Internet Infrastructure Coalition Response

Incentives To Adopt Improved Cybersecurity Practices

A Notice by the National Institute of Standards and Technology and the National Telecommunications and Information Administration on 03/28/2013

The Internet Infrastructure Coalition (i2Coalition) is comprised of key players representing U.S. Internet infrastructure providers and related tech firms that help enable web hosting and cloud services. We are the people who build and maintain the Internet. We are dedicated to educating policy makers, opinion leaders and the media, sharing best practices among our members and promoting the economic benefits that our industry delivers. The Internet infrastructure industry generates $46 billion in annual direct and indirect revenue, and the industry is growing at a rate of nearly 20% per year.

The i2Coalition has a strong concern associated with the privacy of information shared with governmental entities. When an individual or entity places information with an i2Coalition member company they expect that the information will receive the same degree of confidentiality it would receive if it were held internally. The i2Coalition remains gravely concerned that in analyzing cybersecurity, issues associated with sharing information with governmental entities have only received cursory analysis. The purpose of sharing information with governmental entities should be solely to analyze threat information, and not for other purposes.

The use of information entrusted to Internet infrastructure companies for other purposes will significantly erode marketplace trust that has taken over twenty years to establish. In addition, i2Coalition member companies compete on a global scale. The international marketplace already views U.S. government access to data with deep suspicion, placing U.S. companies in a compromised marketing position. Any attempts to address cybersecurity concerns should not further compromise the ability of U.S. companies to compete globally by eroding traditional U.S. guarantees of due process and Fourth Amendment protections.

The i2Coalition has reviewed the notice posted by the Department of Commerce and is providing responses to the following set of the questions posed:

- **Are existing incentives adequate to address the current risk environment for your sector/company?**

  The i2Coalition believes that very few positive incentives exist today for companies to fully address cybersecurity risks. In fact, the overtone set by both Federal and State legislation and regulation is more punitive than incentive driven. We believe that true incentives would be more effective. These incentives should involve a mix of safe harbor procedures, financial assistance and

protection of confidential information. These incentives could be extended and strengthened for companies who attain third party assurance of meeting the baseline standards, providing additional incentive for additional spend on cybersecurity measures.

- **Do particular business sectors or company types lack sufficient incentives to make cybersecurity investments more than others? If so, why?**

  The current lack of true incentives cuts across most sectors and company types. Those sectors that are more heavily regulated, with demonstrated enforcement and fines, are less impacted by the lack of incentives as they find they must already meet certain standards for data protection to remain viable. The reputational, financial and litigation risks of not meeting the standards is simply too high for these types of companies to bear. Examples of these include financial institutions, health care organizations and companies engaged in processing credit card payments. Unfortunately in these sectors many companies purposely implement only the bare minimum level of controls needed to meet the requirements which still leaves them vulnerable and not as secure as they could be. True incentives would likely increase the adoption of more robust security programs leading to a more significant reduction in risk and an enhanced security posture.

- **What are the best ways to encourage businesses to make investments in cybersecurity that are appropriate for the risks that they face?**

  We believe that incentives that help offset the risks of implementing enhanced cybersecurity controls would provide greater adoption of baseline standards. For example, additional legal protections limiting liability, protecting information submitted as part of participation in a program from disclosure under the Freedom of Information Act (FOIA), and preventing its use in civil litigation would also provide increased incentive for companies across all sectors to increase the strength of their cybersecurity programs. Finally, increasing the sharing of threat and vulnerability information from the public sector to the private sector represents another form of incentive. Most everyone understands that the government possesses much more information about current threats and vulnerabilities than is known within the private sector and developing a process that facilitates more timely sharing of this information with the public sector would enable companies to better understand the need for stronger security programs and provide them with actionable information to use in selecting additional cybersecurity controls to protect themselves.

- **How do businesses measure success and the cost-effectiveness of their current cybersecurity programs?**

  For most companies success equates to never being contacted by a third party, whether regulator, industry participant or hacker about their data being leaked. Unfortunately, most companies lack the means to identify if any of their data has been leaked. Some have controls in place to allow them to identify certain types of leaks that occur via channels they are able to monitor, but virtually none have a full picture of what or how much data has been compromised. When it comes to measuring the cost-effectiveness of their current programs, it is more of an art than science. If you don't have a clear picture of your data loss, you lack a key metric to calculating any reasonably accurate measure of cost-effectiveness. Currently, many companies view the cost of cybersecurity programs similar to insurance. It is a necessary expense and the value of the program is very difficult to determine. Of the companies who actually conduct meaningful risk assessments, most attempt to determine the likelihood and impact of threats and vulnerabilities

and then assign estimated costs to the risks. Since there is a lack of data on which to base likelihood and impact, the figures arrived at are often not well founded. On the other side, the costs to implement specific cybersecurity controls that can mitigate these identified risks are very well known. The resulting analysis compares well known costs with not so well known benefits leaving companies to make cost benefit decisions with imbalanced information. In many cases, boards of directors, who are responsible for maintaining the profitability of their organizations, routinely make decisions not to implement security controls due to the perceived imbalance of cost to benefit. It is only when these companies experience a significant data breach and are subjected to the resulting costs that are all too real, do they understand the consequences of their earlier decisions and embark on more aggressive courses of improving their cybersecurity posture.

