Critical Infrastructure and Executive Order 13636

Understanding Impact and Implications

Eric Cosman, Vice President, Standards and Practices, ISA

John Lellis, Chief Technology Officer, Berkana Resources Corporation

Forward

This paper considers the historical evolution of cybersecurity standards, the actions proposed by EO 13636, the implications of the order on asset owners and operators and possible actions that may be indicated as a consequence.

Contents

Figures

1 Introduction

Executive Order 13636 is intended to strengthen the cybersecurity of critical infrastructure by increasing information sharing and by jointly developing and implementing a framework of cybersecurity practices with industry partners. It includes the following mandates:

- New information sharing programs to provide both classified and unclassified threat and attack information to U.S. companies – The Order expands the voluntary Enhanced Cybersecurity Services program, enabling near real time sharing of cyber threat information to assist participating critical infrastructure companies in their cyber protection efforts.
- The development of a Cybersecurity Framework – NIST will work collaboratively with critical infrastructure stakeholders to develop the framework relying on existing international standards, practices, and procedures that have proven to be effective.

The Executive Order also:

- Includes strong privacy and civil liberties protections. Agencies are required to incorporate privacy and civil liberties safeguards in their activities under this order. Those safeguards will be based upon the Fair Information Practice Principles (FIPPS) and other applicable privacy and civil liberties policies, principles, and frameworks. Agencies will conduct regular assessments of privacy and civil liberties impacts of their activities and such assessments will be made public.
- Establishes a voluntary program to promote the adoption of the Cybersecurity Framework. The Department of Homeland Security will work with Sector-Specific Agencies (e.g., Department of Energy) and the Sector Coordinating Councils that represent industry to develop a program to assist companies with implementing the Cybersecurity Framework and to identify incentives for adoption.
- Calls for a review of existing cybersecurity regulation. Regulatory agencies will use the Cybersecurity Framework to assess their cybersecurity regulations, determine if existing requirements are sufficient, and whether any existing regulations can be eliminated as no longer effective. If the existing regulations are ineffective or insufficient, agencies will propose new, cost-effective regulations based upon the Cybersecurity Framework and in consultation with their regulated companies. Independent regulatory agencies are encouraged to leverage the Cybersecurity Framework to consider prioritized actions to mitigate cyber risks for critical infrastructure consistent with their authorities.

2 Why we need an Executive Order

Protecting the nation's critical infrastructure has been a national priority for many years, with emphasis increasing since 2001. Efforts have been concentrated on both physical and cyber threats, but the cyber arena has been the subject of considerably more public attention. Unfortunately, the results of these efforts have not been uniformly effective and efforts to pass appropriate cybersecurity related legislation have been unsuccessful. The Administration seeks to motivate owners and operators of critical infrastructure assets to make the effort to mitigate the cyber risks their holdings face.

There have been numerous efforts in the past to define the appropriate steps that need to be taken to secure national and corporate resources from cyber attack. While the following examples do not comprise a definitive list, they serve to illustrate the time and effort that has already gone into making information systems secure as well as provide a useful list of references.

2.1 BS 7799 (1995)

BS 7799, *Guidelines for Information Security Risk Management*[1], was originally published by BSI Group (BSI) in 1995. Written by the United Kingdom Government's Department of Trade and Industry (DTI), it consisted of three parts: best practices for Information Security Management (later revised in 1998), how to implement an Information Security Management system and finally, risk analysis and management. It aligns with ISO/IEC 27001.

2.2 NIST 800-12 (1995)

NIST Special Publication 800-12, *An Introduction to Computer Security*[2], is a handbook written in October of 1995 that covers the basics of computer security and how to secure computer-based resources (including hardware, software, and information). It illustrates the benefits of security controls, the techniques involved, and important related considerations (such as cost) but does not describe the detailed steps necessary to implement a computer security program.

2.3 COBIT (1996)

COBIT, *Control Objectives for Information and Related Technology*[3], is a framework created by The Information Systems Audit and Control Association (ISACA) to manage information technology (IT) control requirements, technical issues and business risks. The current version, COBIT 5, was updated in 2012.

COBIT defines a set of generic processes for the management of IT. The framework defines each process together with its inputs and outputs, key activities, objectives, business goals, IT goals, performance measurement and a simple maturity model.

---

[1] Visit http://www.bsigroup.com/en-GB/iso-27001-information-security for further discussion of the BS 7799 and BS/ISO/IEC 27001 standards.
[2] Visit http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf to download a copy of the NIST 800-12 document.
[3] Visit www.isaca.org/COBIT for a detailed discussion of the COBIT framework.

