Roger L Caslow, Executive Cyber Consultant, Suss Consulting

April 26, 2012

Testimony to the Joint Subcommittee Hearing: Iranian Cyber Threat to the U.S. Homeland

---

Good morning and thank you for inviting me to share my testimony today. My name is Roger Caslow[i] and I am an executive consultant with Suss Consulting. My background is primarily in the realm of cybersecurity as it relates to computer and network defense. It is an honor to appear before this Joint Subcommittee to testify about the Iranian Cyber Threat to the U.S. Homeland and I hope that my testimony is of benefit in to creating a better defense posture against this stated threat.

According to the 2012 Data Breach Investigations Report[ii], 97% of all reported data breaches were avoidable through basic levels security controls implementation. Allow me to state that in order to protect our way of life we must be prepared to return to the basics of security. Not the flashy and glitzy but rather the foundational aspects of cybersecurity. Once we have secured the basics, across all sectors, then and only then can we have greater certainty that the "weakest link" is not as exploitable by those who seek to do us harm. Within the field of cybersecurity this requires ensuring that the foundation is secure by knowing what is on or connected to our networks, what our basic security posture is and what it should be, and ensuring that the right people with the right skill sets are building, maintaining, and protecting these assets and their data.

Furthermore, within the cybersecurity discipline we require a stronger governance structure. Governance is far from the most exciting area in the field of cybersecurity but it is foundational to ensure better management of our vulnerabilities against our threats. For this to work we must have clearly defined language, write what is meant and leave as little room for negotiation as possible. Good governance is required for best performance of our national, state, local, and industry activities. Good governance supports better integration of cybersecurity and information technology architectures, building in the security requirements upfront. Good governance supports the adoption of risk management based decisions, which are only as good as the information made available to the decision makers responsible for the defense of our interconnected networks, both public and private. Executive Order 13587[iii], *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information,* is a good start but it requires more "teeth" and better communication across all levels, to include our industry partners, lest the bureaucracy overrun the implementation.

Another, not too exciting area, is the emphasis on education, training, and awareness (ETA). Education emphasis, not merely on the hard technology engineering skills but also on basic critical thinking skills, which are all but lost in many technology disciplines. With respect to training, as a nation our standards need to be fully matured and established across all sectors. We can make improvements by leveraging the private sector security based and focused

training organizations, which are aware of the threats, vulnerabilities, and countermeasures. Basic awareness of the threats posed to all sectors and elements of our society is also important. We still have too many people who are ignorant of the threats and become caught in phishing, spear phishing, social engineering, and other types of data manipulation, exploitation, and exfiltration schemes. Again, all sectors are important and require some level of targeted awareness campaigns. Consider it as operational security against the cyber attack. The National Initiative for Cybersecurity Education (NICE)[iv] which evolved from the Comprehensive National Cybersecurity Initiative was intended to address many of the ETA issues but it has not taken root. I fully understand the concept of *"measure twice and cut once"* but when we face the threats we do as a nation, the 85% solution should be enough to start. More focus on results and accomplishment, with less talking; will better serve this initiative, and our overall cybersecurity posture.

Finally, we must seek out and leverage, by name when and where possible, specific people, tailorable processes and integratable security technology solutions. We must allow the subject matter experts to research and propose implementable process and technology solutions and then put them in place with minimal delay, bureaucracy is not our friend in this arena. Also, we must not be afraid to embrace the hacker community, but in order to do so we must leverage a different type of recruiter. Our talent recruiters going to this community via to the major hacker conferences, also known as "CONS", will have little success in three piece suits. They must be people who have the look, feel, and knowledge to speak with this community at the social and technical levels. This is critical to securing the skill sets and knowledge base from a community with a greater knowledge of the offensive side of the battle. It's a known fact in sports, combat, and security that knowledge of the offensive tactics, techniques, tools, and procedures are of utmost importance in further bolstering our defensive posture, and in the case of cybersecurity, securing our networks

There are no easy solutions, and we have been speaking to these topics for a number of years, but if we are serious about protecting our nation's interests we must first secure the basics before moving onto more advanced methods. Thank you again and I look forward to any questions you might have for me.

---

[i] Roger Caslow Bio

[ii] 2012 Data Base Investigations Report, Verizon

[iii] Executive Order 13587 , Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, Signed October 7, 2011

[iv] National Initiative for Cybersecurity Education Strategic Plan, August 2011