- **Are there disincentives or barriers that inhibit cybersecurity investments by firms? Are there specific investment challenges encountered by small businesses and/or multinational companies, respectively? If so, what are the disincentives, barriers or challenges and what should be done to eliminate them?**

  The current complex web of state, federal, industry and international regulations act as a significant barrier to cybersecurity investment. Most companies find it very difficult coalescing regulatory requirements into a cohesive and understandable form. This makes the decisions on which investments to make in security controls difficult. Harmonizing these regulatory requirements into a common set of controls would be extremely helpful. If in the development of the baseline requirements, the government could include a harmonization framework that would allow companies to clearly see a distilled list of security controls that are required to satisfy regulatory requirements, this would provide further incentive to the adoption of a baseline framework.

- **Are incentives different for small businesses? If so, how?**

  We believe that small business face different issues and therefore different incentives may be required. Since most small businesses lack a depth of security expertise, incentives for this space need to focus more heavily on financial and awareness incentives. Providing small businesses with access to clearly explained information on current security threats and vulnerabilities along with actionable steps they can take to improve their security programs would likely foster increased adoption of baseline security guidelines. The use of financial incentives may be more important here as many small businesses simply don't have the budget to implement many of the more costly security controls.

- **For American businesses that are already subject to cybersecurity requirements, what is the cost of compliance and is it burdensome relative to other costs of doing business?**

  We believe that the costs associated with maintaining compliance with existing cybersecurity requirements are generally high and, in many cases, represents a significant percentage of companies' budgets for security and overall IT spend. This is especially true for those organizations that are subject to multiple requirements and those subject to very prescriptive requirements like the Payment Card Industry Data Security Standard. In many cases, the costs associated with audits (internal and external) and reporting rival the costs of many security controls. Simplifying the regulatory landscape and/or allowing validation against a baseline framework to cover off the

reporting/validation requirement for other regulations could significantly decrease the overall costs of compliance.

- **What are the merits of providing legal safe-harbors to individuals and commercial entities that participate in the DHS Program? By contrast, what would be the merits or implications of incentives that hold entities accountable for failure to exercise reasonable care that results in a loss due to inadequate security measures?**

  We believe that providing legal safe-harbors to those who participate in the DHS program has strong merit. The lack of meaningful positive incentives and the reasons for companies to not participate and share data about data breaches. The current regulatory climate is mostly punitive in nature which results in only a fraction of data breaches being reported. Finding a way to provide meaningful legal protection in exchange for participation in the DHS program would likely result in significantly increased participation. However, in creating these protections, the confidentiality and privacy of information disclosed should be firewalled from further use.

- **What would be the impact of requiring entities to join the DHS Program prior to receiving government financial guarantees or assistance in relevant sectors?**

  If the government is providing financial incentives for participation in the program it is reasonable to expect entities to commit to joining the program before these incentives can be realized. It also makes sense as there would be no concrete way for the government to validate claims for the incentives without a registration requirement.

- **Should efforts be taken to better promote and/or support the adoption of the Framework or specific standards, practices, and guidelines beyond the DHS Program? If so, what efforts would be effective?**

  We believe that education and awareness are key components to the adoption of any new framework. Organizations such as ISACA, NIST and ISO heavily promote their respective frameworks by offering training courses, webinars, and industry education events among other methods. Experience shows that this activity has been very successful. The DHS program should also provide these types of events. In addition, the Department of Commerce could also reach out to the network of local Chambers of Commerce to help spread the message. Most of these organizations have well developed community outreach and education programs and this method would closely mirror the grass roots efforts that have proven successful within the political arena in getting information out to large segments of the population. This method would also help reduce the cost of the education and awareness program to the government.

- **What incentives are there to ensure that best practices and standards, once adopted, are updated in the light of changing threats and new business models?**

  The I2Coaltion believes that the current efforts to maintain and update the various industry standards and best practices such as ISO 27001, NIST 800-53, CoBIT will continue and that additional incentives are not necessary in order for the organizations that promulgate and publish these to continue their work. Many of the organizations that maintain these standards are private sector based and have been updating them regularly without any inducement from the government and we believe that will continue.

- **Voluntary industry sector governance mechanisms are sometimes used to stimulate organizations to conform to a set of principles, guidelines, and operations based on best practices, standards, and conformity assessment processes that collectively increase the level of assurance while preserving organizations' brand standing and the integrity of products and services.**
    - **Do organizations participate in voluntary governance mechanisms?**

      Yes, organizations do and will participate in voluntary mechanisms.
    - **Which industries/groups have voluntary governance mechanisms?**

      The most prominent is the Payment Card Industry. This global effort has been very successful in collectively increasing the level of security around the protection of payment cards. In fact, the PCI DSS has been the primary motivating force behind several more recent security technologies such as SIEM, Log management, file integrity monitoring, and data loss prevention. It has also spurred increased use of tools like vulnerability scanning, anti-virus, patching, etc.
    - **Do existing voluntary governance mechanisms have cybersecurity-related constraints?**

      The PCI DSS is a very prescriptive set of controls that are predominantly concerned with cybersecurity. There are some 280+ individual controls within the PCI DSS that, when implemented correctly, result in a significantly stronger security program.