ENCRYPTICS®

Response to NIST Request for Comments: **Developing a Framework to Improve Critical Infrastructure Cybersecurity**

February 28, 2013

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

Contents

Cybersecurity Comments

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.

Current Risk Management Practices

1. What do organizations see as the greatest challenges in improving cybersecurity practices across critical infrastructure?

Legacy systems and processes, developed over time without foresight for cybersecurity risks, pose a significant challenge to organizational efforts to enhance cybersecurity across critical infrastructures. Remediating an array of applications could present significant risk to the organization and result in long delays in achieving the desired cybersecurity improvements. Targeted risk assessments to uncover high-risk cybersecurity vulnerabilities are crucial to understanding and prioritizing the most important areas requiring remediation. Leveraging methodologies that can be applied to achieve higher levels of security without requiring a complete platform rework or overhaul will bring the greatest benefit in the shortest timeframe at the lowest costs.

2. What do organizations see as the greatest challenges in developing a cross-sector standards-based Framework for critical infrastructure?

Collaboration and coordination are critical in developing an effective and usable standards-based framework. Such an endeavor within a single sector would be highly challenging. Cross-sector frameworks amplify the challenge as each sector may seek to protect its investment and minimize costly changes that could adversely impact their current mode of operation. In certain cases in business and technology, gateways have served to minimize impact and facilitate a way for two disparate protocols or entities to interact/interoperate without levying the burden of change upon an individual entity. Perhaps a similar approach could be utilized with regard to cross-sector frameworks. As long as the individual components and the sum of the parts can be made secure, the objective may be achieved without an unfair burden.

3. Describe your organization’s policies and procedures governing risk generally and cybersecurity risk specifically. How does senior management communicate and oversee these policies and procedures?

As a data security company, we tend to stress these topics much more so than companies in other industries. We strive to educate organizations about governing cybersecurity risk, and to do so, we try to focus on solutions rather than scare tactics. Because cybersecurity is our business, senior management is actively involved in creating policies and procedures for ourselves and for outside entities. To govern our cybersecurity risk, we utilize our own products, developed to address issues of authorship and document integrity. Our products provide True Digital Rights Management (DRM) to protect data in all states—at device, in transit, in use, and at rest—as well as Data Loss Prevention (DLP) to automate the encryption process using predefined policies. These mechanisms bridge common security gaps, helping organizations reduce liability and comply with standards and regulations such as the Health Insurance Portability and Accountability Act (HIPAA).

4. Where do organizations locate their cybersecurity risk management program/office?

Many organizations do not have a risk management program/office, but rather leave cybersecurity related risk management responsibilities to the individual responsible for managing the organization's firewall; this is typically a network security function performed within the IT department and is often handled by a lower level technician.

Alternatively, depending upon the industry and the organization's size, the risk management program/office may be located in different areas within the organization. In many organizations, this function resides with the individual that is responsible for general risk management. However, due to the technical complexities of cybersecurity, the individuals given this responsibility often lack the knowledge, skills, and/or experience necessary to effectively support the organization in this capacity.

The program/office should report to senior leadership outside of the reporting structure of IT to minimize conflicts of interest and ensure unbiased auditing.

5. How do organizations define and assess risk generally and cybersecurity risk specifically?

Organizations seem to have a difficult time assessing cybersecurity risks, specifically because they are intangible threats. While they have huge implications, cybersecurity risks are very hard to measure until they have become a perceptible problem. As a result, many organizations take a reactionary rather than a proactive approach to security. This is evident in the amount of time it takes organizations to identify and address a breach that has occurred. If organizations were more proactive in properly assessing risks, they would be able to identify and respond to a breach more quickly.

6. To what extent is cybersecurity risk incorporated into organizations' overarching enterprise risk management?

In general, cybersecurity falls into the hands of the IT department; however, delegating responsibility in this way is a short-sighted solution that only exacerbates security issues. In order to adequately address cybersecurity risks, organizations need to understand that everyone is responsible for preventing and responding to breaches and attempted breaches. Individuals who are not properly trained to prevent and recognize a breach—typically those outside of the IT department—often contribute to security vulnerabilities and weaken an organizations' defenses. Thus, it is the organization's responsibility to educate all employees and implement common solutions across all departments. All employees must understand risks, recognize threats, and be prepared to respond appropriately to a breach, and this can only happen if organizations make security a priority.

