Name: Dong Liu	Email: dongl@andrew.cmu.edu

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

   In my opinion manufacturing companies might be the answer.

   In people's common sense, manufacturing robots / machinery, which have fixed routines, are not likely to be compromised by external intrusions. And for those people in charge in such companies, they might focus more at utilizing production capacity and profit rather than security.

   However, since more and more devices have been connected, it is essential to provide necessary isolation to protect the machinery themselves, which often lack in such systems. In addition, most of the control system were written in old insecure languages such as C, a single mistake might make a serious vulnerability.

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

   Government subsidizing would be an option. In this case, a nation-wide standard should be carried out to make sure they applied the resource to the right place.

   When subsidizing is not an option, we can require businesses to hire security professionals based on the size. A public security ranking system can be also used to inspire businesses to focus more on security

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

   (1) How soon can we detect a security incident after it happens?

(2) Service & data recovery time after an incident

(3) Are we facing less security incident now than before? By how much?

The most important part in cyber security is threat prevention; however it is not easy to actually measure the strength of the defense of an organization. Although one may say that we can conduct penetration testing, but such testing cannot cover all problems. On the other hand, penetration testing, at some level, could also result in data leakage and compromise.

Therefore, the reaction time of incident detection becomes the most important measure. From the perspective of math, if the reaction time is short enough, the harm made by the incident should be indefinitely near to zero because we can start to respond and carry out the countermeasure.

The recovery time is also important since data and service recovery will be the subsequent process after incident detection. The recovery will also have directly impact on the stakeholders. For the same reason that the strength of the defense cannot be easily quantitated, what we can compare is the current situation and the history data.

4. 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?

In China, there is no explicit policy, however, let’s say in government or some organizations, if there was data leak or security breach that result in loss to national assets, the person responsible along with the head of the department, will be held responsible for the incident.

In order to keep his or her position, the head of the department have to pay attention to the security issue. And, investment will be made regularly to improve the security of his department.

5. **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?**

   (1) Security cannot be easily measured and the cost for “enough” security is not easy to be calculated. For the executives, they will focus on things which is more “accountable” and can better convince the board.

   (2) Besides government subsidize, study cases caused by security breach happens in similar companies, which result in losses, might be a feasible way to encourage the company to invest some money (might still “not enough”, but better than “not at all”) to security. Because from the case study, losses are more “accountable”, and the case itself will have more persuasiveness than common security advertisement to the people in charge.

   (3) Long term, multiple investment of small amount is better than one time huge investment since they will have less impact in earnings of the company, while provide continuous improved security for companies.

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

   Small businesses focus more on profit growth and relations to the customers. Based on my experience in a small company (in Europe) that have less than 15 people, security are ensured by company policy and staff’s consciousness. The company’s computers are protected by free security software (which means no support from the vendor) with Administrator’s privileges was locked. In the small business, changeful missions and tight deadlines makes both investments and incentives less than big companies.

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

   First of all, if such program is optional, the initiative is at the companies' side. They may or may not strictly follow the standard before they "get" the assistance. There must be practicable approach for DHS and government to "check" how well they follow the guidelines in the program. Unless enough performance was performed, less financial assistance will be provided.

8. **How can liability structures and insurance, respectively, be used as incentives?**

   Liability will result in changes to the profit formula for the companies, which might force companies to invest in security. Insurance, from my point of view, have no direct impact to security. Although purchasing insurance will reduce the loss to the companies when security issue happens, however, for data like intellectual property, they are indeed lost and this might be bad for entire sector or even the nation.

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

   In my opinion, promoting the competition in the security vendors might be an offbeat approach. Since it might make the security services more affordable, the cost reduction will increase the incentives for companies to invest in security. In China, comparing to 10 years ago, most of the security client is free now. To adapt such situation, the foreign security providers like Kaspersky, ESET, have to make special prices in Chinese market, the result is that more and more users will

have better protection in their computers, which greatly increases the overall security of China's national cyberspace.

10. **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?**

    In people's mind, government's credibility is better than single organizations. DHS could maintain a list of the companies who participated this program and make it public. This list, might increase the reputation and bring potential customers to those companies, which as well act as incentive for the company to put effort in cyber-security.

11. **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?**

    Long term / regularly monitoring and assistance will be the best way to achieve this. A good example should be the cyber storm hold by the DHS, which is performed and updated based on the current situation every 2 years. We should find an optimal update cycle. In this cycle we should re-analyze the threat model and revise the framework as needed, followed by a practice among the organizations.

    In this manner we can ensure that best practices and standards are properly updated.