On Developing a National Critical Infrastructure Cybersecurity Framework

April 8, 2013

John M. Willis, President
pINFOSEC, Inc.
CISSP, ECSA, NSA-IEM, NSA-IAM
CEH, Security+, Linux+, CITRMS
CIPP/US, CIPP/G, CIPP/IT
2020 Pennsylvania Ave NW #400
Washington DC 20006
John.Willis@pINFOSEC.com
LinkedIn.com/in/johnmwillis
(202) 670-7179

Section 1 – Current Risk Management Practices

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

- Budgets not keeping pace with change.
- Effective asset identification and management processes.
- Convincing the organization to adopt software whitelisting on the desktop.
- Keeping up with security patch management.
- Lack of available technical security configuration checklists. Need better commercial adoption of SCAP.
- Implementing behavioral and anomalous activity detection accurately.
- Ever-changing communications and encryption vulnerabilities being discovered.
- Federal mandates that are too burdensome and costly to implement.
- Creating a framework that will withstand technological change, while at the same time providing people, process, and technical controls that are actionable, whose implementation is readily measurable.
- Reconciling NIST and ISO processes and procedures.
- Lack of security engineering common Body of Knowledge.
- Implementing identification credential appropriate to the Level of Assurance for public users, while being sensitive to the National ID card debate and privacy concerns. Especially for financial transactions, while permitting anonymous transactions that do not harm anyone.

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

- Balancing the need to have a single common framework while addressing sector-specific uniquenesses.

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?

- Financial sector generally uses processes and controls developed under ISO 27001.

4. Where do organizations locate their cybersecurity risk management program/office?
- No response provided.

5. How do organizations define and assess risk generally and cybersecurity risk specifically?
- Financial sector looks to DISA STIGs, NSA, and Center for Internet Security for security configuration guidance. More recently, SCAP XCCDF files are available for consideration; however, the financial sector has yet to embrace them.

6. To what extent is cybersecurity risk incorporated into organizations' overarching enterprise risk management?
- Generally, most organizations are not very effective at this, as is evidenced by a defensive posture as opposed to an aggressive Strategic Plan that is focused on business processes in support of security architecture and engineering to prevent security breaches in the first place. This is largely due to the approach of merely buying a technical solution to solve the problem and expending as little as possible to address the problem. In all fairness, at least a number of larger organizations have begun to make an impact on in-house development application security.

7. What standards, guidelines, best practices, and tools are organizations using to understand, measure, and manage risk at the management, operational, and technical levels?
- ISO/IEC 27001
- NIST SP 800 series of special publications
- The SCAP suite, including MAEC, CyBOX, STIX, TAXI, etc.
- News and data feeds
- Open source security tools
- DISA STIGs, NSA, and Center for Internet Security for technical security configuration checklists, and now, SCAP (commercial sector needs better adoption of SCAP)

8. What are the current regulatory and regulatory reporting requirements in the U.S. for organizations relating to cybersecurity?
- States have varying requirements pertaining to data protection and breach notification.
- Varying requirements cause a myriad of issues.
- When it comes to sharing information, various bits of information must be kept confidential. Each source of such data implements its own reporting requirements. This should be standardized.

9. What organizational critical assets are interdependent upon other critical physical and information infrastructures, including telecommunications, energy, financial services, water, and transportation sectors?
- There is an overabundance of interconnectedness—to the extent that it is a real issue. A failure in one critical infrastructure service can cause failure in another critical infrastructure service.

To this extent the critical infrastructure of this country is rather fragile. There is a potential for "butterfly" effects that would result in significant injury in ways not imagined.
- All systems must be safety engineered in a manner so as to fail in a safe mode.
- Failover features must exist and not cause additional failures during the failover process.

10. What performance goals do organizations adopt to ensure their ability to provide essential services while managing cybersecurity risk?
- Not all organizations have an effective program in place to routinely test the effectiveness of their physical and technical security.
- Not all organizations engage in disaster recovery planning and exercises.
- Mandates and incentives should be considered to facilitate corrective action in the above areas. And not just for critical infrastructure sectors.

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?
- No response provided.

12. What role(s) do or should national/international standards and organizations that develop national/international standards play in critical infrastructure cybersecurity conformity assessment?
- Conformity assessment should be performed by US-based entities.
- It is certainly reasonable for the US to adopt an international standard.

