NIST RFI

Developing a Framework to Improve Critical Infrastructure Cyber Security

April 2013

Submitted
By
Regional Cyber and Energy Security (RCES) Center
At
The University of Texas at El Paso
rces@utep.edu

Current Risk Management Practices

NIST has solicited information about how organizations assess risk; how cyber security factors into that risk assessment; the current usage of existing cyber security frameworks, standards, and guidelines; and other management practices related to cyber security. In addition, 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 cyber security practices across critical infrastructure?

- Unpredictable human behavior (dynamic attacks and insider threat).
- Segmentation within Information Technology (IT) organizations.
- Lack of information exchange within an industry's organizations and user communities.
- Lack of communication and documentation.
- No clear understanding of the difference between IT and Operational Technology (OT).
- Gap between IT and OT networks is not properly enforced to ensure integrity.
- New technologies developed and deployed without proper integrated security measures.
- Security impact of mobile devices and storage, particularly in Bring Your Own Device (BYOD) scenarios.
- Not going beyond compliance or only maintaining compliance practices.
- Distrust based on different levels of experience.
- Lack of personnel accountability.
- Understanding the economic return of investment on cyber security.
- Legacy systems and integration with new technologies.
- Lack of common vocabulary in different practices.
- Lack of spectrum awareness for utility owned RF systems used in operations

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

- There are technologies unique to an organization, but not standard across sectors.
- Focus of the sectors is different (e.g., patient records versus finances).
- Concerns about creating static solutions for a dynamic environment.
- Need to merge the lessons of the past with the technologies and techniques of the future.
- Understanding the economic return on investment in cyber security.
- Legacy systems and integration with new technologies.
- Lack of communication between sectors.
- Lack of common vocabulary.
- Difference in regulators from one sector to another.

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

- Our policies are instantiated within The University of Texas at El Paso's institutional compliance and Information Security Office (ISO) Security Policies.

- The university depends on the experience of our security staff. Contact channels are published internally so personnel are aware who appropriate contacts are in case of risk generally and cyber security risk specifically. For cyber risk, the university's Information Security Office is almost always involved, except in rare cases involving insider threats where notification and/or disclosure through normal channels could compromise an investigation.
- We communicate concerns and knowledge on cyber risk to the entire university community based on our organization's research, knowledge, and news feeds.
- Management conducts weekly meetings; a standing topic is discussion of any relevant cyber security risk over the previous week, either within the university community or the overall energy and technology sectors at large.

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

- In our experience, cyber security risk management offices are typically housed within a local Information Security Office, with a Chief Information Security Officer (CISO) leading a team of responders.
- Our own organization improves the existing cyber risk management system of the ISO by providing academic knowledge and innovative research on cyber security for operational technology assets of the University.

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

- Risk is defined according to standards and guidelines set by organizations such as NIST, NERC, DoD and DHS (i.e. CVSS, DIACAP, SCAP, etc.).
- Our organization also uses our internally developed Vulnerability and Risk Management (VARM) process, which is being evaluated by a number of large multi-national services firms for an eminent rollout.
- As part of the supporting research for the VARM process, we have identified a variety of ways to define and calculate risk. The following literature articles are **representative** of the approaches; please contact us for the comprehensive list of surveyed documents, if interested:
    - Philip L. Campbell, Jason E. Stamp, "A Classification Scheme for Risk Assessment Methods", Sandia National Laboratories, 2004.
    - **Patent No. 61/725,474. "System, Method and Apparatus for Assessing a Risk of one or More Assets within an Operational Technology Infrastructure." 2012.**
    - Sandia National Labs. "Sandia National Labs' Security Risk Assessment Methodologies". http://www.sandia.gov/ram
    - Nancy A. Renfroe, Joseph L. Smith, "Threat/Vulnerability Assessment and Risk Analysis", 2011.
    - M.H. Faber, M.G Stewart, "Risk Assessment for Civil Engineering Facilities: Critical Overview and Discussion", 2003.
    - Zeki Yazar, "A qualitative risk analysis and management tool-CRAMM," SANS Institute, 2002.
    - Kang Lin, Keith E. Holbert. "PRA for Vulnerability Assessment of Power System Infrastructure Security." 2005.

