



**A Tipping Point**  
**The Fight for our Nation's Cyber Security**

A GTRA Research Brief

*by Parham Eftekhari*  
*Co-Founder & Director of Research, GTRA*

December 2009

## Introduction

It is a widely accepted belief that an application, network or system must be built with security and risk management as a foundation, not merely a component or element of the whole. Despite this, there is still tremendous work to be done in the area of Cyber Security and as more information and services critical to supporting this country are moved to technology platforms, the urgency is only increasing. In this research brief, GTRA highlights the important security initiatives in 2009, identifies key areas of concern as voiced by executives, and discusses success factors required for cyber security activities moving forward.

- Parham Eftekhari

## It's All About Initiatives Baby

With news stories predicting a single virus taking down the nation's entire financial system, some estimates saying that Cyber Terrorists steal up to \$1 Trillion dollars worth of intellectual property from businesses worldwide and a rise in legitimate cyber attacks on the public and private sectors, it came as no surprise (and much excitement from the federal IT community) that 2009 brought with it a plethora of announcements, movements, and initiatives which indicated that the topic of Cyber Security was finally getting the mainstream attention it deserved. And while some executives from both government and Industry seemed to think that there was more talk than action, the year marked an important milestone in raising awareness, generating new ideas, and beginning to build institutions which could promote real change. Some of the important happenings related to Cyber Security included:

**National Leap Year Initiative-** The National Cyber Leap Year Initiative which launched in October of 2008, took a new approach to fighting Cyber Security by focusing not on ways to protect against cyber crime in today's technological landscape, but rather by suggesting fundamental changes to business processes and use of technology which would create a new landscape and put the advantage back in the hands of the good-guys. The initiative has yielded five categories which "demonstrate game-changing potential" <sup>1</sup>:

1. Digital Provenance - basing trust decisions on verified assertions
2. Moving-target Defense - attacks only work once if at all
3. Hardware-enabled Trust - knowing when we've been had
4. Health-inspired Network Defense - move from forensics to real-time diagnosis
5. Cyber Economics - -crime doesn't pay

---

<sup>1</sup> <http://www.nitrd.gov/leapyear/index.aspx>

"Now... what y'all wanna do? Wanna be ballers? Shot-callers? Brawlers?..."

- Verse from "It's all about the Benjamin's baby"

"If you are playing a game you cannot win, change the game"

- Excerpt from the National Cyber Leap Year Summit 2009 Report

Obama ordered a complete evaluation of the nation's cyber security defenses and strategies in order to develop his cyber security strategy. Melissa Hathaway, who served as the cyber security coordinator executive under former President Bush's Director of National Intelligence was tasked to lead the movement. The reports executive summary concluded that:

1. The Nation is at a crossroads
2. The status quo is no longer acceptable
3. The national dialogue on cyber security must begin today
4. The United States cannot succeed in securing cyberspace if it works in isolation
5. The Federal government cannot entirely delegate or abrogate its role in securing the Nation from a cyber incident or accident
6. Working with the private sector, performance and security objectives must be defined for the next-generation infrastructure
7. The White House must lead the way forward.

**Presidential Cyber Security Strategy-** Following the 60-Day Review and further highlighting the importance Obama's administration places on technology as well as its understanding of the mission-critical nature of cyber security, May of 2009 saw President Obama personally announced his cyber security strategy, which called for the appointment of a Cyber Czar, naming our IT infrastructure as a strategic national asset which should be protected, and getting prime-time Presidential coverage of the fact that cyber threats are increasing in frequency and sophistication and should be considered a top priority.

**Civilian/Defense/Intelligence Community Collaboration-** The Joint Task Force Transformation Initiative was designed to create a cohesive and unified cyber security framework across the entire federal government by bringing together NIST's FISMA activities with efforts happening in the defense and intelligence communities. The result thus far: an August 2009 update to NIST Publication 800-53 which significantly increases the requirements for continuous monitoring in an attempt to produce real-time risk management across the federal government.

