NIST Request for Information (RFI)

Current Risk Management Practices

NIST is interested in understanding whether particular frameworks, standards, guidelines, and/or best practices are mandated by legal or regulatory requirements and the challenges organizations perceive in meeting such requirements. This will assist in NIST's goal of developing a Framework that includes and identifies common practices across sectors.

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

LogRhythm has researched and developed specific product capabilities in support of improving cyber security practices across critical infrastructure. Some of the challenges we see in improving cyber security practices across organizations' critical infrastructure include:

- Education of cyber security risks and practices
  - Properly educating personnel on identifying and mitigating cyber security risks is difficult and costly.
- Lack of formal guidance
  - Existing Cyber Security guidelines are lengthy and too complex to implement.
- Separation between industrial control system engineering and corporate information security
  - The distinct separation between industrial control engineers and corporate information security often creates a silo effect which makes it difficult to implement cybersecurity practices in areas where only engineering personnel fully understand the workings of critical infrastructure. In these types of environments engineering personnel must spend considerable amount of time/resources working with information technology/security personnel to bridge the engineering/security gap.
- Legacy/aging equipment not designed to be secure
  - Aging technology which often lacks basic security support such as vendor software patching, logging capabilities, and built-in access controls.
- Focus on availability vs. Security
  - Specific types of business must sacrifice confidentiality and integrity in order to continue to provide a high level of availability. In these types of environments it can be impossible to take systems offline to regularly patch or even replace outdated systems.

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

Some of the challenges we see in developing a cross-sector standards framework are:

- Different risk thresholds
    - The diverse spectrum of cyber security risk tolerance between organizations. Some organizations may be very averse to risk while others have a higher tolerance for risk.
- Different levels of cyber security capability and maturity
    - The large variance of cyber security maturity and capability between organizations. Some organizations have a notable cyber security maturity level affording them more capability to properly implement cyber security controls.
- Different business operating concerns
    - Differing business operating concerns for organizations. Some organizations lack proper funding or specialized resources and personnel to properly develop a cross-sector framework. There is also a large disparity between organizations business structures and infrastructure architectures which make it difficult to develop a one size fits all framework

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?

The best practice is to develop a comprehensive security program with defined security policies and procedures. Senior management has a key role to communicate and oversee the security program. At a minimum Senior Management should oversee the development, approval, and implementation of the following policies and procedures:

- Access Control
- Configuration Management
- Contingency/Disaster Planning
- Identification & Authentication
- Incident/Event Response
- Information/System Integrity
- Malware Detection/Prevention
- Communication/Network Protection
- Patch/Vulnerability Management
- Personal Security
- Physical/Environmental Security
- Risk Assessment
- Security Assessment
- Security Awareness/Training

- Software Development & Acquisition

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

The best practice is to ensure their cybersecurity risk management program/office resides within their organization at a level where it has direct executive leadership and support. With this in mind most of our customers have located their cybersecurity risk management program/office under the guidance of the office of the CSO/CISO or a similar office reporting to the CEO and/or the Board of Directors.

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

The best practice is to perform a full risk assessment to ensure both general risks and cyber security risks are addressed. The risk assessment at a minimum should include the documenting of business processes, assessment of potential threats, and identification of mitigating controls.

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

The best practice is to incorporate cybersecurity risk management into the overall enterprise risk management program.

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

There are a diverse set of standards, guidelines, best practices, and tools to measure and manage risks. Federal agencies use the “Guide for Applying the Risk Management Framework to Federal Information Systems" described in NIST SP 800-37. Publically traded corporations use the “Enterprise Risk Management Integrated Framework” developed by COSO. Financial institutions use the “IT Risk Management Process” documented in the FFIEC IT Examination Handbook.

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?

There are a diverse set of regulatory requirements and standards related to cybersecurity and breach reporting. Federal agencies follow FISMA, FEDRAMP, DIACAP, and DoDI 8500.2 regulations. Energy providers follow NERC-CIP, NEI 08-09, and NRC RG 5.71 regulations. Many organizations follow regulations specific to their sector like GLBA, HIPAA, and SOX. Some organizations must comply with local state privacy laws like the Massachusetts privacy law 201 CMR 17.00 and The California Online Privacy Protection Act of 2003.