2.4 PDD-63 (1998)

Presidential Decision Directive 63[4] first defined the concept of "critical infrastructure" and declared it a national policy "that the United States will take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures, including especially our cyber systems."

That goal, of course, was not met but the bureaucracy it put in place is still central to the federal government's efforts towards securing the nation's critical infrastructure.

2.5 IEC 17799 (2000)

The British standard BS 7799 was adopted by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) as ISO/IEC 17799[5], later revised in 2005 and renumbered (but otherwise unchanged) in 2007 to align with the other ISO/IEC 27000-series standards. Its current incarnation, ISO/IEC 27002[6], is an information security standard entitled *Information Technology – Security Techniques – Code of Practice for Information Security Management*.

ISO/IEC 27002 defines information security in terms of the C-I-A triad, the preservation of

- **C**onfidentiality (ensuring that information is accessible only to those authorized to have access),
- **I**ntegrity (safeguarding the accuracy and completeness of information and processing methods) and
- **A**vailability (ensuring that authorized users have access to information and associated assets when required).

2.6 AGA-12 (2002)

After the 9/11 attacks the American Gas Association formed a working group to develop a standard to protect Supervisory Control and Data Acquisition (SCADA) systems from cyber attack. The resulting standard known as AGA 12[7] is a suite of four documents, each addressing a different aspect of SCADA communications:

- AGA 12-1 summarizes cyber security policies, the background of the cyber security problem, the need to do a risk assessment and a procedure for testing cryptographic protection systems.

[4] Visit http://www.fas.org/irp/offdocs/pdd/pdd-63.pdf to download a copy of the document.
[5] Visit http://webstore.iec.ch/Webstore/webstore.nsf/ArtNum_PK/41050!opendocument&preview=1 to purchase a copy of ISO/IEC 17799.
[6] Visit http://webstore.iec.ch/Webstore/webstore.nsf/ArtNum_PK/48666!opendocument&preview=1 to purchase a copy of ISO/IEC 27002.
[7] The AGA 12 standard may be found at http://www.scadahacker.com/library/Documents/Standards/AGA%20-%20Cryptographic%20Protection%20of%20SCADA%20Communications%20-%2012%20Part1.pdf.

- AGA 12-2 is a detailed technical specification for building cryptographic modules to protect SCADA communications for low-speed legacy SCADA systems and dial-up maintenance ports.
- AGA 12-3 describes how to protect high-speed communication SCADA systems.
- AGA 12-4 describes how to build next-generation SCADA systems so that their cryptography is compatible with legacy systems.

2.7 API-1164 (2002)

This standard is specific to supervisory control and data acquisition (SCADA) systems in the petroleum pipeline industry. API-1164[8] provides best practices to guide liquid pipeline operators on risk assessments, system design, establishment and review of company policies. It addresses access control, communication security, information distribution classification, physical issues (including disaster recovery and business continuity plans), operating systems, network design, data interchange between enterprise and third-party support/customers, management systems, field devices configuration and local access.

2.8 NERC CIP (2003)

The NERC CIP[9] (North American Electric Reliability Corporation Critical Infrastructure Protection) plan is a set of requirements designed to secure the assets required for operating North America's bulk electric system, comprising 9 standards and 45 requirements covering the security of electronic perimeters and the protection of critical cyber assets as well as personnel and training, security management and disaster recovery planning.

Under NERC CIP, covered entities are required to identify critical assets and to regularly perform a risk analysis of those assets. Organizations are required to enforce IT controls protecting access to critical cyber assets. Systems for monitoring security events must be deployed, and organizations must have comprehensive contingency plans for cyber attacks, natural disasters and other unplanned events.

Penalties for non-compliance can include fines, sanctions or other actions. Because NERC is a trans-national organization, the exact penalties vary from country to country.

2.9 IEC 27001 (2005)

ISO/IEC 27001[10] is an information security management system (ISMS) standard published in October 2005 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It formally specifies a management system that is intended to bring information security under explicit management control. The standard contains 11 domains:

- Security policy - management direction

[8] The API 1164 standard may be found at http://www.scribd.com/doc/150238922/API-STD-1164-2nd-Ed-2009-pdf.
[9] The complete *Reliability Standards for the Bulk Electric Systems of North America* can be downloaded from http://www.nerc.com/pa/Stand/Reliability%20Standards%20Complete%20Set/RSCompleteSet.pdf.
[10] The ISO/IEC 27001 standard may be found at http://web.bryant.edu/~commtech/guidelines/iso27001.pdf.

