The Federal Response of Cybersecurity Threats Within the Obama Administration

Erik Buschardt
Webster University

Abstract

This paper will serve to explore various threat, cyber intelligence methodologies, and techniques in detection to combat and defeat the exposition of known and unknown threats and vulnerabilities, that lie at the heart of federal government data centers as well as industrial military complexes around the world. We shall limit our discussion to majority of recent federal activities that have taken place within the scope of the current White House Administration, while exploring the beginnings and roots of those operations from previous Administrations. While optimistic in nature, this whitepaper shall not shy away from recently leaked and declassified materials, but attempt to paint a true and unbiased portrait of current activities, so that the reader comes to a conclusion of their own standing. Shall we begin?

Introduction

Every day, cybersecurity threats from around the world penetrate and travel through our digital lives in various forms, through various media, on various platforms and for different purposes. Where those threats exist over, under, and through the national infrastructure of the United States, the federal government is tasked with the general upkeep, maintenance and overall basic protections against harm and destruction of said infrastructure. Various formats of national infrastructure exist at present, including national highways, electric power grids, major reservoirs, aquifers and rivers, civil and military airspace, and of course all the networks, routers, cables, switches, hubs and servers that constitute our portion of the Internet.

As such, it is a primary role, task and responsibility of the Obama Administration to protect, enhance and improve the quality and performance of basic services, in the interest of national security and long term economic health. In detecting cybersecurity threats from around the world on a constant and ongoing 24/7 basis, the United States is well poised to defend itself, and maintains a network of incident management and disaster recovery scenarios, from Cheyenne Mountain, to the Presidential Emergency Operations Center, to various undisclosed Continuity of Government locations, to the use of Air Force One and the Boeing E-4 Advanced Airborne Command Post, or "Doomsday" plane.

One of the most recent threats that President Obama's administration faces is China, with a most recent State Visit this past week, following another State Visit from the Holy See. While we

pandered to President Xi's government in order not to be overwhelmed by conflict as a result of a crushing debt, words captured the mood of those who watched carefully President Xi's words: "The Chinese government will not, in whatever form, engage in commercial theft or encourage or support such attempts by anyone. Both commercial cyber theft and hacking against government networks are crimes that must be punished in accordance with the law and relevant international treaties." (President Xi's Double Talk, A34) Never mind the facts that the government need not engage in the lives and activities of commercial hackers, who seem to be doing just fine on their own, taking advantage of American intellectual property as much as they can get away with. Also, the keyword "must" in context with "crimes *must* be punished" seems dubious, given that conflicting priorities within Xi's administration seem quite evident and obvious.

Executive Order 13636 - "Improving Critical Infrastructure Cybersecurity"

One of the major advances in the fight against threats that exist in our national infrastructure was signed on February 12, 2013. Executive Order 13636 ("Improving Critical Infrastructure Cybersecurity") serves three purposes: (1) to share information regarding common threats that would affect national interests and the national infrastructure, (2) to maintain privacy among citizens, and (3) to adopt common industry security best practices. It was formed as a response to the detection of threats and as a prevention of exposure to vulnerabilities in the current national model. Sections 1 and 2 identify the overall scope of the policy in order to be enforceable by reasonable means, and gives us a basic definition of what critical infrastructure is, defining them as "systems and assets, whether physical or virtual, so vital to the United States

that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." Sections 3 through 4 give us a thorough overview of how the information obtained in these efforts would be shared throughout the various parts and offices of the federal government, while Sections 5 and 6 describes the privacies guaranteed not to intrude upon individuals and/or organizations involved in surveillance. Section 7 goes into a bit more detail defining Cybersecurity Framework as "...a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks." Section 8 gives recommendations to various agencies as to how to coordinate activities regarding the sharing of confidential information gathered from the efforts defined in the "Cybersecurity Framework". Sections 9 and 10 identify those areas of the national infrastructure that are at greatest risk, and gives a recommended timeline of implementation towards the plan. Finally, Sections 11 and 12 give footnoted exceptions and disclaimers, saying that it shall not exceed current federal law, it shall co-exist within international obligations and treaties, and it shall not create "any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person." ("Executive Order -- Improving," 2013)

The National Politics of Cybersecurity Efforts

Not surprisingly, the media attention paid to the efforts of the Obama Administration and the federal government as a whole has not been a unified consensus. Rather split along party lines, these efforts have been described in various ways, ranging from modest and steady, to extreme

and “Big Brother” in scope and nature. While one would be best advised to read from a variety of news sources and outlets, it is oftentimes inconvenient and uncomfortable to share an understanding, viewpoint or perspective that one may not share widely. Republicans in Congress do not widely share the same vision in priorities toward cybersecurity exercises while holding the purse strings, earmarking for other priorities in their respective districts and within their constituencies.