In addition, organizations need to understand that in order to successfully implement security solutions, they must also involve entities outside of their organization—customers, vendors, competitors, and the government. Because no organization operates in a vacuum, participation from all parties is essential. Similarly, cybersecurity needs to be factored into the design, development, and adoption of products; that is, organizations need to ensure that all of the products they utilize (regardless of purpose) fit into the overarching security solution. If products do not address security in some way, then they can constitute a weak point within in the organization. Finally, organizations need to view security as an ever-evolving effort. Implementing solutions is only the first step—organizations must continually reevaluate solutions as the risks change.

7. What standards, guidelines, best practices, and tools are organizations using to understand, measure, and manage risk at the management, operational, and technical levels?

Most companies rely on self-governing rules or standards and guidelines already in place within their respective industry to serve as an umbrella that governs risk at every level. For example, HIPAA sets standards for healthcare; state public utility commissions set standards for energy; and the Federal Communications Commission set standards for telecommunications. Nevertheless, it is difficult for organizations to measure risk of breaches by hackers and foreign entities because of the intangible quality of the internet, data collected, etc.

Furthermore, most tools used to measure risk are reactionary in their use or meant for planning purposes only. We need to encourage organizations to take a more proactive approach. The simple fact is that breaches will occur; however, if we can reduce the attack vectors, ensure user authentication, minimize the usability of the data gained through a breach, and be aware of breaches as they occur, we are better positioned to identify and address them, or prevent them altogether.

Unfortunately, there is no central or industry-specific place for organizations to go to for suggestions about security standards, guidelines, or practices. There is also no campaign or awareness program to help educate organizations about the risks to each industry or the wide-reaching ramifications that breaches can have on consumers and businesses.

8. What are the current regulatory and regulatory reporting requirements in the United States (e.g. local, state, national, and other) for organizations relating to cybersecurity?

We are not aware of any reporting requirements within our specific industry. We are aware of regulations within healthcare (HIPAA), finance (Gramm-Leach-Bliley Act) and national security (Homeland Security Act). We are also aware of various acts and bills under consideration that have not yet passed.

We feel that the inconsistency in regulations within and across industries only adds to the confusion surrounding cybersecurity. Different acts and bills attempt to address the same problem in different ways, and many organizations fall under multiple regulations, making it more costly and complicated to comply. We believe that an attack on one organization is essentially an attack on all organizations, regardless of industry. We need a flexible framework that provides unified guidance for industry-agnostic areas such as user authentication.

9. What organizational critical assets are interdependent upon other critical physical and information infrastructures, including telecommunications, energy, financial services, water, and transportation sectors?

Similar to the OSI model, organizational critical assets depend on other foundational physical and information infrastructures. The foundation's base layer includes energy and water, as it is the fundamental enabler for virtually all other critical assets. The second layer includes transportation and telecommunications for the transport of people/goods and information, respectively. The upper layers contain the critical organizational infrastructures that enable operations such as financial.

10. What performance goals do organizations adopt to ensure their ability to provide essential services while managing cybersecurity risk?

Organizations are gradually beginning to understand how important it is to take a proactive approach—before a breach occurs—when it comes to managing cybersecurity risks. More important, however, is the ability to manage risks without incurring high cost or interrupting the organization's normal workflow. As a result, many organizations compromise high levels of security and manage risks simply by meeting minimum security requirements (if any) for their organization. Concerns about ease of implementation, ease of use, and cost of service often inhibit an organization's efforts to mitigate risks.

When organizations do take a proactive approach to manage risks, they tend to favor simple, out-of-sight solutions. For example, some products provide security at a particular point within an organization's infrastructure—at a gateway, server, etc. This way, users don't have to do anything to secure data, but there are security gaps between the device and the network hardware. With solutions that offer Data Loss Prevention (DLP) and automated options at the device level, organizations can maintain normal workflow without comprising security.

11. If your organization is required to report to more than one regulatory body, what information does your organization report and what has been your organization's reporting experience?

We have no obligation to report any information.

12. What role(s) do or should national/international standards and organizations that develop national/international standards play in critical infrastructure cybersecurity conformity assessment?

