Comments :Incentives To Adopt Improved Cybersecurity Practices

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

Businesses in different sectors generally have different incentives to make cybersecurity investments, due to the nature of their businesses and their businesses' operational dependencies upon cyber capabilities. A business that happens to be primarily a large steel producer will not ordinarily have the same operational dependencies upon cyber capabilities, as would another business that functioned as a multinational electronic commerce business. Due to the operational difference between these two types of businesses, for example, the ecommerce business is inherently incentivized with an appreciation for cybersecurity. The appreciation is based on the value of the business' dependency on ecommerce and the cybersecurity that attempts to assure that the business' information systems and information are continuously available for the variety of multinational's customer base. Further, such a multinational electronic commerce business, by virtue of being a multinational business will have a multitude of merchant partnerships, whose operations will extend into the cyber realm, and whose information systems infrastructure also have to be concurrently available to the multinational's customer base. The effect of the type of operational dependency of the multinational electronic commerce business is such that it is inherently incentivized to make cybersecurity investments more than a business that is primarily large steel producer, for example.

For a business that is primarily a large steel producer, provided its main operational effort is still associated with the manufacture of steel, a realization of incentives to make cybersecurity investments may be more abstracted. Particularly if a cyber attacks do are not known to such a business to have negatively, significantly, and directly impacted its operational capabilities, i.e., the steel business is not prevented from having its continuously hot smelting furnace smelt steel. There may be indirect negative impacts, such as a cyber attack on the electric power grid that supplies electricity to the steel plant, however, such a steel business, although concerned about power supply, would probably take steps that are other than cybersecurity, to mitigate the impact of such power outages. Overall, in this example, the impacts of cybersecurity on the bottom-line may be different for both types of businesses because of the difference of the impact of a cyber presence on each of their bottom-lines.

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

Since many businesses exist to make a profit for its shareholders or proprietors, and seek to do so continuously into the future. Most businesses align their efforts and investments to buttress the goal of amassing profit. Most businesses, ostensibly, do not appreciate cybersecurity's contributions to their goal of amassing profit. It is usually when such businesses' main operational effort is undermined, usually through cyber attacks, that there arises a sense of appreciation for cybersecurity. Most of the business that realize this are usually businesses that have a significant operational business aspect that is dependent on

cyber capabilities and that have to be protected through some means of cybersecurity. Because many businesses will reach these points of realization at different paces and in different forms, consequently the assessments of the costs and benefits of enhancing their cybersecurity will differ correspondingly to the rate at which the businesses realize the need for cybersecurity. Therefore the manner in which an electronic commerce business would assess the costs and benefits of enhancing their cybersecurity will differ significantly from the way a business that manufactures steel would conduct the same sort assessments of the costs and benefits of enhancing their cybersecurity.

An electronic commerce business is generally heavily cyber based and so it is able to realize more immediately the costs and benefits of enhancing their cybersecurity in order to ensure the availability of its information systems to support its profit making. The assessment for an electronic commerce business, for example, would be based heavily on the cost of implementing security technical controls as well as the operational costs the that the technical controls will bring about, versus the benefit of the assurance that their information systems are likely to remain available at critical times of high online sales. It is conceivable that an ecommerce business will take further precautions during the days of anticipated high sales, such as the annual Black Friday and Cyber Monday Sales days. Whereas, for a steel manufacturer, provided its main operational effort is still associated with the manufacture of steel, such realization of the need for cybersecurity efforts may be farther fetched. Particularly if a cyber attack does not hamper a steel business from having its continuously hot smelting furnace to smelt steel. The impacts of cybersecurity on the bottom-line will be different for both businesses because of the impact of a cyber presence to the bottom-line.

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

Perhaps one effective way to encourage businesses to make investments in cybersecurity is to expose them to the economic theories of Coase Theorem and Pareto efficiency. Though this is a cybersecurity issue, the approach to the solution may not be within the cybersecurity field. The fact is that many businesses do not consider cybersecurity a worthy investment because the returns are not apparent to them, whereas in fact, those same businesses pose a set of externalities in the economic sense. The externalities are that the cost or benefit of the same businesses to not engage in cybersecurity investment impacts another business that would otherwise not involved with the business and that also has not chosen to take on either the costs nor benefits from the same situation.

What the Coase Theorem does is that it addresses the economic efficiencies of the economic outcome of the lack in investments in cybersecurity with consideration of the externalities brought upon businesses by the lack in investments in cybersecurity. The Pareto efficiency is more controversial in this context than Coase Theorem in that, even though the goal is to combine Pareto with Coase to reach an optimal distribution investments in cybersecurity, this combination could be perceived as the government "picking winners and losers" with a heavy hand. However, since businesses are not the same and are not in the same situations at the same times, their respective appetite for investments in cybersecurity will likely be different

so the optimal investments in cybersecurity will differ from business to business over time, hence there is a need to optimize each business' investments in cybersecurity through Pareto optimality.

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

One way to determine whether a business can measure the success and the cost-effectiveness of their cybersecurity programs is by establishing a definition for the cost-effectiveness of cybersecurity programs. The OMB Circular No. A-94 (Revised) defines it by stating that a cybersecurity "program is cost-effective if, on the basis of life cycle cost analysis of competing alternatives, it is determined to have the lowest costs expressed in present value terms for a given amount of benefits." This implies first, that a business' cybersecurity costs are to be analyzed on a security life cycle approach, and second, that cybersecurity programs could be implemented such that they are designed to achieve a selected risk profile at the lowest present value cost, and third, is that this measurement of success and the cost-effectiveness be conducted within a framework of risk management. Some businesses already conduct these risk management in order to measure the success and the cost-effectiveness of their current cybersecurity programs. Some small businesses do not see the connections among these three factors nor do they appreciate how implementing an efficient risk management framework supports the continued success of their business.

