INSIGHT

Making a Case for Cybersecurity R&D

Author: Samuel S. Visner, Senior Vice President and General Manager, Cybersecurity, ICF International

Cybersecurity is a national imperative. In his January 2015 State of the Union speech, President Obama equated combating cyber threats with combating terrorism. He has issued multiple presidential directives on protecting cyberspace and our technology-enabled critical infrastructure, and signed Executive Order 13636 Improving Critical Infrastructure Cybersecurity. With the importance of cybersecurity made clearer every day, the critical next step is identification and prioritization of the cybersecurity issues we face, including research and development (R&D) challenges that must be met.

This concern is not new. Testimony offered to Congress by the U.S. Government Accountability Office (GAO) in 2009[1] pointed to the need for such a strategy. A 2013 GAO report[2] noted:

> *"The goal of supporting targeted cyber R&D has been impeded by implementation challenges among federal agencies. In June 2010, GAO reported that R&D initiatives were hindered by limited sharing of detailed information about ongoing research, including the lack of a repository to track R&D projects and funding, as required by law. GAO recommended that a mechanism be established for tracking ongoing and completed federal cybersecurity R&D projects and associated funding, and that this mechanism be utilized to develop an ongoing process to make federal R&D information available to federal agencies and the private sector. However, as of September 2012, this mechanism had not yet been fully developed."*

We must move from our current strategy of intent—we want to be protected—to a strategy of responsibility, resources and action. Protection now and in the future will require sustained scientific research and technological advancement. It also will entail collaboration from the public and private sectors, along with academia. In other words, we need a whole-of-nation approach to cybersecurity research and development.

[1] See: http://www.gao.gov/assets/130/121810.pdf, accessed 1/30/2015.
[2] See: http://www.gao.gov/assets/660/652170.pdf, accessed 1/30/2015.

As a point of reference, we can recall the scale of post-WWII efforts in other national security domains such as nuclear energy and aerospace engineering. Meeting these requirements successfully demanded an orchestrated effort by government, industry, our national laboratories, universities, and leading think tanks. Now a similar partnership is mandatory to identify our cybersecurity R&D goals and assign responsibility to the parties best suited to achieving them.

Some competing priorities to consider:

- The "Internet of Things"[3] continues to grow and will drive the need for Internet Protocol Version 6 (IPV6) that will add billions of new IP addresses to the Internet.[4] **How can we secure so many interconnected things?**
- As cloud computing capabilities and shared resources continue to proliferate, organizations and individuals no longer necessarily control all the infrastructure they are using. **How can assets outside of one's control be secured?**
- We are deploying new IT capabilities to the battlefield, building quantum systems, developing optical systems, and more. **How can old systems secure evolving technologies?**

How do we get there? How do we address these issues and other vital challenges? We need to convene cybersecurity leaders at the national level to define an approach that encompasses the need to identify national cyber priorities, existing R&D resources, and gaps in the nation's R&D base by:

- Establishing the means of identifying the cyber R&D challenges to be met and problems to be solved.
- Pulling together a national R&D community capable of addressing these challenges and problems.
- Creating the architecture by which challenges, problems, responsibilities, and resources are allocated.
- Institutionalizing continuing effort to cultivate and improve national cyber R&D resources.
- Ensuring the fruits of cyber R&D are applied to the nation's cyber challenges and problems.

Advanced thinking about cybersecurity is taking place in many venues around our nation. Coordinating this thinking against prioritized challenges and allocating resources accordingly is the next step. With support from the White House, it's a step we can take.

[3] Defined as the interconnection of uniquely identifiable embedded computing devices within the existing Internet infrastructure.

[4] To connect devices across the Internet, each device must have an Internet protocol (IP) address. Internet Protocol version 6 (IPv6) is the latest version of the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet.

icfi.com

About ICF International

ICF International (NASDAQ:ICFI) provides professional services and technology solutions that deliver beneficial impact in areas critical to the world's future. ICF is fluent in the language of change, whether driven by markets, technology, or policy. Since 1969, we have combined a passion for our work with deep industry expertise to tackle our clients' most important challenges. We partner with clients around the globe—advising, executing, innovating—to help them define and achieve success. Our more than 5,000 employees serve government and commercial clients from more than 70 offices worldwide. ICF's website is www.icfi.com.

Any views or opinions expressed in this insight are solely those of the author(s) and do not necessarily represent those of ICF International. This insight is provided for informational purposes only and the contents are subject to change without notice. No contractual obligations are formed directly or indirectly by this document. ICF MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.