Section 2 – Use of Frameworks, Standards, Guidelines, and Best Practices

1. What additional approaches already exist?
- There are numerous approaches. ISO 27001 is most comprehensive. Proper application of ISO 27001 should ensure conformance to others.
- NIST SP 800-53 and the 20 Critical Security Controls, plus technical security configuration checklists

2. Which of these approaches apply across sectors?
- ISO 27001 and NIST

3. Which organizations use these approaches?
- Generally, regulated industries and government.

4. What, if any, are the limitations of using such approaches?
- Most are limited due to sector focus. ISO 27001 is considered to be an umbrella standard.
- Each framework has to be customized for each enterprise's business model, technology environment, etc.
- They don't address social engineering issues.

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

On Developing a National Critical Infrastructure Cybersecurity Framework

- ISO 27001 should be used as a starting point for a new document or modification.
- Ensure sector-specific concerns are incorporated.
- Ensure alignment with NIST Risk Management Framework.
- Incorporate the 20 Critical Security Controls.
- Generate actionable business and IT standards and controls. Utilize NIST SP 800-53 and SP 800-53A, and NIST Checklists (SCAP, STIGs, NSA, etc.).
- Make them detailed enough so that it is possible to identify and collect metrics appropriate to document conformance to the controls.
- Information that is sector-specific goes into an appendix.
- Sample process and procedure examples may be helpful to compensate for tendency to just buy a solution and try to do as little work as possible.
- NIST should designate a certifying entity, who should test the implementation of processes and controls.
- Continue efforts with the IETF SACM, eventually solidifying situational awareness capabilities.

6. How do these approaches take into account sector-specific needs?
- Some have sector-specific standards. Others tailor something like ISO 27001.

7. When using an existing framework, should there be a related sector-specific standards development process or voluntary program?
- A sector-specific development process is needed to cover the unique aspects of each sector.
- Sectors, regulators, and security experts should be engaged in the framework and standards development process, and adherence to should be mandated by law.
- Each sector has its own specific risks, issues and concerns.
- Common language should be in the main set of documentation. Sector-specific information should be an appendix/annex to that documentation.
- Phase-in mandated changes to minimize impact to organizations, and resulting economic adjustments.
- Organizational change is already hard, and is even harder when trying to implement voluntarily.

8. What can the role of sector-specific agencies and related sector coordinating councils be in developing and promoting the use of these approaches?
- Serve as responsible entity driving standards development as well as the overall compliance and enforcement responsibility through designated entities.
- Facilitate information sharing.

9. What other outreach efforts would be helpful?
- Regular meetings of the common body, as well as specific sectors, as part of a continuous improvement methodology for the Nation.
- Increased education and cybersecurity exercises specifically covering critical infrastructure attacks, countermeasures, kinetic effects, economic effects, terrorism, organized cybercrime and collateral damage.
- Initiate efforts to focus on creating Cyber Strategic Plans in order to gain control of the

situations and significantly decrease the level of reactive efforts. Focus on goals and objectives to turn the situation around. The perfect storm we have now is like a company that is going under. Turnaround management techniques need to be applied. Focus industry on security research engineering of proactive solutions. Engage vendors, companies and agencies in this cooperative program. Make funding of novel research easier. Peel back the onion. Focus on each part of the puzzle.

- Increase public education, workshops and assistance in planning and preparing for critical infrastructure outages. This will serve to reduce the likelihood of cascading failures across sectors.

Section 3 – Specific Industry Practices

1. Are these practices widely used throughout critical infrastructure and industry?
   - The state of asset management is abysmal.
   - Log analysis, if performed, is getting more challenging by the moment.
   - Identification, authentication and authorization have many issues with being implemented properly.
   - Adoption of Systems Security Engineering Capability Maturity Model (SSE-CMM) has been too slow.

2. How do these practices relate to existing international standards and practices?
   - ISO 27001 is the principally relevant international standard of practice.