Companies that seek to provide technology products and services to US and Canadian governments are required to comply with certifications such as the Federal Information Processing Standard (FIPS), and there are rigorous processes in place to ensure compliance. Companies that serve in critical roles associated with supporting critical infrastructures should be required to demonstrate conformity with cybersecurity standards. The entities responsible for establishing the national/international standards should be accountable for ensuring a program is in place to assess compliance and ensure conformity.

Specific Industry Practices

1. Are these practices widely used throughout critical infrastructure and industry?

In our experience, the answer is "not always." Unfortunately, not all organizations within our scope widely use these practices. Barriers to acceptance involve many factors: organizations may be ignorant of the risks, they may not have the resources necessary, or they simply may not stress the urgency of implementing these practices.

2. How do these practices relate to existing international standards and practices?

Our service deals primarily with the needs of public and private organizations domestically.

3. Which of these practices do commenters see as being the most critical for the secure operation of critical infrastructure?

In our opinion, the practices most critical for the secure operation of critical infrastructure are Encryption and Key Management and Identification and Authorization of Users Accessing Systems. Protecting data—whether it is intellectual property, personal information, financial or legal documents, etc.—must be a top priority. However, many organizations feel that they don't need *that* level of security. The issue is that most organizations don't prioritize security until after they experience a breach and/or a significant interruption in their process.

4. Are some of these practices not applicable for business or mission needs within particular sectors?

In the industry sectors we regularly deal with, the practices apply directly to business or mission needs. Because every industry sector is interconnected on a global scale, we believe that these practices should not be divided by industry, but unified to better protect information across all industries.

5. Which of these practices pose the most significant implementation challenge?

Privacy and Civil Liberties Protection and Identification and Authorization of Users Accessing Systems pose the most significant implementation challenge because these practices affect everyone. To overcome these challenges, we need to develop user-friendly solutions that can easily integrate into existing workflows. In addition, these solutions should give users the power to decide what information is available, control the usage and access of that information, and maintain control even after the information has left their possession.

6. How are standards or guidelines utilized by organizations in the implementation of these practices?

In the industry sectors we regularly deal with, most organizations do have some technology standards or technology business implementation plan. However, in many cases, organizations don't understand the implications of not including a practice like Identification and Authorization of Users Accessing Systems in the plan.

7. Do organizations have a methodology in place for the proper allocation of business resources to invest in, create, and maintain IT standards?

This area is often overlooked if the business is focused on sales or growth. In some cases, IT is outsourced and the creation and maintenance of IT standards are deferred in the interest of cost savings.

8. Do organizations have a formal escalation process to address cybersecurity risks that suddenly increase in severity?

We are not aware of any organizations that have a formal escalation process to address cybersecurity risks, but as a company that strives to educate others about security, we would certainly support the adoption of such processes. It is important that organizations understand the ramifications of a breach and educate their employees accordingly.

9. What risks to privacy and civil liberties do commenters perceive in the application of these practices?

Many organizations want adopt practices like Bring Your Own Device (BYOD) to accommodate traveling and remote employees. However, when personal and business-related data is stored on a single device, any administrative access to the device or to the user's account information can be construed as a violation of privacy and/or civil liberties. Nevertheless, administrative access is needed to manage the organization's network and protect its critical data. Solutions that can mitigate risks regardless of the device, delivery method, and storage location will help minimize these potential violations.

10. What are the international implications of this Framework on your global business or in policymaking in other countries?

While we primarily sell to and support domestic organizations, during discussions with international law firms, we discovered potential barriers in countries like Russia, Indonesia, and Malaysia whose governments monitor all incoming and outgoing communication. For example, if such a government utilizes 128-bit encryption, then users within that country would not be able to adopt 256-bit encryption, and so on.

11. How should any risks to privacy and civil liberties be managed?

Ideal solutions will empower both the individual and the organization to manage the data that they are entitled to control over the course of its lifecycle while ensuring that access is limited to necessary participants only.

12. In addition to the practices noted above, are there other core practices that should be considered for inclusion in the Framework?

We have mentioned several far-reaching concepts that are applicable across virtually all core practices. To be most useful and universally acceptable, we feel the framework must demand that data is encrypted at its source, users are properly authenticated, and users maintain control over their data even after it has left their possession.