Response

cyberincentives@ntia.doc.gov

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

A No

Q Do particular business sectors or company types lack sufficient incentives to make cybersecurity investments more than others?

A Yes

Q If so, why?

Health and Financial business sectors and companies specializing in entrepreneurial endeavors all lack sufficient incentives to make investments. In the Health sector, there is no incentive other than regulation and the same is true of the financial sector. The method of cybersecurity is not understood and the ability to protect servers and or end-points from intruders has not worked, even with investments in IT staff, equipment, software and security services. Money already spent has not protected data and companies, individuals and even US Government agencies are unable to protect their devices. All are waiting for solutions first before expending capital.

Q How do businesses/your business assess the costs and benefits of enhancing their cybersecurity?

A Whether it works or not for the application, costs and ease of use. Learning curves are another factor.

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

A It is no longer the responsibility of businesses or individuals to “make investments” in cybersecurity because the risks they face have already happened or are impossible for them to protect themselves from. If even the top cybersecurity experts in the World cannot protect themselves, how can businesses? Especially small businesses run by non technical persons.

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

A If the cost is affordable for their circumstances and if it protects their devices from intruders. Of course, they have to first know the intruder is there and recent reporting suggests that these intruders can remain clandestinely in an operating system for months or years without detection.

Q Are there public policies or private sector initiatives in the United States or other countries that have successfully increased incentives to make security investments or other investments that can be applied to security?

A NIST and NASA, DARPA and other US Government Agencies have established grant policies that have worked to a small degree for attracting talent to address the issue, but the current methodology of expecting volunteers to work for free and fix the problems is unrealistic. If anything, initiatives like the recent threat attempt by the UN Telecommunications Union to allow Telcos to become bottlenecks for the Internet and charge access fees has scared some companies and Governments into initiatives to try and understand the scope and details of the problem/s. The idea that companies will make investments to be “cyber secure” means that they can accomplish this and as their systems are interdependent on so many other factors, (especially the hardware they use), they cannot fix the problem alone for their own systems.

Q Are there specific investment challenges encountered by small businesses and/or multinational companies, respectively?

A The main investment challenge encountered by small businesses is that they cannot afford security, especially when it has little or no real effect and they do not understand it anyway. The time it takes to figure out computers is time away from their business. They have no way to redress grievances due to high legal costs and anonymity, which prevents any obtainable documentation into the intrusions. If they report a problem, it is ignored for investigation unless the sum of damages is high. They are at a complete disadvantage and expect that an investment in equipment and software should include cybersecurity. After all, they are not responsible for the networks.

The main investment challenge for multinational companies is the same on a larger scale. IT expenditures are drastically increasing due to the need to keep servers running and computers from being hacked, mostly by State sponsored operatives from China and East Europe.

Q If so, what are the disincentives, barriers or challenges and what should be done to eliminate them?

A The main disincentives, barriers and challenges are knowing what to do. At this point it does not appear that this basic question has been adequately addressed. What should be done to eliminate them is a Presidential Order that gets to the core problems of cybersecurity as quickly as possible and effectiveness is measured.

Q Are incentives different for small businesses? If so, how?

A Incentives are definitely different for small businesses in that they cannot afford even rudimentary protection over and above the expenditures on equipment, high Internet access fees and obsolete software and hardware timeframes. They need grant money for this.

Q 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?

A Definitely it is a burdensome for Health regulated companies and financial regulated companies to comply with regulations, but this is the only way they will comply at all.

Q What are the merits of providing legal safe-harbors to individuals and commercial entities that participate in the DHS Program?

A Why should they need it? If the US Government has a legal right and a need to know information, they should be able to obtain it without giving companies immunity. If the companies are the ones doing wrong with customers internet traffic or records, why should they be immune from prosecution? They should instead by subjected to severe penalties for non compliance with valid and transparent requests. If the requests are a violation of individual liberties, privacy or Constitutional rights, then companies should be rewarded for non compliance as Government Whistleblowers.

Q 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?

A Merits; it might help solve the problem.

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

A DHS should be sharing cybersecurity tactics with everyone in the United States, not just large companies.

Q How can liability structures and insurance, respectively, be used as incentives?

A Insurance? No way. It is just a tax for something which is not their fault in many cases.

What other market tools are available to encourage cybersecurity best practices?

Q 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?

A Presidential Orders

Ran out of time here....

In what way should these standards, practices, and guidelines be promoted to small businesses and multinationals, respectively, and through what mechanisms? How can they be promoted and adapted for multinational companies in various jurisdictions?

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?

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?

○ Which industries/groups have voluntary governance mechanisms?

○ Do existing voluntary governance mechanisms have cybersecurity-related constraints?

○ What are the benefits and challenges associated with voluntary governance mechanisms?