- In addition, the following standards documents are of interest to this questionnaire:
    - National Institute of Standard and Technology, "Guide for Conducting Risk Assessment," NIST Special Publication 800-30, Revision 1. 2011.
    - National Institute of Standard and Technology, "Security and Privacy Controls for Federal Information Systems and Organizations," NIST Special Publication 800-53, Revision 4. 2012.
    - National Institute of Standard and Technology, "Guide for Mapping Types of Information and Information Systems for Security Categories," NIST Special Publication 800-60, Volume 1, Revision 1. 2008.
    - National Institute of Standard and Technology, "Guide to Industrial Control Systems (ICS) Security," NIST Special Publication 800-82, 2011.
    - Department of Energy, "Electricity Subsector Cybersecurity Capability Maturity Model," Version 1.0, 2012.
    - National Electric Sector CyberSecurity Organization Resource (NESCOR), "Electric Sector Failure Scenarios and Impact Analyses," Version 1.0, 2012.

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

- Cyber security risk is becoming a bigger and bigger component of organizations' enterprise risk management, since just about every organization of every size relies on systems which maintain the security and privacy of the data.
- Administrators (particularly in information technology) maintain compliance with the standards.
- Unfortunately, most organizations remain reactive to events instead of proactively trying to prevent them.
- Network designs are typically flexible to address the tradeoff between access to operational equipment and security, but the enterprise risk management plan must demonstrate an understanding of these tradeoffs.
- Budget constraints also impact (typically negatively) a holistic approach to deploying a cyber security risk management plan.
- There is no understanding of the cyber risks to an organization through spectrum initiated cyber attacks and wireless systems.

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

- National Institute of Standards and Technology (NIST) publications, particularly the 800 series of special publications.
- Department of Homeland Security (DHS).
- Security Content Automation Protocol (SCAP).
- Department of Defense (DoD) Information Assurance policies, including DIACAP.
- North American Electric Reliability Corporation (NERC).
- Federal Energy Regulatory Commission (FERC).

- Information systems certifications including CISSP, CISA, C|EH, CEPT, CompTIA Security.
- Cyber security news feeds.
- Training and conferences such as Blackhat, SANS, ShmooCon, Defcon.
- Open source and proprietary penetration testing tools.

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 cyber security?

- Our organization is not aware of any standard or regulatory reporting requirement besides the fact the information has to be maintained confidential and can only be shared with the parties involved in the process.
- Each organization implements its own reporting requirements. The following organizations implement reporting requirements when providing the results of their cyber studies:
    - DHS, CIA, FBI, NSA.
    - Infragard.
    - Private security firms: Gartner, Pike, Mandiant, Red Tiger Security, InGuardians.
    - Antivirus and Anti-malware developers: Symantec, McAfee, Avira, TrendMicro, Kapersky, etc.
- The following citation provides an approach to categorize risk approaches that could be extended to leverage reporting requirements.
    - Philip L. Campbell, Jason E. Stamp, "A Classification Scheme for Risk Assessment Methods", Sandia National Laboratories, 2004.

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

- Based on the Vulnerability And Risk Management (VARM) process conducted on the operational technology at The University of Texas at El Paso, we have learned that an interdependence connection exists between different critical sectors. We identified critical assets in the university infrastructure (e.g. critical buildings); these critical assets depend on a reliable energy source to conduct day-to-day operations. Such energy sources are typically supported by operational technology that is often controlled by cyber components (e.g. human machine interfaces, standalone computers, etc.) connected through various communication channels (e.g. local area network cables, wireless communications). Any one of these components, if compromised, can bring down all of the interconnected elements.

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

- Meeting work deadlines to provide the required result of any given task/project, and making sure cyber security does not interfere with regular processes.
- Efficiently providing services.
- Guaranteed continuity of service.
- Minimal emergency response time.
- Train organization personnel to achieve pre-determined evaluation criteria.
- Emergency plans and drills to minimize outages with set goals.

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?

- Even though this Center is not required to report to regulatory agencies, from a systems standpoint, we report to the university's information technology and information security departments, and document all of our communications with these entities.
- The information we report relates to projects that require certain clearances and permissions to use University resources for cyber and physical security exercises.
- We also report suspicious cyber activities from external sources into our system.

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

- One of the best roles these groups can provide is to assist in understanding existing threats, and to provide critical guidance to those organizations which must meet the existing and evolving regulations and standards. These organizations can then act as educators relating the newest attacks and threat vectors and enforce data sharing among organizations.
- These organizations should also consider policies that speak to ethical standards to stop unethical practices.

Use of Frameworks, Standards, Guidelines, and Best Practices

As set forth in the Executive Order, the Framework will consist of standards, guidelines, and/or best practices that promote the protection of information and information systems supporting organizational missions and business functions.

