**An Assessment of the Viability of Public-private**

**Partnerships on Cyber Security**

**Preface**

The exponential growth of cyberspace has allowed the United States access to numerous economic opportunities, but has also allowed our adversaries equal access to threaten the security of such opportunities. More and more of the USA’s private, institutional, and government information are being stored in digitized databases and traveling through insecure networks, vulnerable to hostile cyber attacks. Protecting this information is critical to the security of the United States, just as important as the physical defense of our borders. A hostile breach of our cyber security can give our adversary almost uninhibited control of the United States’ military secrets, its arsenal, and essential state infrastructures such as electricity, water, and financial services. (1)

But the government cannot single handedly ensure the safety of American cyberspace, as an overwhelming portion of the cyberspace is operated and used by the private sector. (3) Therefore, the cooperation of the private sector is vital to the goal of making the cyberspace secure. While the government should provide leadership and articulate clear policy expectations pertaining to cyber security, the private sector should share the responsibility to make its own information secure.

**Executive Summary**

1. Government should provide an encryption API (Application Programming Interface) to help small private firms keep their data secure. Many resource-strapped companies simply cannot hire cyber security experts; such experts are prohibitively expensive for many cash-strapped companies. The first step to cyber security is removing the material barriers for the private sector.
2. An independent panel of industry leaders in Silicon Valley, convened and paid for by the government, should select industries that present the highest security vulnerability, and should direct the government’s attention to those key industries.
3. The government should strive to create an atmosphere that reward security programmers. With so many applications that deal with sensitive information, the only way to ensure a comprehensive defense of cyber resources is to make more developers knowledgeable about them.

**Recommendations of the Cyber Policy Review**

The policy review makes two broad recommendations on approaching cyber security partnerships with the private sector. 1) Assign monetary incentives to cyber security, so that private firms would have an incentive to reform, and 2) minimize the institutional and policy confusion coming from previous uncoordinated partnership efforts with clear policy. (1)

1. *Monetary incentives*

Because of the large costs associated with security maintenance of software, the management will not risk the bottom line voluntarily unless there is a clear regulatory reason to do so. The report states, “The private sector often seeks a business case to justify the resource expenditures needed for integrating information and communications system security...” (1) Adopting software safety measures will have to be done under the government’s direction, just like the adoption of environmental or labor regulations. American corporate history has shown that companies are willing to engage in child labor, human rights abuses, and systemic environmental damage for profit, if government directives do not prohibit them from doing so. (2) Just as the government gave the private sector a reason to clean up its labor policies and install water filters, it can and should tax companies that do not protect the information of their customers.

1. *Streamline government policy/ agencies*

There are many existing models of private-public cyber security. The models that the report pinpoints include the Enduring Security Framework, the Sector Coordinating Councils, the Infragard of the FBI, and the Enduring Security Framework. (1) The main problem with these programs is the large overlap of their objectives and responsibilities. The Enduring security Framework “has been forged to examine issues surrounding critical infrastructure network security,” (3) and the Infragard of the FBI was created to “increase interaction and information sharing among Infragard members and the FBI regarding threats to critical infrastructures, vulnerabilities….” (5) Indeed, many of the agencies and cooperatives noted in the Review have overlapping members and have fulfilled similar functions over the years. These organizations represent knee-jerk reactions by different government agencies to various security breaches, designed out of political pressure rather than substantive policy mandates. The Review recommends that these various agencies and platforms be streamlined and centrally coordinated by the federal government. (3)

**Concerns Regarding the Recommendations**

Providing monetary incentives to private companies have to follow a careful consideration of the private firms’ variance in capability. Not all firms are capable of securing their cyber assets even if they were willing; the cost of hiring security experts are prohibitively expensive for some companies, especially smaller ones. (2) Furthermore, some firms may not be able to cooperate with the government due to the sensitivity of the information they handle; for example, it may not be appropriate for a bank to share access to their database containing the financial information of its clients with government agencies. A crude monetary incentive for implementing security systems cannot suffice, because such a policy arbitrarily punishes firms that are incapable of abiding by it.