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

Critical assets are highly interdependent upon physical and information infrastructures. For example Energy providers' critical assets are interdependent on both physical infrastructure such as power generation and monitoring equipment and information infrastructure such as networking hardware and software.

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

Organizations provide a diverse set of services which drastically varies their specific performance goals in providing essential services. Energy providers are concerned with providing reliable electrical services which focuses their performance goals on power availability and reliability. DoD (Department of Defense) agencies are far more concerned with providing national defense services which are more focused on performance goals related to the continuance of confidentiality of government information.

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?

Organizations are bound by a diverse set of regulatory requirements each with their own specific reporting requirements. Organizations bound by multiple independent reporting requirements prefer to develop a single report that meets all individual regulating body reporting requirements rather than having to create separate reports for each.

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

National/international standards and organizations like NIST should continue to provide regulatory guidance for 3rd party certified auditors. However, national/international standards organizations shouldn't necessarily be involved in enforcement of regulations, which should probably be left up to the regulating bodies.

Use of Frameworks, Standards, Guidelines, and Best Practices

NIST is seeking information on the current usage of these existing approaches throughout industry, the robustness and applicability of these frameworks and standards, and what would encourage their increased usage. Please provide information related to the following:

1. What additional approaches already exist?

LogRhythm has researched and developed specific product capabilities in support of various frameworks, standards, guidelines, and best practices. Some of the specific frameworks, standards, and guidelines are listed in the table below.

Framework, Standard, Guideline	Organization	Cross Sector	Details
DoDI 8500.2	Department of Defense Agencies	False	The United States Department of Defense Instruction (DoDI) 8500.2 established Information Assurance (IA) implementation guidelines.
FedRAMP	Federal Agencies and Cloud Service Providers	False	The Federal Risk and Authorization Management Program (FedRAMP) established a process to assess and authorize cloud based services consisting of a subset of NIIST SP 800-53 security controls.
FISMA	Federal Agencies	False	The Federal Information Security Management Act of 2002 (FISMA) requires federal agencies to develop, implement, and document a security program to provide protection for agency information and information systems.
GLBA	Financial Institutions	False	The Gramm Leach Bliley Act of 1999 (GLBA) Safe Guards Rule requires financial institutions to develop an information security plan to protect customers personal information.
GPG 13	User of the United Kingdom's Government Connect Secure Extranet	False	The Good Practice Guide number 13 (GPG 13) establishes a set of security practices in order to meet protective monitoring obligations defined in the Security Policy Framework.
HIPAA	Health Care Providers and Insurers	False	The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule requires protection of Electronic Protect Health information (EPHI) by implementing administrative, physical, and technical safeguards.

Framework, Standard, Guideline	Organization	Cross Sector	Details
ISO 27001	Organizations	True	The International Organization for Standardization (ISO) published information technology security standards 27001 in 2005 which explicitly requires formal management control of information security.
NERC-CIP	North American Bulk Electrical System Providers	False	The North American Electric Reliability Corporation – Critical Infrastructure Protection establishes cyber security standards to protect crucial cyber assets that control the reliability of North America's Bulk Electric System (BES)
PCI-DSS	Credit Card Processors	True	The Payment Card Industry Data Security Standard (PCI-DSS) establishes information security standards for the handling of cardholder information.
SOX	Publically Traded Companies	True	The Sarbanes Oxley Act of 2002 (SOX) Section 404 requires management and external audit of the adequacy of a publically traded companies internal control of financial reporting.

2. Which of these approaches apply across sectors?

See table above in question1.

3. Which organizations use these approaches?

See table above in question 1.

4. What, if any, are the limitations of using such approaches?

Some of the limitations to these types of approaches are:

- Sector Specific
    - Approaches which are industry specific ate limited to a narrow application.
- Create Conflicts of Interest

    - Some of these approaches put too much of the assessment onto the organization which can create a conflict of interest.

- Create a “Check Box” Mentality
    - These types of approaches often lead organizations to be focused on practices and technologies that meet a specific requirement rather than having an adaptive cyber security approach.

- Designed for Specific Architectures & Infrastructures
    - A singular approach cannot possibly take into account all possible architectures and infrastructures so some risks may not be properly identified and mitigated.