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

Because some small businesses generally have, as a commonality, an immature cybersecurity program, they generally need the technical assistance to be able to implement an efficient risk management approach. Small businesses are also more apt to seeing how they can gain a competitive advantage by being seen to take security seriously. In that a small businesses usually has a core of attached and loyal customers, and these small businesses want to be known as a business that protect its assets, its reputation, and its customers. So, an incentive for a small business need not only be in the form of technical assistance, but also in the form of understanding the relationships between a thriving small business and the implementation of an efficient risk management approach in support of a robust cybersecurity program. Further, an efficient risk management approach not only brings about a maturing and robust cybersecurity program, it also informs the proprietors about salient details previously unknown to the proprietors of the small business. Therefore, two incentives that could be particularly different for small businesses is the technical assistance that a small business may need since they may be unable or unwilling to pay for, and the knowledge and intelligence of their business that an efficient risk management approach can bring to them.

6. 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?

One of the cost of compliance is the externalities imposed upon small businesses that are already subject to cybersecurity requirements. Requirements enacted to protect patients from big businesses have been externalized as a burden upon small businesses. One such cost of compliance results from HIPAA. Some small businesses in the health field would rather reduce their operational costs by leasing virtualized cloud resources, however, due to HIPAA, they are forced to house their own information systems infrastructure due to the liabilities associated with transferring patient information to a third party cloud services provider. Therefore, if there are mandates imposed upon small businesses, particularly those in healthcare sector, the cost of compliance will become onerous upon the small medical businesses that have not been able to developed a mature cybersecurity program.

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?

For small businesses, one thing that the process of providing governmental financial guarantees or assistance could accomplish, alongside the governmental financial guarantee, is the business intelligence that a business comes to know about itself after going through the requirements needed to be able to be eligible for governmental financial guarantees. This intelligence would arise from the introduction of the use of a framework of risk management. An efficient risk management approach not only brings about a maturing and robust cybersecurity program, it also informs small business' proprietors about salient detail previously unknown to the proprietors of the business.

Two possible impacts of requiring entities to join the DHS Program prior to receiving government financial guarantees or assistance is that cost of compliance could discourage small businesses from being viewed as an entity that ought to be affected by such a mandate or requirement, and second, the lost opportunity to enable a small business to gain the business intelligence it may have otherwise gained had the business gone through the process of receiving government financial guarantees. As previously stated, the business intelligence would arise from the use of an efficient risk management approach. Though a small business could do this on their own without government assistance, however, many small businesses do not have the depth and breadth of data available to be able to develop the most efficient risk management approach suitable for their business. In addition, mandates that are not market based have a tendency to skew the marketplace such that businesses that are uncertain about the benefits of joining a DHS program in exchange for receiving governmental financial assistance pursuant to cybersecurity incident are likely to posture themselves in a way that exempts them from the mandates altogether.

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

Through the implementation of Coase Theorem, liability structures can used to incentivize businesses to adopt cybersecurity programs that are based on a security life cycle approach within a framework of risk management. In such a case, property rights are assigned regardless of the allocation. The implementation of Coase Theorem will support the

implementation of insurance where risks by entities can be shifted based on the known property rights, and premiums can be determined based, in part, on an efficient risk management approach to the way a business' information systems infrastructure are postured for cybersecurity.

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

Perhaps this suggestion would not be appropriate for small businesses, however, large multinationals and national governments may be able to participate in vulnerability markets. As a way to forestall unknown forms of vulnerabilities. Discoveries of zero-day exploits have been becoming a booming market lately and many startups as well as large defense contractor companies participate in the market of vulnerabilities. Such a market can be brokered by entities such as CERT. This will enable the large corporations that can be heavily affected by a vulnerability and that benefit from the absence of the same vulnerability, to address the vulnerability without having to shift its burden onto smaller businesses or individuals in the form of an externality. Such markets also have the ancillary effect of fostering the search for vulnerabilities. This, ostensibly, is bad because it can be argued that vulnerabilities need not be discovered because they serve to enable malicious attackers to undermine the cybersecurity of many businesses. However, undermining the vulnerabilities market and relegating it to the black-market has a similar effect as Prohibition did. If there is money to be made and the market can exist, then there should be a framework to enable the free trade of vulnerabilities within an appropriate regulatory framework.

10. 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?

From a business perspective, the Coase Theorem, if that were the framework within which many business were operating, would cause those same businesses to update their practices provided the businesses understand that there is a need for updating and that the updating would be better for their business while in the Coase Theorem framework.

References:

Blumm, Michael C. "Public Choice Theory and the Public Lands: Why Multiple Use Failed." Harv. Envtl. L. Rev. 18 (1994): 405.

Böhme, Rainer. "A comparison of market approaches to software vulnerability disclosure." Emerging Trends in Information and Communication Security. Springer Berlin Heidelberg, 2006. 298-311.

Eskridge Jr, William N. "Politics without romance: Implications of public choice theory for statutory interpretation." Va. L. Rev. 74 (1988): 275.