ENCRYPTICS™

Response to NIST Inquiry:
Incentives to Adopt Improved Cybersecurity Practices
April 29, 2013

NL Systems, LLC dba Encryptics
5566 W. Main Street, Suite 207
Frisco, Texas 75033
877.503.4781
encryptics.com

First of all, we want to begin by expressing our excitement about the national effort to standardize best practices and guidelines regarding cybersecurity and critical infrastructure. As a growing company involved in cybersecurity, we intend to participate as much as possible in this process. Our comments below are based on our own operational policies as well as feedback we receive from our partners and customers. To learn more about our organization, please visit encryptics.com.

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

   We are not aware of any incentives.

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

   All business sectors lack sufficient incentives to make cybersecurity investments. Critical infrastructure sectors such as defense, energy, and information technology have higher liability due to the type and amount of data they transfer and store. Perhaps these sectors should have greater incentives than others.

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

   Most businesses weigh the risk versus the cost, and only enhance cybersecurity if the risk is high enough to justify the cost. When businesses decide to take a proactive approach to enhancing cybersecurity, they generally go with the least expensive solution or one that meets the minimum requirements. A more common response is a reactionary one in which businesses wait until they experience a serious security breach before they make significant investments.

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

   Any rewards-based program designed to help grow businesses would encourage greater investments in cybersecurity. Such incentives could include tax breaks, government refunds, and/or insurance programs. Rewards could include lower costs or refunds for compliance as well as additional benefits for early adopters. An incentive program could define metrics in order to track improvements, designate levels of success, and award certifications for security. Insurance programs in particular could help mitigate the financial implications a business faces after experiencing a security breach. An insurance program could also provide discounts to businesses that meet certain voluntary and/or mandatory requirements. A well designed insurance program should encourage participants to report security breaches in order to facilitate the use of breach analytics.

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

   Businesses assess total cost of ownership when considering cybersecurity solutions. To measure the success of a cybersecurity solution currently in place, businesses generally ask the following questions: (1) Did we experience a security breach? (2) How many records were associated with the breach? (3) How much money did we lose? Unfortunately, businesses must measure success and

cost-effectiveness of cybersecurity solutions internally, using a trial-and-error method, because businesses that experience security breaches don't want to disclose this information. For example, in Texas, state agencies and universities are supposed to report security breaches to the Chief Information Security Officer at the state's Department of Information Resources, but such reporting has been a challenge. If we could encourage greater information sharing about cybersecurity, businesses would have a much easier time measuring success and making decisions. Such sharing would also promote stronger networks across sectors and better protect critical infrastructure.

6. **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?**

   Most policies in the Unites States are based on penalties rather than rewards. Policies such as HIPAA (Health Insurance Portability and Accountability Act) are effective because businesses want to avoid fines, but in these cases, businesses generally do the bare minimum to comply. Rewards-based incentives are needed to encourage more serious and effective security investments.

7. **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?**

   Small businesses encounter steeper barriers because cybersecurity investments are cost prohibitive. Multi-national businesses also encounter barriers due to legalities involved in global commerce. For example, a partner of ours based in Europe chooses not sign contracts with US companies due to indemnification clauses. As a result, such businesses may not be able to procure the best cybersecurity solution on the market and will be less likely to make cybersecurity investments if solutions are limited.

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

   We are not aware of any incentives specific to small business.

9. **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?**

   The cost of compliance varies by industry. For example, businesses in the healthcare industry must comply with HIPPA regulations; similarly, businesses in the credit card industry must comply with PCI security standards. Compliance is expensive, and because the regulations are complex, businesses are often forced to implement solutions that are not easy to integrate into their normal workflow or manage across their organization.

10. --
11. --
12. --

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

    Several encryption tools are available to help organizations secure their data. For example, Encryptics provides an enterprise solution that eliminates common security gaps where breaches occur, specifically at the device level. Some solutions, however, give organizations a false sense of security. Encryption tools are plentiful, but many organizations lack the knowledge to make informed decisions about security. If an incentive program also provided resources and encouraged information sharing, businesses would be able to distinguish between security solutions and implement the best one for their infrastructure.

14. --

15. **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?**

    Through the Small Business Administration, young companies could be directed to resources such as a list of suggested cybersecurity experts to consult with while their business is in its early stages. This way, businesses would have a jump start on security, which would grow as they grow, and they would not have to implement large-scale security solutions later on. On a global stage, security leaders could come together and create an international organization to set security standards for multi-national businesses. This would alleviate the burden businesses face when trying to meet complex and sometimes contradictory regulations that vary by country.

16. **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?**

    None to our knowledge.

17. **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.**

a. Do organizations participate in voluntary governance mechanisms?
Generally, organizations will not participate in voluntary programs unless they see a benefit. For example, organizations may be more willing to adopt security standards and best practices if they understand it will give them a competitive advantage in the market place—participants will be better equipped to mitigate risks and assure customers of this capability.

b. Which industries/groups have voluntary governance mechanisms?
We are not aware of any voluntary governance mechanisms.

c. Do existing voluntary governance mechanisms have cybersecurity-related constraints?
NA

d. What are the benefits and challenges associated with voluntary governance mechanisms?
A benefit is that rather than requiring organizations to meet mandatory standards, voluntary governance lowers the financial burden because organizations are able to implement financially viable solutions. A challenge, however, is that data exchanges between organizations lack consistency because each organization is free to implement solutions that may not be secure or compatible with other solutions.