Table of Contents

1.0 CURRENT RISK MANAGEMENT PRACTICES

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

Although improved critical infrastructure cybersecurity practices are vital to our national security, many companies have not considered this risk as part of their risk management process. The tendency for some companies is to believe, this risk is acceptable, and the business case does not justify the cost for investment (or there are higher priorities for their investment). However, some companies only support doing the bare minimum required by regulations that does not always meet the full compliance of a risk management program, which can lead to insecure portions of the critical infrastructure. A lack of comprehension of the risk management process at lower levels of the organization and the resistance of senior management acceptance of the process will lead to critical infrastructure being compromised. These shortfalls in the cybersecurity improvement process can be overcome by engaging subject matter expert (SME) that embraces a clearly defined risk methodology. The SME must actively support the Companies with the risk management process from inception to completion and provide training for various levels of the organization.

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

Many have the belief, standards will increase cost to their business case. While standards are a critical part of the security, they do not always provide coverage for specialized areas of critical infrastructure to make them secure. Most standards leverage previous works and they are written to broadly and leave gaps for interpretation, which are fundamental weaknesses. Primarily the standards development process is very slow tedious for the generation and approval of new standards that becomes outdated during implementing. Thus, the vulnerabilities and there exploitation outpace the remediation provided by the standards. The second major weakness is the fundamental nature of a standard where many players cannot reach consensus on any change or additions. This behavior leads to the best solutions not implemented or terminology added that allows someone to bypass critical features. When attacking any system, the easiest way to find the primary weakness is reading the standard often, it easily identifies where the primary weakness exist. Becoming leaders in the standards effort is important to bring experience in cybersecurity improvement and influencing the best practices.

1.3 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 Risk Management (RISK) domain comprises three objectives:

1) Establish Cybersecurity Risk Management Strategy
2) Manage Cybersecurity Risk
3) Manage RISK Activities (common objective).

EnerNex provides a cybersecurity risk management strategy that is a high-level strategy, which provides direction for analyzing and prioritizing cybersecurity risk and defines risk tolerance. The cybersecurity risk management strategy includes a risk assessment methodology, risk monitoring strategy, and cybersecurity governance program; this then feeds into a low-level testing process to check the high-level work for gaps. This includes defining the enterprise risk criteria (e.g. impact thresholds, risk response approaches) that guides the cybersecurity program. The cybersecurity risk management strategy should always align with the enterprise risk management strategy to ensure that cybersecurity risk is managed in a manner that is consistent with the organization's mission and business objectives. Senior management uses a top-down approach instituted through the cybersecurity governance program.

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

This depends on the organization's structure; the most important would be to have a Risk Management Organization with subgroups, such as Governance, Auditing, and possibly IT. However, to integrate the risk management process throughout the organization, a three-tiered approach should be established that addresses risk at the organization level, mission/business process level, and information system level. Lastly, an organization may choose to outsource their risk management program to a qualified third-party that actively participates in standards groups and has significant experience developing programs.

1.5 How do organizations define and assess risk generally and cybersecurity risk specifically?

Utilities that do not fall under NERC-CIP requirements have not been required to pay attention to cyber security risk specifically. This is a fundamental change for the electric utility industry that typically defines risk, as a danger to the grid, power delivery, itself. This mindset is often times fundamentally at odds with cyber security or risk mitigation programs. The current mindset is to keep the grid operational at all costs. This could mean not using any encryption or security whatsoever and where security has been implemented they diligently maintain the default passwords to eliminate all possibilities that a technician might not be allowed access because they do not have the proper password.

A standard way of define risk is through the use of a risk equation,

- Risk = Vulnerability X Likelihood X Impact

Where

- Vulnerability -- is a weakness in an asset
- Likelihood – is the probability of the vulnerability being exploited
- Impact – is the consequence to the infrastructure from the exploitation of the asset

Risk can assessed through a process that develops a methodology and provides a framework to address rick throughout a "risk management lifecycle." It inform decision makers and reinforce risk responses by identifying relevant threats to organizations; identifies vulnerabilities both internal and external to organizations; and impact to organizations that may occur given the potential for threats exploiting vulnerabilities; and defines the likelihood that harm will occur.