Monetary incentives may also create diplomatic issues. Web services provided by foreign vendors pose cyber security risks to the United States if used by Americans. However, requiring foreign companies to adopt security measures is difficult, as they are based in different jurisdictions that will not expect the same of their cyberspaces. Even if foreign firms can be coerced into abiding by security guidelines, such technical requirements – even if promoted in the name of national security – can be interpreted as attempts to create trade barriers. (6) A security requirement could easily be interpreted by less technologically advanced nations as preferential treatment for American firms, with easier institutional access to cyber security frameworks.

Streamlining existing frameworks to create private-public partnerships is a noble idea, but the government should not actively participate in securing private cyberspace until it can demonstrate the robustness of its own cyber security. The most oft-mentioned objection against public-private partnerships that share information of security vulnerabilities is that the information shared with the government is not secure. The government should assist industry-wide efforts to secure private cyberspace with policy and providing initiatives with clear value propositions, until it is capable of providing technical direction.

**Action Plans**

Before the government can start requiring and prodding the private sector to keep the cyberspace secure, it must remove existing barriers facing private companies. As mentioned, these barriers are numerous and substantial, the most important of which is the high cost of security technology.

First, the government can provide direct technical support by providing an API[[1]](#footnote-1) (Application Programming Interface) for encrypting and protecting data. Something as simple as a secure sockets layer can be extremely useful in providing primitive protection. Direct technical support is advantageous in that it immediately makes implementing secure software easier. It is already widely practiced in industry, with framework owners such as Apple or Google providing debugging and API support to developers working with their frameworks. Such API support has been extremely successful. In fact, Apple’s systemic support of its developers has made iOS programming very easy, allowing even beginner developers to quickly launch workable applications.

Second, the government should lower the long-term cost of security software engineering through signaling the labor market. The government should work with companies to prefer programmers with experience in security programming. It should also offer scholarships to students wanting to explore careers in information security. One of the main reasons security classes are not widely taught or taken by computer science students is that knowing security is not big with employers. (6) Once the government indicates a higher demand for security programming to the market, students will respond by taking security related classes.

Third, the government should focus on protecting the cyberspace of a few key industries. It’s unlikely that the intrusion on the Abercrombie and Fitch website will jeopardize the safety of the American cyberspace, but attacks on banks and power plants will. These industries pose greater security risks and therefore merit more protection. The government should work with experts in the private sector to identify these key industries, and direct its policy goals toward them.

**Conclusion**

This Assessment recommends that the government focus on removing barriers to building secure programs in the private sector. Stacking more regulations and requirements without an earnest attempt to lower costs of compliance will not result in a more secure cyberspace. Private-sector solutions with focused government leadership, in which the state assists and does not require will.

**References**

(1) United States. Executive Office of the President. *Cyberspace Policy Review Assuring a Trusted and Resilient Information and Communications Infrastructure.* Washington, DC: Executive Office of the President of the United States, 2009. Print.

(2) CSIS Commission on Cybersecurity for the 44th Presidency, Securing Cyberspace for the 44th Presidency, December 2008, at 49ff.

(3) Internet Security Alliance, Issue Area 3: Norms of Behavior—Hathaway Questions,

March 24, 2009, at 2, 4-7

(4) Corrin, Amber. "DOD Considers Shielding Private Networks -- Washington Technology." Washington Technology. Web. 08 May 2012. <http://washingtontechnology.com/articles/2010/05/27/strategic-command-einstein-cybersecurity.aspx>.

(5) "InfraGard - Public Private Partnership -Federal Bureau of Investigation (FBI) | About InfraGard." *InfraGard - Public Private Partnership -Federal Bureau of Investigation (FBI) | About InfraGard*. 08 May 2012. Web. 08 May 2012. <http://www.infragard.net/about.php?mn=1>.

(6) Written testimony of Scott Charney (Microsoft) to the House Committee on Homeland Security, Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, March 10, 2009, at 4-5.

1. An application programming interface (API) is a specification intended to be used as an interface by software components to communicate with each other. [↑](#footnote-ref-1)