- Organization of information security - governance of information security
- Asset management - inventory and classification of information assets
- Human resources security - security aspects for employees joining, moving and leaving an organization
- Physical and environmental security - protection of the computer facilities
- Communications and operations management - management of technical security controls in systems and networks
- Access control - restriction of access rights to networks, systems, applications, functions and data
- Information systems acquisition, development and maintenance - building security into applications
- Information security incident management - anticipating and responding appropriately to information security breaches
- Business continuity management - protecting, maintaining and recovering business-critical processes and systems
- Compliance - ensuring conformance with information security policies, standards, laws and regulations

2.10 ISA-62443 (2007)

ISA-62443[11] is a series of standards, technical reports, and related information that define procedures for implementing electronically secure Industrial Automation and Control Systems (IACS). These standards are developed by the ISA99 committee of the International Society for Automation (ISA). This guidance applies to end-users (i.e., asset owners), system integrators, security practitioners, and control systems manufacturers responsible for manufacturing, designing, implementing, or managing industrial automation and control systems.

The standards and technical reports in the ISA-62443 series are organized into four general categories called General, Policies and Procedures, System and Component, as shown in the following figure:

[11] The documents originally referred to as ANSI/ISA-99 or ISA-99 standards, as they were created by the International Society for Automation (ISA) and publicly released as American National Standards Institute (ANSI) documents, were renumbered in 2010 to be the ANSI/ISA-62443 series. This change was intended to align the ISA and ANSI document numbering with the corresponding International Electrotechnical Commission (IEC) standards. Copies of the completed and working documents in this standard can be found at http://isa99.isa.org.

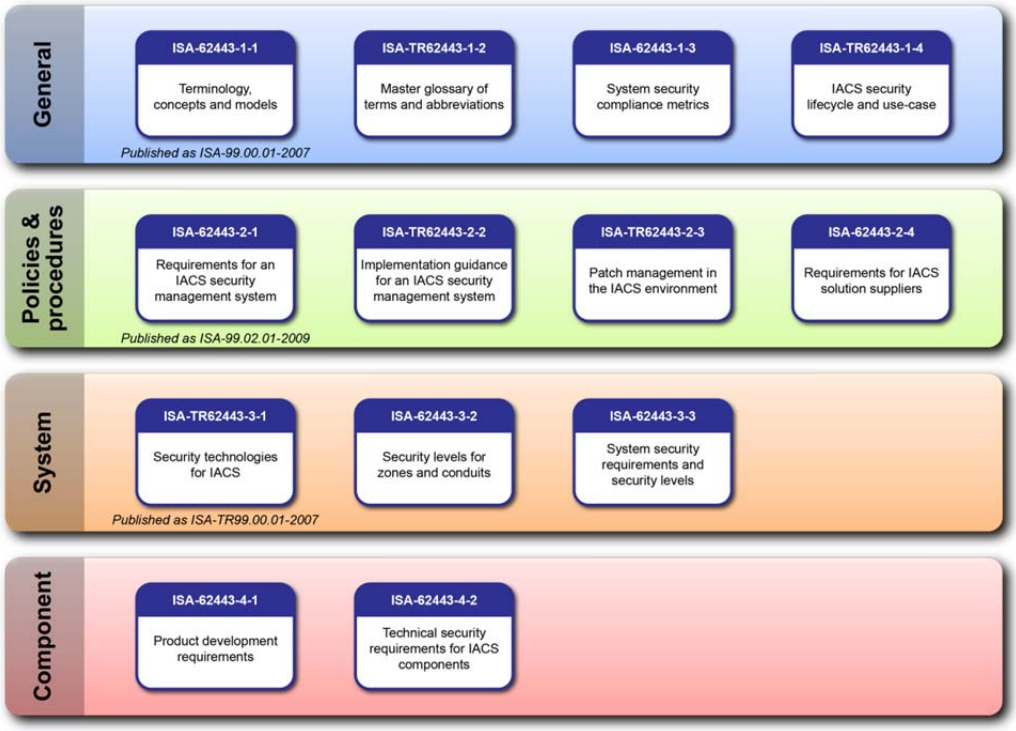

Figure 1 – The ISA-62443 Series

- The first (top) category includes common or foundational information such as concepts, models and terminology. Also included are work products that describe security metrics and security life cycles for IACS.
- The second category of work products targets the Asset Owner. These address various aspects of creating and maintaining an effective IACS security program.
- The third category includes work products that describe system design guidance and requirements for the secure integration of control systems. Core in this is the zone and conduit design model.
- The fourth category includes work products that describe the specific product development and technical requirements of control system products. This is primarily intended for control product vendors, but can be used by integrator and asset owners for to assist in the procurement of secure products.