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

It should be applied at all three tiers within the risk management hierarchy—organization level, mission/business process level, and information system level.

a. Tier 1—organization-wide information security programs, policies, procedures, and guidance
b. Tier 2—enterprise architecture/security architecture design decisions; the selection of common controls; selection of suppliers, services, and contractors support for missions/business functions.
c. Tier 3—design decisions; tailoring, and supplementation of security controls; selection of information technology products; product configurations meet security control requirements; and operational decisions that includes level of monitoring activity

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

Standards include NIST 800-30, NIST 800-37, NIST 800-39, NIST 800-53, NISTIR 7628, NERC CIP (2-9), FIPS 199, and FIPS 200.

Tools include NESCOR Failure Scenarios, DOE ES-C2M2, DHS CSET, etc. While the standards and tools provide some degree of guidance, it takes significant experience to apply them to an organization's mission without impeding their vision and purpose. Being involved in, or working with SMEs who are involved in, these groups can provide the necessary level of experience.

1.8 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?

- NERC and NERC-CIP
- PCI
- SOX
- GLBA
- US-CERT
- ICS-CERT

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

In the electric utility industry, it is an interwoven web of many technologies. Generation facilities often have requirements for water. Peak load generators often have a dependency on natural gas pipelines while others may be dependent on transportation to supply fuel oil. Substations often have dependencies on telecommunications networks for SCADA communications.

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

The electric utility industry tries to maintain one-hundred percent uptime. Cyber security is only now starting to creep in to is space as networks and systems become more interconnected. Engaging cyber-security experts that understand risk management, business process analysis, and low-level technical testing are key components to providing the necessary services securely.

1.11 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?

Most utilities report to the public utility commissions in their service territories. For larger utilities they may have to report to several along with government requirements because of their inclusion into NERC-CIP requirements because the size of the load that they manage. For small organizations reporting to multiple agencies could be very cost prohibitive.

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

Why we think it will be critical for the formation of guidelines and best practices in for creating uniformity between different countries allowing for manufacturers and customers to benefit from economies of scale. We do not feel that these organizations are significantly nimble enough to handle the day-to-day requirements that cyber security currently dictates. Should the change management process and ability to update in accordance with rapidly changing threat and attach vectors, these organizations may be able to provide some sort of guidance in the conformance space.

2.0 USE OF FRAMEWORKS, STANDARDS, GUIDELINES, AND BEST PRACTICES

2.1 What additional approaches already exist?

There are multiple approaches to risk management which have been developed in response to an incident or by private organizations. Many are hard to understand except by the people who created them as they were not part of a formal process.

2.2 Which of these approaches apply across sectors?

Thus far, the IT-centric and the financial model approaches to risk management tend to span sectors most easily because of the requirement for some sort of network connectivity between devices and functionality. Both approaches also seek to serve the end goal of providing communications, or the ability to facilitate a financial transaction to completion.

2.3 Which organizations use these approaches?

Most organizations have a concept of IT risk management and the banking industry has done an excellent job in furthering PCI DSS 2.0 into the financial world. The PCI framework allows for the accrediting of third-party auditors and entities giving end clients the ability to choose from several providers as they attempt to manage their financial risk.

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

In many cases they're quite complex and extremely confusing requiring large inputs of time from a very diverse group of stakeholders which makes them extremely expensive to integrate into their existing policies, procedures and processes. The availability of the subject matter experts is extremely limited and it can be difficult to ascertain the quality of the auditor or organization assisting with risk management.

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

Workforce education and training initiatives must progress so that there non-security personnel can understand and select qualified assessors and auditors. The current reliance on test-based certifications produces too wide a range of ability to accurately determine actual competency.

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

Some efforts such as ASAP – SG were designed specifically for the electric utility industry other efforts such as the SGIP were also targeted specifically at utility industry. More often best practices are pulled from the IT sectors and applied where appropriate. Finding personnel with the correct experience in critical infrastructure operations and engineering combined with deep technical cyber security is key to building a successful approach.

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

In the some critical infrastructure industries, these efforts already exist. These efforts can be ineffective because of the fundamental practices in standards developments whereas the best solution to a specific problem rarely make it into the standards. While standards may provide a base framework to secure critical infrastructure, the possibility exists to always be outpaced by your adversaries who are not impeded by any such requirements for compliance or cooperation. In order to succeed, smaller tactical groups must be created utilizing the correct combination of personnel in order to keep pace with potential attackers. Examples of these smaller groups include NESCOR, ASAP-SG, and NESCO.