5. What, if any, modifications could make these approaches more useful?

In order for organizations to adopt an adaptive cyber security approach the following modifications are suggested:

- Collecting and centralizing all log data and other forensically valuable machine data related cyber activities within the IT environment.
- Monitoring and generating deep forensic activity detail on target hosts not present in the existing machine data.
- Monitoring and generating deep forensic activity detail at network ingress/egress points not present in existing machine data.
- Storing all collected and generated forensic machine data for at least 1 year in support of after the fact forensic analysis.
- Applying advanced real-time analysis capabilities against collected/generated machine data for the detection of threats, intrusions, and regulatory compliance violations.
- Applying automated behavioral profiling and baselining techniques to detect abnormal behaviors in support of the above.
- Minimally developing a virtual “Security Operations Center” capability that minimally analyzes highest risk events observed within the environment and implements a formally defined incident response process.

6. How do these approaches take into account sector-specific needs?

Approaches like the ones listed above take into account specific sector needs by addressing specific sector security risks. For example NERC-CIP focus on the protection of critical cyber assets in the bulk electrical system, GLBA focuses on protecting personal financial information, and HIPAA focuses on the protecting personal health information.

7. When using an existing framework, should there be a related sector-specific standards development process or voluntary program?

There should be a model where cross-sector standards are defined that applies to any industry. This cross-sector standard should be supplemented by industry specific standards that augment the cross-sector standard by omitting, further qualifying, or adding additional standards.

8. What can the role of sector-specific agencies and related sector coordinating councils be in developing and promoting the use of these approaches?

Sector specific agencies and coordinating councils play a large role in developing and promoting these approaches. At a minimum they should develop the approaches, chair an advisory board made up of representatives from the sector, and provide training in the form of webinars, workshops, and conferences.

9. What other outreach efforts would be helpful?

Organizations need to have access to supplemental materials to help decipher regulations, guidelines, and standards.

Specific Industry Practices

NIST is interested in information on the adoption of the following practices as they pertain to critical infrastructure components:

- *Separation of business from operational systems;*
- *Use of encryption and key management;*
- *Identification and authorization of users accessing systems;*
- *Asset identification and management;*
- *Monitoring and incident detection tools and capabilities;*
- *Incident handling policies and procedures;*
- *Mission/system resiliency practices;*
- *Security engineering practices;*
- *Privacy and civil liberties protection.*

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

Organizations fall into two categories: those mature in their cybersecurity efforts and those still early in their development. Some organizations are extremely advanced in the cybersecurity efforts which have already implemented the majority, if not all, of these practices. However other organizations' cybersecurity initiatives have been stagnant due to a variety of factor such as the maturity of the organization, type of organization, budgeting constraints, and resource allocation.

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

The large majority of cybersecurity standards and guidelines already include some form of these practices.

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

Organizations place a great deal of value on monitoring and incident response tools and capabilities which form the basis for security control validation. Monitoring practices and procedures provide verification of the other listed practices being implemented correctly and create a means to learn about and potentially improve on the other cybersecurity practices.

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

These practices are truly the core of cybersecurity so they are applicable; however details of implementation may vary dependent on sector due to technology.

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

Two areas that are significantly challenging to implement are:

- Identification and authorization of users accessing systems
- Asset identification and management

These particular challenges are introduced due to the rapidly changing nature of IT and resulting daily introduction and sprawl of new IT components. Monitoring and behavioral analytics can provide an effective mitigating control in this area. For example security tools that provide an independent audit trail based on behavioral analytics can bridge the gap in attribution caused by minimal logging on legacy industrial control system devices.

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

The standards/guidelines provide an industry acceptable framework for properly adopting these cybersecurity practices. However the practices themselves are still general and vague at this point in the process.

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

The best practice is to develop a methodology around allocation of business resources based on their RA (Risk Assessment) and governance requirements. Organizations must assess the likelihood of a risk and the negative impact to the business the risk presents.

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

Incident response polices/processes dictate the escalation to address cybersecurity based on severity/impact.

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

N/A

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

N/A

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

N/A

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

The following additional practices should be included in the framework:

- Centralized Logging
- Forensic Data Generation
- Real-time and Forensic Security Analytics Capabilities
- Virtual or Physical Security Operations Center Capability
- Incident Response and Management