Business Executives
for National Security

RFI Response: Developing a Framework to Improve Critical Infrastructure Cybersecurity

This comment is in response to the Request for Information (RFI) from the National Institute of Standards and Technology (NIST) published in the Federal Register on February 26, 2013. NIST is conducting a comprehensive review to develop a framework to reduce cyber risks to critical infrastructure (the "Cybersecurity Framework"). NIST has issued a RFI to gather initial information on the many interrelated considerations, challenges, and efforts needed to develop the Framework.

I. Introduction

Business Executives for National Security (BENS) is a nonpartisan non-profit composed of 450+ senior executive members nationwide. BENS assists government partners in developing best business practice solutions to our nation's greatest national security challenges. BENS is member driven and financed—members individually participate in and fund the work BENS undertakes and BENS does not seek government funding.

BENS has been undertaking an effort to heighten the awareness of CEOs and board members of the severity of the cybersecurity threat and its risk to business operations. Many members are proponents of the inclusion of cybersecurity in enterprise risk management at the Board and CEO level.

The following comments are a compilation of individual member views and do not represent the position of the organization.

II. General Considerations

In developing the Cybersecurity Framework, NIST should rely on current industry best practices and existing standards. Be mindful that one size does not fit all and cyber best practices may vary by sector. Furthermore, aim for international voluntary standards in developing the Framework. The Framework must be flexible enough to evolve with rapid changes in technology. Finally, legislation is still necessary to ensure the success of the Framework, particularly in incentivizing voluntary participation (e.g., by providing liability protection) and in facilitating much needed two-way information sharing. NIST should learn from history when creating the Framework, noting instances where standards or regulatory regimes resulted in negative unintended consequences.

III. Specific Responses

In addition to the above general comments, BENS members provided specific responses to the RFI in regards to managing cyber risk as noted below:

Process for Assessing and Managing Cyber Risk

Response 1

1. Establish risk priority:
   a. Vulnerability of IT systems to large scale corruption of databases and/or stopping production.
   b. Disclosure of confidential customer information.
   c. Disclosure of financial/sensitive information.
   d. Specific, targeted attacks on services such as website order entry systems.
2. Annual formal review of IT risks documented in a risk assessment document.
3. Informal review of assets most vulnerable to attack, including websites.
4. Reliance on internal and external Auditors to provide risk feedback as part of routine audit work.

Response 2

Companies should consider the following approaches when assessing and managing cyber risk:

1. Establishing a security risk management program and/or organization dedicated to identifying and managing risk.
2. Conducting risk assessments and policy reviews of new products and projects at the onset to identify and mitigate potential security risks from the beginning.
3. Implementing security measures into corporate processes. These measures should be sufficiently flexible to accommodate new demands and regularly reviewed.

Use of Third Party Publications and Approaches

Response 1

The following resources are helpful in improving cybersecurity practices:

- COBIT/ISACA
- InfraGard
- Gartner Group
- Global CIO Executive Summit
- Private Equity CIO Roundtable

The NIST publications are very thorough and serve as a reference document as needed. However, we believe the inclusion of more “elevator speech” summaries in the front of documents would be helpful. In practice, few practitioners have the time to go through many pages of text in order to find good practices. The academic model of writing, where every pro and con is considered, does not serve the interests of most industry practitioners. Plain talk and the avoidance of terms such as “attack vectors” would go a long way towards improving the usefulness of these documents. As a minimum, cybersecurity documents/standards should be divided into a shortened, “active verb” front section and a back section which includes details and more nuanced considerations.

Response 2

Companies may use approaches they develop on their own as well as approaches adopted from a wide variety of external, third party sources, based on their individual needs. External points of reference include, for example, national and global standards-setting groups, which play a key role in the global cyber ecosystem by resolving technical differences and fostering efficiencies. These groups include, but are not limited to, the Alliance for Telecommunications Industry Solutions (ATIS), the Institute of Electrical and Electronics Engineers (IEEE), and the American National Standards Institute (ANSI), as well as the Third Generation Partnership Project (3GPP), a consensus-driven international partnership of telecommunications standards bodies. Using a combination of third party approaches offers greater flexibility to prevent, detect, mitigate, and manage cyber risk.

Cybersecurity Best Practices

Response 1

To reduce their risk profile, companies have implemented:

1. Standard industry practices for infrastructure, including firewalls, anti-virus, and intrusion detection monitoring.
2. Application security, including segregation of duties for core systems, passwords and secure audit trails.
3. Systems development lifecycle (SDLC) for medium to large systems. The lifecycle includes risk assessment.
4. Creation of an IT Security director position, to maintain continuing focus on risks.
5. Routine external and internal audits.
6. High level "macro review" of financials.

Response 2

Cybersecurity practices are an important element of any comprehensive risk management program. Organizations may develop their own as well as consider and adopt practices from multiple sources. Once the relevant practices are chosen, a "top-down" approach to security combined with a "governance framework," may be used to implement them. Such an approach to security, which leverages security across all company business units, has proven to be an effective way to protect and sustain business operations. In addition, a "defense in depth" approach, which provides for multiple layers of security, is a widely accepted practice.