2.11 Risk IT (2009)

Risk IT[12] was published in 2009 by the Information Systems Audit and Control Association (ISACA). The Risk IT framework provides an end-to-end, comprehensive view of all risks related to the use of IT and a similarly thorough treatment of risk management, from the tone and culture at the top, to operational issues and enables users to:

- Integrate the management of IT risk with the overall ERM

[12] Visit http://community.mis.temple.edu/mis5205spring2013/files/2013/02/RiskIT-FW-18Nov09-Research.pdf to view the Risk IT framework document.

- Compare assessed IT risk with risk appetite and risk tolerance of the organization
- Understand how to manage the risk

2.12 IEC 62443 (2012)

In 2010, the documents originally referred to as ANSI/ISA-99 or ISA 99 standards, as they were created by the International Society for Automation (ISA) and publicly released as American National Standards Institute (ANSI) documents, were renumbered to be the ANSI/ISA-62443[13] series. This change was intended to align the ISA and ANSI document numbering with the corresponding International Electrotechnical Commission (IEC) standards.

All ISA work products are now numbered using the convention "ISA-62443-x-y" and previous ISA99 nomenclature is maintained for continuity purposes only. Corresponding IEC documents are referenced as "IEC 62443-x-y". The approved IEC and ISA versions are generally identical for all functional purposes.

ISA99 remains the name of the Industrial Automation and Control System Security Committee of the ISA. Since 2002, the committee has been developing a multi-part series of standards and technical reports on the subject of IACS security. These work products are then submitted to the ISA approval and then publishing under ANSI. They are also submitted to IEC for review and approval as standards and specifications in the IEC 62443 series.

2.13 EO 13636 (2013)

Executive Order 13636[14] seeks to strengthen the cybersecurity of critical infrastructure by increasing information sharing and by jointly developing and implementing a framework of cybersecurity practices with industry partners. It calls for government and industry to collaborate on measures to reduce our nation's cyber risks voluntarily but also suggests that additional regulation may be required if the current incentives prove insufficient to accomplish the stated goal.

While each of the standards developed over the years has contributed to the overall knowledge and expertise of the IT community, none of them stands out as the single definitive document by which the security of a system can be judged. The EO charges NIST with identifying and including the best features from each of them in its *Cybersecurity Framework* document. In this way it is hoped that the best of the best will become the new de facto industry standard.

3 Implications of the Executive Order

Executive Order (EO) 13636 identifies the need for improvements to critical infrastructure cybersecurity.

It directs NIST to develop a "Cybersecurity Framework" to serve as a baseline against which individual asset owners can compare their efforts to reduce cyber risk in their critical infrastructure.

[13] Copies of the completed and working documents in this standard can be found at http://isa99.isa.org.
[14] The text of EO 13636 can be found at http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.

It directs the Secretary of Homeland Security to "identify critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security."

"If current regulatory requirements are deemed to be insufficient" it authorizes the Secretary to require "prioritized, risk-based, efficient and coordinated actions … to mitigate cyber risk."

The language of the EO leads many to believe that additional government regulation may be used to promote the effort to secure the nation's critical infrastructure. In fact, the Department of Homeland Security says as much in the Fact Sheet[15] they issued on 12 March 2013, interpreting the presidential directive as requiring the nation "to:

- Develop a technology-neutral voluntary Cybersecurity Framework
- Promote and incentivize the adoption of cybersecurity practices
- Increase the volume, timeliness and quality of cyber threat information sharing
- Incorporate strong privacy and civil liberties protections into every initiative to secure our critical infrastructure
- Explore the use of existing regulation to promote cyber security"

For those who would prefer to avoid having government dictate their business practices, it should be clear that a priority should be to develop and implement policies of their own to secure those critical assets that are under their control.

4 What is this "framework" I hear about?

NIST has recently published a *Preliminary Cybersecurity Framework*[16] document for comment as directed by EO 13636. Its stated intent is to "provide guidance to an organization on managing cybersecurity risk." It is currently only informative, with no hint of any additional regulatory requirements.

The document references many of the standards described above in defining a process for evaluating infrastructure risk and deciding how to mitigate that risk economically and effectively. Appendix A of the document includes informative references from CCS, COBIT, IEC, ISA and ISO as well as NIST.

Briefly stated, the Framework presents a set of four elements (Functions, Categories, Subcategories and Informative References) to manage cybersecurity risk. These elements are tied together into Framework Implementation Tiers (Partial, Risk-Informed, Repeatable and Adaptive) that describe how an organization manages its cybersecurity risk.

[15] Visit http://www.dhs.gov/sites/default/files/publications/EO-PPD%20Fact%20Sheet%2012March13.pdf to view the DHS fact sheet.
[16] Read the entire document at http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf.