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

These organizations can be valuable in educating their communities about the real issues in which they are facing. Additionally, they can give real-world advice on how to mitigate the challenges that they will be faced with regardless of the current state of any regulation or standard. Unfortunately many organizations are currently only concerned with compliance metrics and do not focus on large-scale risk management. A sector-specific agency could provide education and training that displays how the implementation of a robust cyber security and risk management program would provide best practices security which would exceed the compliance metrics put forth by regulatory entities.

2.9 What other outreach efforts would be helpful?

A neutral third-party expert being involved in the testing and development of standards and groups is critical as this industry moves forward. The frameworks, standards, and guidelines developed must be flexible yet applicable to any size of organization. The utilization of a neutral third-party can be instrumental to ensure that what is developed is scalable for large and small organizations without being overbearing or light on actionable material. Examples of this would include third-party testing labs, public private collaborative groups that adequately represent the infrastructure sector, and involving vendors with independent third-party experts during the development of new hardware, software, and firmware.

3.0 SPECIFIC INDUSTRY PRACTICES

3.1 Are these practices widely used throughout critical infrastructure and industry?

No, the electric utility industry has seldom used best practices because they power delivery systems have not historically been interconnected with IT communications systems. The exception to this would be some of the newest infrastructure systems that have utilized newer efforts such as NESCOR Failure Scenarios, DOE ES-C2M2, and DHS CSET. Public utility commissions are starting to provide pressure on some issues however education and partnership may prove to be more beneficial than increased regulation. In equipment that has the ability to operate in a secure fashion, the security mechanisms disabled or completely turned off leaving the end-user to understand, configure, implement, and maintain.

3.2 How do these practices relate to existing international standards and practices?

In general newer standards have had some international involvement and would be aligned. More work still needs to take place to ensure national needs are being met for the unique environments provided by privately owned critical infrastructure. In some international areas, the government owns the infrastructure and their standards may not be applicable in the US.

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

The education of the workforce from the end-user to the technical expert in security must constantly evolve and adapt to the rapid changes in these environments. This effort begins with better training of the security personnel and then the follow-on training of end users to show the how and why of security. Of equal importance is the empowerment and enforcement of security practices being implemented.

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

Good security practices should always align with the business mission and the ability to discern what supports the mission and what interferes must be handled carefully. Collaborative groups with independent third-parties, asset owners, and vendors should work cooperatively to establish best practices that are flexible yet authoritative.

3.5 Which of these practices pose the most significant implementation challenge?

We feel the key management and encryption will be the most difficult to implement especially as these networks penetrate further into the field and into the customer's locations in homes. Many of these devices that are being placed on premise must be cost-effective in performing the desired functionality and do not contain the additional capabilities to implement some features in regards to key management and encryption.

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

Best practices are observed in some entities and others focus solely on compliance.

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

In larger organizations this is true, but in the vast majority of smaller enterprises within the United States it is not. The vast majority of companies do not have any dedicated IT staff to begin with much less ones that can dedicate a significant part of their time to security-related issues. A paradigm shift form profitability to resiliency or sustainability will help with budgeting future efforts.

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

Incident response is often an under-developed process if it exists at all. The ability to escalate would be defendant on this process existing.

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

There may be a perception of a loss of privacy by consumers however independent third-party research should be performed to alleviate these fears. Engaging a third-party provider and making some testing results and plans public can assist in putting some fear to rest. The smaller cooperative utility companies are very good at this.

3.10 What are the international implications of this Framework on your global business or in

policymaking in other countries?

Having companies within the United States being secure and implementing best practices is critical for this to occur for us to maintain our position in good standing within the international community. The United States must maintain its position as a global leader in security and financial prosperity.

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

They should be managed with extreme prejudice these are critical to what we stand for and is one of the core premises to the American way of life. It is also the cornerstone of commerce and without customer confidence our economy will suffer severely. The whole of our economy is based on trust from the purchase of a widget on the Internet to the stock market. Customers have to be able to trust the information they get to company stays safe and secure.

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

It will take a very dedicated effort in education to make these core concepts understandable and actionable to the people that will be required to implement them the education needs to teach these people the reasoning and logic behind these decisions and why it is important for each and every one of us to be secure in the things we do and the transactions we conduct on a daily basis.