BANK INFO SECURITY®

State of Union: What Should Obama Say?

Experts Take a Crack at Writing Passage on Cybersecurity

By: Eric Chabrow - February 11, 2013

President Obama devoted only 26 words - 27 words if you count cyberthreat as two words - on cybersecurity in his 7,200-word State of the Union Address in 2012 [see The State of the Union's Cybersecurity]. Here's what the president said:

"To stay one step ahead of our adversaries, I have already sent this Congress legislation that will secure our country from the growing danger of cyberthreats"

Although the president spent only 0.36 percent of the address on IT security, the mere fact that he mentioned it at all was seen as his administration's strong commitment to cybersecurity.

Will the president allot more time on cybersecurity in this year's address? Stay tuned. Meanwhile, we asked information security and privacy experts to play speechwriter, and write a passage of 50 to 75 words (some contributors went a bit longer) on what the president should say Tuesday night about cybersecurity. Here's what they would want the president to say:

Phil Reitinger
Chief Information Security Office, Sony; former Homeland Security Deputy Undersecretary

The Internet has untold potential to drive freedom and prosperity - a potential that won't be realized unless we act now. I am therefore announcing three initiatives. First, a Cybersecurity Workforce Program to train future cybersecurity professionals starting in middle school. Second, a Secure Ecosystem Initiative to increase exponentially the level of security and privacy available on the Internet. Third, a Cybersecurity Standards Program that includes positive incentives for industry to meet self-developed cybersecurity standards.

Chris Buse
Chief Information Security Officer, State of Minnesota

It is time to recognize that cyberrisks are real, impacting all levels and branches of government, the private sector and citizens. My administration will once again try to work with Congress to put in place a framework to address cyberthreats holistically.

Eugene Spafford
Professor of Computer Science, Purdue University, and Executive Director, Purdue Center for Education and Research in Information Assurance and Security

Our nation faces a number of security challenges, including in the realm of cybersecurity. I am proposing several new initiatives to:

- Allocate significant new resources to the FBI and state law enforcement agencies to pursue computer criminal;
- Exact penalties against countries that continue to attack U.S. companies and our government or that tolerate such attacks and then fail to cooperate with law enforcement in bringing the perpetrators to justice;
- Provide incentives to companies to keep their cybersecurity up to date and for them to support cybersecurity studies in postsecondary education;
- Increase K-12 education in all areas of computing, including security and privacy aspects.

Larry Clinton
Chief Executive Officer, Internet Security Alliance

The digital world fundamentally changes our assumptions about national defense, economics and everyday life. But these cybersystems are under constant attack from organized criminals and nation states. Our top priority must be to secure our government's systems. Realizing government relies on privately owned systems and that antiquated regulatory models are not well suited to address the problems of the digital age, I propose a new approach that creates a modernized partnership between the government and industry assuring the proper economic incentives are in place for cyberdefense.

Robert Bigman
Retired Chief Information Security Officer, Central Intelligence Agency

It is time to move cybersecurity from discussion to action. We must move forward with either legislative or executive action that articulates security standards for our national critical infrastructure and invest in the research and development of secure computer systems and networks. We must also make cybersecurity education a priority like we made science and math priorities post Sputnik.

George Tubin
Senior Security Strategist, Trusteer

Cyberthreats are very real, they're very dangerous, and this government is taking them very seriously. The secretary of defense has been tasked with developing an immediate plan to ensure all national cyber-assets across all departments are secure, including government, private government contractors and former employees. I will actively work with Congress to enact legislation requiring our critical economic infrastructure to deploy appropriate protections to secure our country from the growing danger of cyberthreats.

Jim Harper
Director of Information Policy Studies, Cato Institute

Having studied the issues more carefully, I've determined that the vast bulk of cybersecurity protection must be provided by the owners of computers, networks and data themselves. The federal government is ready to assist and our diplomatic efforts when countries harbor or produce cyberthreats will be stern and serious. But I'm directing our national security agencies immediately to stop cultivating and stockpiling

vulnerabilities. Instead, we will close them, making everyone, around the world, more secure.

Mukul Pareek
Co-Creator, Index of Cybersecurity
Just like we need our armed forces, an advanced information society such as ours needs strong cyberdefenses as well to protect our freedom, liberty and uphold across the globe the cause of the values we hold dear. To that end, and to defend our businesses from cyber attacks, I am expanding the mandate of the U.S. Cyber Command to protect our private sector businesses, large and small, and deny our adversaries the opportunity to sabotage our industry or attack our infrastructure.

Richard Stiennon
Author, Surviving Cyberwar

I am issuing a presidential order requiring every agency and department of the government to appoint a cybersecurity director whose responsibility will be to prevent any and all cyber-attacks against our federal information systems. This role will come with a mandate to secure our computers and networks. Any breach that occurs will be deemed a failure on the part of the cybersecurity director and he or she will have to look for work elsewhere.

Françoise Gilbert
Founder, IT Law Group; General Counsel, Cloud Security Alliance

To stay one step ahead of our adversaries, I will encourage and create incentives for students to excel in math, physics, computer science, programming, and for schools and universities to offer these courses. In other words, I see too many kids spending an inordinate amount of time on the ballet activities or traveling with the choir or participating in the pottery club or the debate team. I never hear parents around me talk about their kids being in a software-development class or computer-programming class. We need more computer scientists, more technical people, more physicist. Some of these courses should be mandatory or there should be some incentive for students to attend them.