Indeed, Cybersecurity bills passed in the House and Senate both faced opposition from privacy advocates and public interest groups such as the American Civil Liberties Union and the Center for Democracy and Technology, who argue against the Big Brother concept, advocating instead for anonymity, which these bills fall short of.

In this respect, the threat is a social one, purely man-made and artificial by nature. The argument is for identification v. surveillance and abuse. Should we have the will to understand the technology, a pseudo-anonymic interface can be constructed for certain activities such as democratic voting, police surveillance and enforcement of current law. (Shortcomings of Cybersecurity Bills, A26)

Threats and Challenges, both domestic and international

While all federal agencies are granted access to public information, only a few are granted secure classified information. These agencies include the Federal Bureau of Investigation (FBI), the Central Intelligence Agency (CIA), the Department of Defense (DOD), the Department of Homeland Security (DHS, 2001 -), the Office of Personnel Management (OPM), where a 2015 data breach yielded up to 21.5 million records stolen! In addition, from 2010 to 2013 there were numerous challenges facing the administration, beginning with President Obama's landmark "bipartisan" legislation from 2010 regarding the implementation of the Patient Protection and Affordable Care Act (PPACA), commonly called the Affordable Care Act (ACA) or colloquially "Obamacare". A major tenant of the implementation of that health plan involved the use of a central website called Healthcare.gov. As has been widely reported since, the official public launch of that website on October 1, 2013 was a complete logistical nightmare, with outages, crashes and bugs to last more than a few years. However, regarding the threat of private patient information towards the use of that site, many users were reluctant to use the site, opting instead to use the main hotline offered - 1-800-318-2596. Among the outrage caused by the mandatory plan itself, the initial failures of the website (notwithstanding similar local or state-run health exchanges), and the removal of Kathleen Sebelius, the 21st United States Secretary of Health and Human Services, (2009-2014). (Zengerle, 65)

Edward Snowden

Let us diverge our thoughts for a bit and wonder if all government hacks are good hacks. Such a discussion raises the question - "*What is a threat?*" Should we blindly trust the government

when they obviously have the capability, expertise and technology at present in order to conduct massive surveillance programs upon their citizenry? The protection, health and welfare of a population in order to maintain the continuance of a government builds a relationship, and is threatened when either the population learns of a malice attempt of surveillance on the part of the government, or a grassroots revolution on the part of the population (think: Arab Spring, 2010).

That was the intent of a sole contractor who in 2013 made public details of an invasive surveillance program called PRISM, launched in 2007 via the National Security Agency. PRISM was designed to "receive" photos, emails, video and voice calls, social networking profiles, and login credentials from several popular tech firms including Microsoft, Google, Facebook, Yahoo, AOL and Apple. The information leaked in 2013, per Mr. Kelion, included the fact that the cost of the PRISM program reached upwards of $20 million a year, and was designed primarily to specifically conquer earlier "constraints" within the government's data mining efforts since 2001. As the cartoon above illustrates, the relationship of trust between the public and its government is strained and tested more than ever, as we sort out the ethics of Mr. Snowden's actions. The concept of threat detection comes into highlight when we consider who the source of the threat is, in light of the government's actions and the particular consequences of Mr. Snowden's leaked information.

Conclusions

So what have we gathered? That we are no more prepared for a cyber event or attack 10 to 15 years ago than we are now? That we are far superior to other countries in terms of manpower, or technical prowess? Hardly. But as we become part of a generation of technologically literate users, we are most vulnerable to those among us who would cause harm or large-scale damage to our society. Gaining awareness about issues that surround us, oftentimes issues that did not exist fifteen to twenty years ago such as social media, online classrooms, or the ubiquity of smartphones also doles out to us a responsibly to use such powerful tools wisely, let they be misused by us or others. Understanding threats as we do today, we can better manage and interpret their intent, and use that information to drive enforcement results going forward.

References

Chung, L. (1 October 2013). "HealthCare.gov is a Technological Disaster". Retrieved 1 October 2015.

Exec. Order. No. 13636, 3 C.F.R 203 (2013)

Kelion, L. (2013, July). Q&A: *NSA's Prism internet surveillance scheme.* BBC News Retrieved from http://www.bbc.com/news/technology-23051248

President Xi's Double Talk on Doing Business in China. [Editorial]. (2015, September 25). The New York Times, p. A34. Retrieved from http://www.nytimes.com/2015/09/25/opinion/president-xis-double-talk-on-doing-business-in-china.html

Shortcomings of Cybersecurity Bills. [Editorial]. (2015, May 14). The New York Times, p. A26. Retrieved from http://www.nytimes.com/2015/05/14/opinion/shortcomings-of-cybersecurity-bills.html

Zengerle, P.; Cassella, M. (2015-07-09). "Estimate of Americans hit by government personnel data hack skyrockets". Reuters. Retrieved 2015-07-09.