NIST seeks comments on the applicability of existing publications to address cyber security needs, including, but not limited to the documents developed by: international standards organizations; U.S. Government Agencies and organizations; State regulators or Public Utility Commissions; Industry and industry associations; other Governments, and non-profits and other non-government organizations.

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?

- Discovering and proving vulnerabilities through penetration testing; unfortunately, no universally-recognized standards exist for this activity.
- Using cyber security appliances (CSAs) to increase security on operational devices.
- Companies like Cisco are developing Security Information and Event Managers (SIEMs) to support Bring Your Own Device (BYOD) policies for employees.
- Companies like IBM have created powerful SIEMs like QRadar to monitor the network flow.
- Consulting firms actively search for vulnerabilities in technologies to help improve cyber security practices for industry.

- Numerous conferences and specialized work groups (e.g., SGIP) focus on specific sectors of network infrastructure. They convene and release critical knowledge that ISOs can use for their benefit.
- Security firms specializing in OT and other areas go beyond the traditional enterprise or financial IT perspective.
- A select few educational and training companies actively disseminate cyber security information to enterprises.

2. Which of these approaches apply across sectors?
- Common approaches across sectors include recognition and use of government standards and industry compliance mechanisms; auditing and security firms verify compliance.
- Many companies and industries across all sectors attend conferences to be better informed and up to date in cyber security.
- Penetration testing and SIEMs can be applied across most sectors, although the utility sector has been particularly reluctant to employ penetration testing.

3. Which organizations use these approaches?
- Utilities, military, factories, healthcare, financial and educational institutions, as well as others—generally, organizations truly concerned about risk (particularly cyber risk) employs some combination of the aforementioned approaches.

4. What, if any, are the limitations of using such approaches?
- The biggest limitation is that enterprises cannot depend solely on standards and compliance when cyber threats are dynamic and evolve based on human behavior. The installation of antivirus and firewall solutions doesn't save an institution from social engineering, phising scams, or an infected USB drive that could compromise an entire organization.
- The introduction of highly sophisticated mobile devices into an intranet can potentially compromise the whole information technology infrastructure with man in the middle attacks or hijacking. New mobile technologies can be also potentially compromised through Near Field Communications (NFC) attacks.
- Still-evolving cloud technologies are becoming more complex and more complicated to secure, even in the absence of standards to address many aspects of the cloud
- Penetration testing is not generally standardized and is constantly evolving.

5. What, if any, modifications could make these approaches more useful?
- Improve standards and complement them with dynamic security technologies.
- Better understand the need to constantly verify and improve security methods and technologies.
- Educate the public on cyber security, with the goal of developing a true cyber culture with ethics and values.
- Expand cyber security education modules to early stages of education.
- Identify the strong functional and inter-related relationship between IT and OT.

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

- Standards are typically very general; while some can be used in different sectors, sector-specific needs must be better identified. Each sector must be studied by working groups composed of members from a variety of sectors, as well as ethical hackers to help identify needs.

7. When using an existing framework, should there be a related sector-specific standards development process or voluntary program?
- We would recommend sector-specific standards development processes, with collaboration from voluntary entities. Many security firms and ethical hackers already perform voluntary work to demonstrate vulnerabilities to different sectors. However, the output of these firms may be seen as a threat instead of a benefit.

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 sectors must share information through proper secure channels. The real dynamic discoveries on cyber security are typically performed by the private sector; however, this information is often not shared until after an attack has been executed. The question is one of privacy and intellectual property versus security.

9. What other outreach efforts would be helpful?
- All the different sectors should convene and meet regularly to determine and address the proper questions and answers that affect the cyber infrastructure, which continues to further evolve into a system of systems solution that requires ethics, values, technology and common sense.
- Education is also a key item for cyber security. More awareness and responsibility must be given to this topic.

Specific Industry Practices

In addition to the approaches above, NIST is interested in identifying core practices that are broadly applicable across sectors and throughout industry.

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;
• Spectrum awareness policies and procedures to identify wireless threats and attacks;
• Mission/system resiliency practices;
• Security engineering practices;
• Privacy and civil liberties protection.

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

- Not in their entirety. The lack of information exchange and compliance mechanisms prevents the faster adoption of such concepts in industry.

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

- Regulations differ from country to country according to their ethics and cultural backgrounds, making it a challenge to develop a consistent set and application of common practices.

