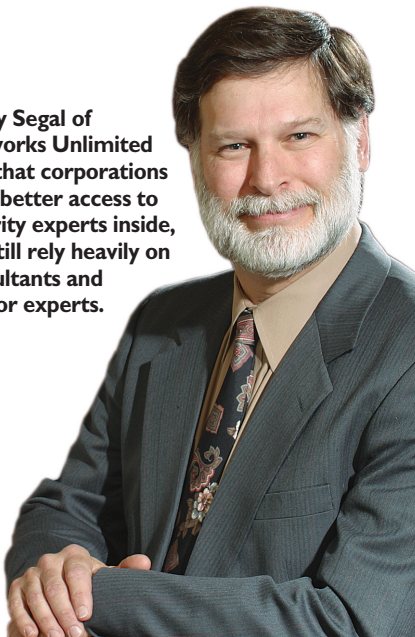
Enterasys chief technology officer John Roese said that Enterasys was forced to purchase whole companies to keep its security expertise in line with market demand, but that even now it struggles to do so.

"In 2000 it was brutal and that was why we did acquisitions," Roese said, comparing then to today. "We never could have gotten the people we needed by hiring incrementally. We also refocused our engineers and got them to participate in (security) standards bodies."

Such shifts of talent make it difficult to estimate staffing changes within companies. The Information Technology Association of America said in August that 63 percent of the time, companies fill cybersecurity positions by retraining employees they already have.

Security is one of the few IT sectors not to have a drag on salaries from the trend in outsourcing, said Foote Partners LLC, a Connecticut-based IT compensation research firm. A Foote Partners survey in January found that IT workers earn 23 percent less today than in 2001, but those with certain security certifications won increases between

**Harry Segal of Networks Unlimited says that corporations have better access to security experts inside, but still rely heavily on consultants and vendor experts.**



W. MARC BERNSAU / BUSINESS JOURNAL

12 percent and 25 percent.

The Massachusetts Software Council lists Waltham's Netegrity Inc. as is the third-largest security company in the area, with more than 350 employees.

Stephanie Feraday, vice president of marketing for Netegrity, noted that it was only last year that the RSA Conference added a program for CISOs, or chief information security officers of corporations, an emerging designation at some companies in addition to the chief information officer.

Fresh off \$8.5 million in financing, CoreStreet Ltd. is one-tenth Netegrity's size, but plans to double its staff within the next year. The company's board of investors

includes MIT professor Ronald Rivest, who is the "R" in RSA.

"We could not have put together 35 people four years ago," said Phil Libin, president of CoreStreet, who agreed with peers at other companies that market forces have been most responsible for the deepening well of talent. "There has been a spate of articles in security-oriented magazines over the past few months talking about the convergence trend. People are no longer interested in buying technology like PKI (public key infrastructure, a protocol that unlocks data for specific users). They want to buy applications."

When Harry Segal founded Hudson-based Networks Unlimited Inc. in 1985, few companies outside of banks gave much thought to securing data, and their efforts were clumsy at best.

By 1990, more companies were attempting to create secure, continuous connections between branch offices. In 2000, firewalls and anti-virus protections were common, he said, and large companies were beginning to employ sophisticated intrusion-detection systems.

That level of sophistication is beginning to trickle down to midsize companies with less than 2,500 employees, Segal said, but added that it is still very challenging for such firms to find employees with outstanding credentials in computer security.

"You tend to see people who may have some of the ingredients — they come out of an end-user environment where they were running one to five firewalls, but to a large degree they don't understand the innards," Segal said. "They can't drill down and understand the (Internet) protocol adequately and understand how the attacks are crafted. They don't have a good comprehension of how hackers work, and how to compensate."

Ed Gaudet, vice president of product marketing at Lexington's Liquid Machines Inc., said that the steady drumbeat of hacker attacks has helped raise security to its present level of attention.

"Security didn't have its rightful place in the enterprise until recently," Gaudet said. "(Before), everything was about generating top-line revenue in ways that leverage the Internet. A pretty significant amount of the IT budget goes into security projects now. It has been an expense item for a number of years, a necessary evil. I think now that people are starting to understand its importance."