10 CHEAP TRICKS TO IMPROVE OUR CYBERSECURITY: PART I

On September 15, 2016, the Internet Security Alliance will publish a 400 page, 17 chapter, book containing 106 recommendations for the incoming Administration and Congress. One of the recommendations is that, frankly, we need to invest more in cyber defense. We are chasing a $500 billion to $1 trillion dollar a year issue with about $9 billion in non-defense cyber spending and successfully prosecuting maybe one or two percent of cyber criminals.

However, when talking with government officials, one of the first things we are told is that getting increased spending for anything is extremely difficult. So, without getting into a spending debate, we will now offer 10 ideas that will cost virtually nothing in the federal spending sense yet can substantially improve our cybersecurity. This blog presents the first 5 of these.

1. We need to train our senior government officials similarly to the way corporate boards are getting trained about cyber security. In 2014, the National Association of Corporate Directors published a Handbook of cyber risk management targeting corporate boards and has been actively training directors consistent with its principles. PWC reported on the effect of this training saying that it had resulted in a 24% increase in cyber spending, better risk management, better alignment of organization goals with security and creating a culture of security. The government equivalents of corporate boards – Members of Congress, Cabinet Officers, Agency heads – need a similar training program for that audience as NACD is providing.

2. Pilot Test the NIST Cybersecurity Framework for effectiveness and cost effectiveness. It is nearly 3 years since the NIST Framework was unveiled and we have not a single piece of objective data that indicates if it has changed behavior, or operationally improved security, what aspects of it are most effective for various populations and what is cost effective. If we can demonstrate what will actually improve security on a cost effective basis, firms will naturally and voluntarily adopt those mechanisms.

3. We need to dramatically increase our emphasis on small companies. Smaller companies do far less on cybersecurity than larger ones. Small companies not only need government help more than larger ones, but their vulnerabilities are often exploited to provide access to larger firms, including critical infrastructure. Yet our government programs and structures focus primarily on larger firms who are easier to access. Programs for smaller firms are largely confined to occasional superficial road shows on pamphlets. Proper risk management demands resources be placed at the point of maximum vulnerability that is smaller companies.

4. Cyber assessments need to transform from the current "pass-fail" compliance model to a more practical maturity model. Legacy regulatory programs are

standards based and determine if you are, or are not, in compliance. Cybersecurity is not a binary field where you are either secure or insecure. Modifying compliance regimes so that they determine cyber maturity would be more useful and could provide incentives for improving cybersecurity.

5. The clearance process should be modernized to allow for greater and more efficient private sector participation and partnership. The current clearance process was designed largely to deal with classified information and controlled by sector specific agencies. Clearance by one department doesn’t necessarily apply to another and a cleared person working for one company can lose their clearance simply by changing firms even within the same sector. Partnership for cybersecurity requires greater participation and more flexibility. Modernizing the clearance process for the digital age will result in greater collaboration and more security.