Arizona Republic

Cybersecurity Valley

by Rich Davis and Vinnie Liu
Phoenix, 14 July 2013

As Presidents Obama and Xi Jinping of China met in California last month to discuss, amongst other things, cybersecurity and the attacks emanating from China on the American government and industry, white hat security professionals based in Arizona were busy protecting our nation's top companies from the very same threats.

While the issue of cybersecurity has been receiving a great deal of media attention lately, most of it leaves the reader or viewer with the idea that government is leading the charge to defend our country from cyber threats across the globe. The actual situation is quite different. The US Government is focused on cyber warfare and is doing very little to help American companies address cyber espionage and theft from China, the Middle East and the crime syndicates of Eastern Europe.

For example, a senior executive at a Fortune 50 manufacturing conglomerate recently informed us that Chinese hackers had stolen deepwater drilling equipment designs and that they would soon be facing stiff competition with Chinese manufacturing firms that were copying their proprietary equipment using stolen designs. Theft like this has become commonplace and defending against it has become big business.

General Alexander, the head of the U.S. Cyber Command and the National Security Agency recently said that cyberattacks are causing "the greatest transfer of wealth in history." McAfee, a security software company, estimates that the global cost of cybercrime exceeds $1 trillion.

The challenge of defending against these hackers is far more complex, requiring more than just technical solutions, than one may imagine. Oftentimes, hackers are offered entry into highly sensitive computer environments by the actions of an unsuspecting employee on the system. American government hackers were able to disrupt Iran's nuclear enrichment program by leaving memory sticks with an embedded virus at public venues where employees of the nuclear facility visited.

The crime syndicates of Eastern Europe have become masters at understanding human behavior and interaction with technology. Who hasn't received emails that looked like they were from a friend or colleague when in reality it was a cleverly designed attack?

The hacking menace so threatens our economic well being that it is critical for public and private sector leaders to push for the development a strong cyber defense industry that can protect our economic interests and national security. Though our government will continue to develop cyber warriors, an even greater number of security professionals and companies will be needed from the private sector. So where will these cybersecurity professionals work and their cyber defense companies be based?

How about Arizona?

Arizona is uniquely positioned to develop a "Cybersecurity Valley". We have real talent here. Cybersecurity professionals based in Arizona protect many of America's top companies. Arizona State University has a budding Information Assurance Center and schools like the University of Advancing Technology in Tempe produce recruits for clandestine agencies of the U.S. Government along with feeding cybersecurity firms with young talent.

For a variety of reasons, which include the high tech environment, existing defense contractors, and a rare

blend of Google style culture in existing firms, some of the brightest cybersecurity talent is drawn to the Valley. The talent is attracted by boutique firms like Bishop Fox and Securosis, in part, because they protect many of the Fortune 100 and because the firms recognize and appreciate the inclinations for working odd hours from strange locations like the couch and the café. Even large companies like Honeywell, Charles Schwab, and American Express have some or all their security teams based in the valley, while other research firms like ARTIS work to understand human and state behavior related to cyber warfare.

With this burgeoning base of talent, the question is, 'what can we do to encourage the cybersecurity industry to further develop in Arizona akin to something like the Silicon Valley'?

For starters let's look at two models used in other states to capture and develop an industry. In the 1940s, the Dean of Engineering Stanford School, Frederick Terman, encouraged the students at Stanford to start their own technology companies. Successful enterprises stayed in the area to capture the talent being produced at the engineering school. Students at Stanford used the term Silicon Valley until it became recognized as the commercial persona of the region attracting capital and investment from all over the world. Today the Silicon Valley has over 40,000 high paying, high-tech jobs.

The Research Triangle Park in North Carolina was started in 1958 when leaders of Wachovia Bank, Duke University, NC State University and the University of North Carolina partnered with then Governor, Luther Hodges, and several entrepreneurs to privately buy up land and market it as a research park, in part to attract new industry and to stop the 'brain-drain' from the state. Today the park is one of the largest research centers in the world, housing140 companies and employing 38,000 people.

Cybersecurity firms and professionals are in high demand. There is a massive amount of money looking for investments in the security field, especially from venture capital and private equity. As the world continues to technically evolve, the cybersecurity industry will be a job creator for years, perhaps decades, to come. These are high earning jobs that, if geographically concentrated in Arizona, could increase the standard of living for all Arizonans.

The competition for cybersecurity professionals is robust. Large defense contractors, mostly located in Washington DC, have bought up many boutique cyber penetration and defense firms only to realize a culture clash that has resulted in much of that talent leaving, some returning to Arizona. As the private sector talent pool increases, Arizona has a real shot at hosting the nucleus of the industry.

What we need now is for all of our universities to further develop specific degree programs in information security and for a few community leaders, university presidents, local banks, entrepreneurs and industry leaders to come together to make the "Cybersecurity Valley" a reality.

Rich Davis is the CEO for ARTIS Research, a conflict research firm based in the Valley. He was the former Director of Terrorism Prevention at the White House.

Vinnie Liu is the Co-Founder and Managing Partner of Bishop Fox, a cyber penetration and defense firm based in the Valley. He was a former security professional for the National Security Agency.