



June 1, 2011

Power of many: Government and private sector alliance

By Ryan Goldberg

<http://www.scmagazineus.com/power-of-many-government-and-private-sector-alliance/article/pP6W8XXJVKI%3d/t/>

*Government and industry partnerships have been slow to take shape, reports **Ryan Goldberg.***

At the center of national cybersecurity policy for the last decade has been the voluntary partnership between government and the private sector. But this marriage is well past its honeymoon period. After all the vows to love each other and stay committed, it has turned out to be harder in practice than either side expected.

As a policy to defend the Commons, this relationship finds itself at a crossroads. The current debate over how to approach cybersecurity – particularly after a year that saw major breaches of Google and other Fortune 500 companies, the Stuxnet worm and denial-of-service attacks over WikiLeaks – is framed as one between continuing this partnership versus greater government regulation.

An assortment of industry groups – including the Business Software Alliance, Internet Security Alliance (ISA), privacy groups and the U.S. Chamber of Commerce – released a white paper in March reaffirming their commitment to an assertive voluntary partnership of equals. Their approach reinforces what the Obama administration concluded in 2009 in its Cyberspace Policy Review, which called for, among other things, procurement and tax incentives to add some legs to the partnership.

The problem is that most of these decade-old prescriptions “simply haven’t been implemented,” says Larry

Clinton, ISA’s chief executive. “Our cyber systems are not as strong as they should be and can be.”

The internet wasn’t designed to be a global infrastructure on which so many people would depend. That cyberspace is under constant attack comes as no surprise – the economic and legal incentives favor the attackers. The internet has stayed open and free. The 2003 National Strategy to Secure Cyberspace expected, wrongly as it turned out, that market efficiencies would drive companies to allocate money to security. It also established the public/private partnering as official policy. The 2006 National Infrastructure Protection Plan refined this partnership.

But issues of competition among companies and mistrust about sharing information between industry and government have buffeted this arrangement. Each side, Clinton says, harbors different motives.

The private sector looks at risk in economic terms, whereas the public sector must consider economics alongside the law, national security and politics. In addition, private companies own 85 percent of critical U.S. infrastructure. Clinton says companies have been quick to savor the benefits of the internet, but slow to spend on cybersecurity.

James Lewis of the Center for Strategic and International Studies calls these problems intractable. A January report he co-authored recommends a greater regulatory backbone to give companies and agencies more “skin in the game.” It also calls for a more comprehensive national strategy and scrapping voluntary partnerships for binding contractual obligations among sides.

The present back-and-forth debate sounds “so theoretical because it is theoretical,” says David Koretz, CEO of Mykonos Software, which provides web application security products. Koretz, who founded Mykonos in 2009, says there are technical and cultural reasons for why a robust alliance rooted in information sharing has not been achieved. “In order to agree to share information there’s an assumption that we have the information to share.”

That assumption, Koretz says, is false. The ever-increasing sophistication of cybercrime has stayed ahead of the defenses against it. He recently conducted an informal poll of

CISOs and found that 80 percent would be unable to identify when they were sustaining a web-application attack, and the rest acknowledged they would only know afterward. Security programs are “like a fire alarm that tells you your house burnt down two weeks ago,” he says.

Hovering above the technical deficiencies – as well as the demands on companies to filter through endless data and then decide what to share – is a cloud of suspicion. “Go ask a CEO how interested they are in sharing confidential data on who’s attacking them and why and you’d find great reticence,” Koretz says.

Amid the uneven history of public-private partnerships, several successes stand out. Few others have done as much as Robert Rodriguez, a former Secret Service agent who founded the Security Innovation Network.

Although he admits these partnerships have been maligned over the years, Rodriguez says their execution takes time. Calls for a change in policy ignore the incremental nature of bringing together different communities. “It’s hard to scale it over a global and domestic environment,” he says.

In December 2001, Rodriguez created a partnership in California mandated by Congressional law: the Secret Service Electronic Crimes Task Force. He built it up from two people to 200, bringing in universities like UC-Berkeley and Stanford and companies like eBay and Wells Fargo.

Rodriguez retired in June 2004 after 22 years in the Secret Service, and pivoted to entrepreneurship. He started two more public-private partnerships based at Stanford, including the IT Security Entrepreneurs’ Forum, which matches Silicon Valley with the Beltway.

And, he sees progress. Five years ago, CISOs would never share information with their industry peers, but now they do because they’re putting out fires every day, he says.

Will Pelgrin, the chair of the Multi-State Information Sharing and Analysis Center (MS-ISAC), may offer the best example of the potential for collaboration between government and industry. Pelgrin, then the CISO of New York State, started the center in 2003 with the Albany State Police and Department of Homeland Security.

MS-ISAC is now part of the nonprofit Center for Internet Security, where Pelgrin is the chief executive. It includes all 50 states, four territories and representatives from critical industries, federal and state government, and the military and intelligence communities.

“I’m going to share no matter what,” he says. And, this may be catching on. ISA’s Clinton also counts the creation of the Critical Infrastructure Partnership Advisory Council legal structure and the development of cybersecurity standards and best practices by several standard-setting organizations as additional accomplishments. But for renewed direction at this decisive moment his sights have turned toward a century ago.

In America at the turn of the 20th century, the telephone and electricity were revolutionary technologies not serving the broad public interest. Similarly for cybersecurity today, he says, the goal should be to inject market forces into the system to provide incentives for innovation and investment, and encourage information sharing.

The answer should not be a divorce, Clinton says. “We are at a point in our relationship where we have to do some hard work. We have to stay together – for the kids.”