R & D Tax Credit Aspects of Cyber Security and Homeland Protection

By Charles R. Goulding, Andrea Albanese and Raymond Kumar

Charles R. Goulding, Andrea Albanese and Raymond Kumar discuss the need for the development of cyber security technology and encourage companies to use the R & D tax credit as an incentive to create new methods for securing America's digital infrastructure.

President Obama has identified cyber security as being not only one of the most serious economic and national security challenges we face as a nation, but also one that we as a government or as a country are not adequately prepared to counter. Shortly after taking office, the President therefore ordered a thorough review of federal efforts to defend the U.S. information and communications infrastructure and the development of a comprehensive approach to securing America's digital infrastructure.[1]

As we have recently witnessed in the holiday season breach of Target's computer systems, the expanding vulnerability of the Internet we all increasingly rely on continues to be a concern to all companies, large and small. Cyber-attack exposure to the U.S. homeland electric grids, military bases, defense contractors, transportation networks and critical infrastructure is of major concern. Due to our increasing reliance on the Internet, the homeland cannot and will not tolerate cyber attacks. The necessary security enhancements will require crucial private sector innovation that will be potentially eligible for Research & Development (R & D) tax credits.

The Research & Development Tax Credit

Many of the private industry and industry-supported University R & D efforts will be eligible for federal R & D tax credits.

Enacted in 1981, the federal R & D Tax Credit allows a credit of up to 13 percent of eligible spending for new and improved products and processes. Qualified research must meet the following four criteria:

- new or improved products, processes, or software;
- technological in nature;
- elimination of uncertainty; and
- process of experimentation.

Eligible costs include employee wages, cost of supplies, cost of testing, contract research expenses and costs associated with developing a patent.

Charles R. Goulding, Attorney/CPA, is the President of Energy Tax Savers, Inc., an interdisciplinary tax and engineering firm that specializes in the energy-efficient aspects of buildings.

Andrea Albanese is an Analyst with Energy Tax Savers, Inc.

Raymond Kumar, CPA, is a Senior Analyst at Energy Tax Savers, Inc.

On January 2, 2013, President Obama signed the bill extending the R & D Tax Credit for 2012 and 2013 tax years.

Wide Range of Private Solutions Required

According to the Gartner, a high-tech research firm, the global market for cyber security will total $65.7 billion in 2013 and climb to $85 billion by 2016 for a compound annual growth rate of nine percent.[2] As threats increase, a wide range of industries are investing more in cyber security including financial services, utilities, defense industries, energy companies and media companies.

The scope of the challenge is so great that it will require the resources of large companies with security expertise such as IBM, Symantec, Cisco, McAfee, Raytheon, BAE Systems and Northrop Grumman. This is a very fragmented market with the top four players only comprising 30 percent of the product offerings.[3]

There is a need to move from the traditional reactive techniques to more anticipatory and predictive methods given the vast consequences of even a single breach to a large computer system.

Numerous small companies with a cyber security R & D focus are developing throughout the country. This development is taking place in Silicon Valley (due to long standing software engineering expertise), in New York City (to service the financial services industry), in Virginia (for its proximity to various federal government headquarters) and in Boston (because of the supply of cyber entrepreneurs and software engineers).

New methods must also be explored; it is no longer sufficient to find a security breach and fix it. There is a need to move from the traditional reactive techniques to more anticipatory and predictive methods given the vast consequences of even a single breach to a large computer system.

Mobile Virus Trends

As we have seen with industrial control devices, PCs and notebook computers, virus attacks are expected to advance to mobile devices. Websense, a technology security firm, says they have found evidence that the "black hole" software which now infects PCs, is specifically targeting Apple iPhone and Google Android smartphones.[4]

Continued improvements to smartphone technology, in addition to advancements in software, greatly decrease the threat of mobile phone viruses and simultaneously qualify for R & D tax credits.[5]

Focus on Computer Attacks from China

Over the past few years, the United States has seen an increased number of computer attacks from China, including last year's New York Times hack and Google and Intel's 2010 hacks. These Internet invasions target many different users with private information to protect, including large companies, government agencies, law firms, news organizations, universities and tech startups.

In a recent secret intelligence assessment, the United States was found to be the target of "a massive and prolonged computer espionage campaign from China that threatens the U.S. economy."[6] The report also describes the different sectors where focus is being directed, including the energy, finance, information technology, aerospace and automotives sectors.[7]

U.S. Government Offensive Cyber Security Initiatives

The U.S. Government announced on March 12, 2013, that for the first time, it will take offensive measures as opposed to a historic defensive-only approach to cyber security attacks. General Keith Alexander, head of the new Cyber Command, is forming teams of computer programmers and experts capable of offensive cyber attacks on foreign nations in the event of a major U.S. network attack. The public announcement of cyber weapon development for wartime use is a first for the Obama administration.[8]

Alexander makes it clear that "this defend-the-nation team is not a defensive team." Initiatives include adding 40 cyber teams, 13 of which will be dedicated to offense and ramping employees up from 900 to 4,000. Alexander also notes the best defense relies on being able to monitor incoming traffic to the United States through Internet service providers (ISPs). Developing such a defense system would allow

these private ISPs to quickly alert the government about potential cyber attacks.

Conclusion

America's high-tech software engineers create the Internet infrastructure that creates the existing connected world we live in. This same brain trust is now called upon to develop the new products and firewalls that will enable us to safely and securely rely on this empowering technology. R & D tax credits can support these critical activities.

Endnotes

1 National Security Council, *The Comprehensive National Cybersecurity Initiative,* accessed at *www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative.*

2 Matthew Flamm, *A Paranoia Industrial Complex Emerges,* Crain's NY Bus., Feb. 17, 2013. Accessed at *www.crainsnewyork.com/article/20130217/TECHNOLOGY/302179976.*

3 Robert Wright, *Lockheed Plots Survival Strategy,* Financial Times, March 6, 2013, at 16.

4 *Mobile Virus Attacks Expected,* Investor's Bus. Daily, March 5, 2013, at A2.

5 Charles R. Goulding, Jonathan Saltzman and Charles G. Goulding, *The R & D Tax Credit Opportunities for Mobile Devices,* Corp. Bus. Tax'n Monthly, Feb. 2013.

6 Dune Lawrence and Michael Riley, *To Catch a Hacker,* Bloomberg Businessweek, Feb. 24, 2013, at 54.

7 Ellen Nakashima, *U.S. Said to Be Target of Massive Cyber-Espionage Campaign,* The Washington Post, Feb. 10, 2013. Accessed at *http://articles.washingtonpost.com/2013-02-10/world/37026024_1_cyber-espionage-national-counterintelligence-executive-trade-secrets.*

8 Mark Mazzetti and David E. Sanger, *Security Leader Says U.S. Would Retaliate Against Cyberattacks,* The NY Times, March 12, 2013. Accessed at *www.nytimes.com/2013/03/13/us/intelligence-official-warns-congress-that-cyberattacks-pose-threat-to-us.html?pagewanted=all.*