**Creation of Federal CIO Council's Information Security and Identity Management Committee-** Created in February 2009, the committee, co-chaired by Transportation CIO Van Hitch and Navy CIO Drew Carey has not only helped represent security concerns to the Federal CIO Council, but has issued guidelines on issues ranging from Web 2.0 Security and ID Management.

*"The national security and economic health of the United States depend on the security, stability and integrity of our nation's cyberspace, both in the public and private sectors."*

-John Brennan, assistant to the President for Counterterrorism and Homeland Security

**60-Day Review -** In one of the first moves of his Presidency,

Given the major initiatives mentioned above and the hundreds (if not thousands) more which undoubtedly exist, the government IT community seems to be gaining momentum, becoming more innovative and working more effectively as a community to battle the overarching problem of cyber security, a viewpoint which GTRA shares with many in the community.

However, in interviews conducted by GTRA with government and industry executives, praise of the community's progress was often followed by concerns that not enough is being done to catch-up, much less get ahead in the fight for cyber security given the complex challenges facing the nation today. Some of the top security concerns and topics raised by executives include:

- No Cyber Czar- Why has no Cyber Czar been appointed yet? *Some blame the focus on the recovery act and healthcare reform for diverting attention away from this. Regardless, many are anxious for this role to be filled.*
- Risk Management- The science behind managing risks is become more crucial, and complicated, daily. Some executives already believe that it will soon become *the* defining component in the fight for cyber security.
- Cloud Computing Security- The push toward Cloud Computing coupled with a general lack of knowledge and experience with the technology has resulted in much concern over the security implications of deploying Cloud networks.
- Identity & Access Management- Initiatives in Health IT, Cloud Computing, Social Networking, Web 2.0, and information sharing have all lead many to re-evaluate existing ID and Access Management policies and technologies to ensure continued effectiveness of existing strategies.
- Privacy- The rise in social networking, telework, mobile devices, and the sheer amount of digital data are raising serious questions about the privacy of personal information

The overarching consensus as 2009 draws to a close is that we are at a tipping point in the fight for cyber security and failure is not an option. Today, virtually all critical infrastructures which collectively facilitate our day-to-day lives are dependent on information technology including our national defenses, financial systems, public transportation networks, power grid, communications, and soon most of our healthcare records. The message is clear: concrete action must be taken immediately to develop and implement common security standards and practices to protect the nation and its citizens.

*"2010 is a tipping point for the Cyber Security community."*

-Consensus from Panel of Government and Industry Executives at the December 2009 GTRA Council Meeting

**A Tipping Point**

*“Cyber Security is a team effort that includes the government, industry, intelligence communities, law enforcement and international involvement. As we move forward, DHS is willing to take on the challenge of finding ways to work together more efficiently.”*

-Randy Vickers, **Acting** Director, US- CERT, DHS

*“We need to operate without heavy restrictions. There are enormous restrictions in the offensive domain. The biggest problem isn't the enemy, the biggest problem is us.”*

-Lt. Gen. William Lord, Chief of Warfighting Integration and Chief Information Officer, Office of the Secretary of the Air Force

## **Critical Success Factors in the Fight Against Cyber Security**

Unfortunately, as we are all well aware, there is no magic answer that will resolve all of the current security threats facing the government IT community. However, by looking at the various activities of the past few years we should find hope in the fact that some consistent trends are emerging that are shaping the critical success factors required to developing a comprehensive, nation-wide cyber security strategy:

**More Collaboration-** The guidance, recommendations and findings that have come out of the various collaborative initiatives over the years has been outstanding, and should be evidence that collaboration between government, academia, non-government, and solution providers works and should continue in even more impactful capacities.

**Industry/Government Partnership-** Government/Industry partnerships have proved to be critical in developing common standards and cutting edge solutions to a host of IT issues over the years. Cyber Security efforts are no exception and are perhaps even more adept to these types of collaboration given that information sharing on threats as well as solutions is critical to developing a winning strategy.

**Ability to Act Quickly-** Cyber terrorists do not follow any rules but their own, yet those tasked to fight them have to face lengthy review and approval processes whenever they want to act. A balance must be found that gives appropriate controls along with the power to quickly respond to threats as they emerge.