3. Which of these practices do commenters see as being the most critical for the secure operation of critical infrastructure?
   - Security Engineering
   - Separation of business from operational systems. Compliance and Standards setting group must be separate from operations group, and separate from application development group. Each of these groups should have extensive expertise in security engineering.
   - Air gap control systems based on potential degree of direct kinetic injury. There should be no digital or electrical control path from business network to such control systems.
   - Market adoption of quantum encryption technologies.
   - Proper security of engineering identification, authentication and authorization for critical infrastructure networks and systems.
   - Improving the current state of asset identification and management.
   - Implementation of anomaly, behavioral and syntactical inspection algorithms in network, operating system and application environments.
   - Security engineering practices. No clear standard exists. Most practices are both industry-specific and proprietary.
   - Proper planning. Realistic procedures that are actually followed.
   - Mandates and incentives should be considered to facilitate corrective action in the above areas. And not just for critical infrastructure sectors.
4. Are some of these practices not applicable for business or mission needs within particular sectors?

- No response provided

5. Which of these practices pose the most significant implementation challenge?
    - Proper security engineering discipline, and publicly available common Body of Knowledge.
    - Getting everyone focused on re-engineering to prevent security incidents.

6. How are standards or guidelines utilized by organizations in the implementation of these practices?
    - Frameworks provide the flexibility to be creative in tailoring to the environment so that the level of effort and expense to comply may be minimized or eliminated.
    - Because there are so many frameworks to choose from, and there being no standardized actionable standards mandated, there is virtually no way to ensure a repeatable, sustainable and measurable implementation of security controls.
    - Implementation generally does not progress well until there is a compromise of data, or there is a regulatory mandate that has a data reporting requirement.
    - Some organizations have policies, standards and procedures addressing some or all of these areas. Their degree of completeness and utilization varies widely.

7. Do organizations have a methodology in place for the proper allocation of business resources to invest in, create and maintain IT standards?
    - This depends on the maturity of the organization. If the organization does not routinely incorporate maturity models and continuous improvement into its operational processes, then it should do so.

8. Do organizations have a formal escalation process to address cybersecurity risks that suddenly increase in severity?
    - Even where such a process exists, there is detail lacking for the technical response on the network side. Regarding access to applications and data, most organizations lack the ability to automate the deauthorization process, not to mention the lack of dynamic attribute based access control.
    - Organizations that do not actively follow a functional set of security processes are going to have issues responding and escalating effectively.

9. What risks to privacy and civil liberties do commenters perceive in the application of these practices?
    - Risk of disclosure of personal information. Ownership of this information is often unclear. The individual lacks capability to update appropriate information and trigger update to downstream systems. Systems lack the ability to inform the individual of all downstream disclosures. Personal information should be locked and encrypted by the individual, and accessible only for permitted uses. The individual should be able to inspect all downstream disclosures and uses. All downstream users of the data also have a liability stake in tracking downstream disclosures and uses.
    - Due to the swiss cheese nature of the current state of cyber security there is already a plethora of personal data available. This does not mean we should throw up our hands. While those currently alive are potentially exposed to financial, political and other risks, a lot of work still

needs to be completed to stop the hemorrhaging. We should at least fix the problem for the generations yet to be born. Also look to Congressional, regulatory and judicial activity for specific areas to focus on.

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

- No response provided.

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

- With great care.
- See response to question 9, above.
- Refer to the Cascading Disclosure Control Language (CDCL) and the National Information Exchange Model (NIEM) Information Exchange Package Documentation (IEPD) Lifecycle for ideas on how to implement a downstream disclosure architecture.
- Also consider individual encryption of XACML objects that are passed along to downstream systems.

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

- Treat the desktop browser as a principal attack vector to the user's machine.
- Information sharing should have various levels, including public.
- If allowing remote access to a critical infrastructure environment, only allow access from systems controlled by the organization.
- Critical infrastructure operational environments with potential for major kinetic injury or economic damage should be classified as National Security Systems. Criteria for making this determination should be clearly defined.
- Penetration testing and ethical hacking should be openly taught and encouraged. If you outlaw hacking tools, only unethical hackers will have hacking tools. Don't constrain the free flow of security research information—even from part-time hobbyists working in their garage.
- Physically isolated, air-gapped networks, with stringent personnel and access controls may not need to encrypt network traffic on the critical infrastructure operational network—but encryption of all other critical infrastructure networks should be mandated. The exception process must be risk-based and well documented.
- Specific guidance on what is acceptable as a countermeasure, or retaliatory cyber strike, incident response. If someone just came into your yard, jumped on your bicycle and started riding off, is it okay to chase after them and stop them on the road? On private property? What are the rules?
- Mandates and incentives should be considered to facilitate corrective action in the above areas. There should be hefty penalties and consequences for non-conformance. And not just for critical infrastructure sectors.