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

- Our organization believes that all of the practices are critical to ensure proper cyber-security protection.
- Separation of business from operational systems: this is one of the newer approaches; the most sophisticated malware has been found trying to compromise OT systems. Extensive public discussion started with Stuxnet, and is now being further publicized with Gauss and other attacks. System separation is highly critical.
- Use of encryption and key management: this is the most traditional approach but one which is also constantly challenged through parallel computing (GPU-CUDA) hash cracking (e.g. Cryptohaze) and newly discovered attacks on vulnerabilities in old encryption technologies (e.g., SSL decrypt authentication cookies). Cryptographers and mathematicians have to constantly be on alert for old techniques being cracked.
- Identification and authorization of users accessing systems: “man in the middle” and “hijacking attacks” are becoming more sophisticated and creative using mobile devices. These issues are similar to previous issues but with a new approach and different Trojan horses.
- Asset identification and management: this means compliance and standards for many sectors. However, critical assets definition must be modified. New capabilities and exploits are now causing creation and/or reclassification of new critical assets (i.e. SCADA systems were thought to be secure until IP ports and new technologies started appearing in the picture).
- Monitoring and incident detection tools and capabilities: monitoring and incident response are classified under the compliance umbrella. These tools and capabilities are slowly evolving with the understanding that threats are constantly changing. Fortunately, companies like Cisco, IBM, and others are evolving with new systems that seek to address new concerns.
- Incident handling policies and procedures: compliance and policies work fine until new technologies are introduced. Smart Grids are redefining and creating the needs for new policies.
- Mission/system resiliency practices: many successful resilience practices were defined by the military and have now been adopted and adapted by other sectors. However, every sector has its own definitions of what is critical; resilience practices depend on the criticality of the assets.

- Security engineering practices: Unfortunately, no clear standard exists; most practices are both industry-specific and proprietary.
- Privacy and civil liberties protection: This is a very sensitive area because you need to leverage security vs. privacy. In order to secure the operational technology, some privacy has to be given up. However, there must be a legal process in placed to ensure that the yielded privacy is legally protected from being misused.

4. Are some of these practices not applicable for business or mission needs within particular sectors?
- These practices work in every sector, but must be adapted and customized based on each sector's priorities and needs.

5. Which of these practices pose the most significant implementation challenge?
- All of them represent a challenge—as well as an opportunity. However, the priorities and needs of each sector are dependent on sector-specific criticality factors.

6. How are standards or guidelines utilized by organizations in the implementation of these practices?
- Most sectors have a range of compliance requirements, but these requirements typically don't improve until they get compromised, or are obligated by compliance or government institutions to abide to new norms.

7. Do organizations have a methodology in place for the proper allocation of business resources to invest in, create, and maintain IT standards?
- IT methodologies have been developed and applied based on many years of practice. However, these methodologies must rapidly evolve based on the introduction of new technologies: the cloud, mobile devices, Smart Grid, air gaps and IP touch points on Industrial Control Systems (ICS), among many others. The Internet constantly creates the need for IT to look outside their area of expertise and start talking to workgroups, academic institutions, research labs, specialized security firms and other entities to define new standards.

8. Do organizations have a formal escalation process to address cyber security risks that suddenly increase in severity?
- Most organizations have formal escalation processes, including covering those cases where severity suddenly increases. However, the lack of well-defined vulnerability assessment methodologies, and adherence to well-defined risk management frameworks, means that the vast majority of organizations are ill-equipped to respond to these sudden severity increases. Our own organization is creating methods to address security risks levels with the VARM process.
- Some organizations have escalation processes in place with restricted disclosure; the challenge being that restricted disclosure means less information sharing, which means less opportunity for beneficial collaboration.

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

- Personal privacy may be jeopardized to ensure the security of the masses; however, careful consideration must be given whenever personal liberty is affected.

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

- While the Framework does not necessarily apply to our organization at this moment, a well-defined Framework will incorporate a focus on cyber security training and education, which our organization looks to play a key role in developing and delivering. Since the University of Texas at El Paso has both the highest percentage and number of bilingual students of any university in the United States, we expect to make a significant impact on both the United States and all other countries throughout the Americas, particularly Spanish-speaking countries.

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

- Increasing security while mitigating risks to privacy and civil liberties is, and will continue to be, an ongoing challenge. For example, to avoid email account compromise, a network security operator must monitor traffic, which could enable the operator to discover personal information about the parties in the e-mail conversation. The tradeoff is how much information should be allowed to be monitored and blocked without making the user self conscious or uncomfortable. This is a deep concept that needs further understanding and development.
- Further collaborative research support on policy and security technology support for such risks.

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

- Implementation of Cyber Security Appliances that specialize on OT technology.
- Policies that assist education to develop curious minds on penetration testing techniques with a positive focus (ethical hacking, etc), instead of penalization and demonization of those activities.