



Securing our Digital Future

Kelli Tarala

originally printed July 9, 2009

What is Cyber Security

Cyber security is basically the protection of data and computers connected to the Internet. All computers including massive governmental networks as well as your family' home computer involves cyber security. Thanks to recent efforts of the Obama Administration, cyber security has been transformed from a concern chiefly of computer geeks and technology managers to an issue of pressing national importance.

The nation's critical infrastructure, such as the telephone and data networks to businesses and homes, the electric power grid, air traffic control systems, and financial systems depend extensively on information technology for its operation. How long could each of us continue our daily lives without these services? The globally-interconnected communications infrastructure known as cyberspace underpins almost every facet of modern society. Cyber space provides critical support for the U.S. economy, public safety, civil infrastructure, and national security. This technology has transformed the global economy and connected people in ways never imagined.

Concerns about the vulnerability of these infrastructure systems have heightened since the September 11, 2001, attacks. National policy makers have become increasingly concerned that adversaries backed by substantial resources will attempt to exploit the computer vulnerabilities in the critical infrastructure, thereby inflicting substantial harm on our nation. Security professionals and government agencies have witnessed countless

intrusions that have allowed criminals to steal of millions of dollars. Foreign nations have stolen our intellectual property and sensitive military information. Hackers also have the ability to threaten or interrupt of our critical infrastructure. One recent example from November 2008 illustrates both the speed and the scope of these challenges. In a single 30-minute period, 130 automated teller machines in 49 cities around the world were illicitly emptied of cash.

Cyber Attacks and Cyber Warfare

Cyber warfare is the use of computers and the Internet in conducting warfare in cyberspace. The range of potential threats in the cyber world is as wide as our use of information technology. Our nation's critical infrastructure is already under attack. The number of attacks is astronomical.

One attack was code named Titan Rain. This was the U.S. government's designation given to a series of coordinated attacks on American computer systems since 2003. The attacks infiltrated our government's most sensitive and secret networks. According the director of the SANS Institute, an information security research organization, the attacks were most likely the result of Chinese military hackers attempting to gather information on U.S. systems. Titan Rain hackers gained access to many U.S. computer networks, including NASA, Lockheed Martin, and Sandia National Laboratories.

GhostNet was the name given to a large-scale cyber spying operation discovered in March



Securing our Digital Future

Kelli Tarala

originally printed July 9, 2009

2009 that infiltrated political and economic organizations in 103 countries. The GhostNet sends malware to recipients via stolen emails and addresses. Once recipients open the email, The GhostNet infection causes computers to download malicious code that allows attackers to gain complete, real-time control of computers. They might as well be sitting in the room where our nation's secrets are being discussed! Once these computers are controlled, the hackers can turn on cameras and microphones and monitor not only the information on the computer, but the conversations going on around the infected computer. That is some pretty scary stuff!

As these two examples illustrate, our national computer networks are under attack.

Obama Administration's 60 Day Review of Cyber Security

Security and government experts have said that our Federal government is not organized appropriately to address this growing problem. Many of the responsibilities for cyberspace are distributed across a wide array of federal departments and agencies. Many of these agencies have overlapping duties. Also, there has been no one decision maker for federal cyber security. Without a 'cyber czar', no one person has had the sufficient decision authority to direct actions that can address the country's cyber security problems completely.

President Obama identified cyber security as one of the top priorities for his Administration and directed an early 60-day, comprehensive review to assess U.S. cyber policy and

structures. The President requested a "clean-slate" review to gather information towards building a common understanding and acceptance of the problem of cyber security. The report was completed on April 17th, and calls for a cyber security chief residing in the National Security Council, reporting directly to the President.

In the coming months, we will see more news articles about cyber security. The national dialogue on cyber security must advance now, and it must include every day citizens as well. To read more about securing our digital future, check out the White House Website and the White House Blog
<http://www.whitehouse.gov/cyberreview/>

Article reprinted courtesy