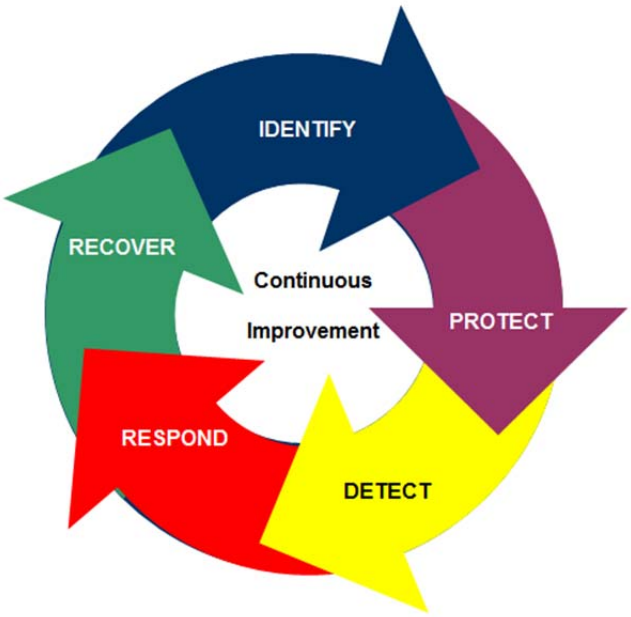

Figure 2 – Using the Framework Functions to Create a Cybersecurity Program

The document recommends a series of recursive steps for an organization to use the Framework to create a new cybersecurity program or improve an existing cybersecurity program.

- Step 1: **Identify**. The organization identifies its mission objectives, related systems and assets, regulatory requirements and overall risk approach.
- Step 2: **Create a Current Profile**. Beginning with the Categories specified in the Framework Core, the organization develops a Current Profile that reflects its understanding of its current cybersecurity outcomes based on its implementation of the Identify Function.
- Step 3: **Conduct a Risk Assessment**. The organization analyzes the operational environment in order to assess the likelihood of a cybersecurity event and discern the impact that such an event could have on the organization.
- Step 4: **Create a Target Profile**. The organization creates a Target Profile that focuses on the assessment of the Framework Elements (e.g., Categories, Subcategories) describing the organization's desired cybersecurity outcomes.
- Step 5: **Determine, Analyze, and Prioritize Gaps**. The organization compares the Current Profile and the Target Profile to determine gaps, and then determines resources necessary to address the gaps.
- Step 6: **Implement Action Plan**. The organization implements the steps defined in the action plan and monitors its current cybersecurity practices against the Target Profile.

Encouragingly, in Appendix C the NIST document states "The need for confidence in conformity assessment activities must be balanced with cost to the private and public sectors, including direct program costs, time-to-market delays, diverse global requirements, additional legal obligations, and the cost of nonconformity in the market." This suggests that the authors are not totally oblivious to the needs of the private sector.

5 How does EO 13636 affect me?

The most effective means of assessing the implications of the Executive Order is to consider answers to a series of commonly asked questions. These answers will vary by situation and can be used to shape an individual response. Several such questions are addressed in the following paragraphs.

5.1 Are my assets considered critical infrastructure?

A good first step is to determine whether or not your situation fits that being addressed by EO 13636, which defines critical infrastructure as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

If this sounds like a description of your business, you can bet that the government will take an interest in you and how you are protecting yourself from cyber attack. It is therefore in your own interest to prepare for the day when you will have to explain what measures you are taking to protect the national interest from compromise and forestall the creation of additional government regulations to which you may have to become compliant.

But even if your business is not significant enough to merit the government's scrutiny, your shareholders will still have a significant interest, especially if any substantial losses were to occur as a result of a cyber incident. Avoiding such encounters is always going to be preferable to recovering from them.

5.2 Do I need to establish a corporate cybersecurity standard for critical infrastructure?

Not necessarily. You can mitigate your cyber risks without a corporate standard in place, but it will be considerably easier to justify if you are complying with an already existing standard.

If you already have a corporate policy in place this is good news. Your higher management is conscious of the costs of being unprotected and has already taken steps to mitigate the risks involved. If a policy has been or is in the process of being implemented then the NIST Framework is a useful tool for examining it and evaluating its potential effectiveness.

If not, EO 13636 provides an excellent opportunity to pitch the need for having a corporate standard and a policy in place to follow it.

5.3 Do I need to be proactive or can I just be reactive?

This is difficult to answer. If you're lucky enough to not be the first in line to be subjected to government regulation, you may be able to react quickly enough to the news of the first unlucky asset owner and keep yourself on the right side of the authorities. Better that you should at least have a plan in place and perhaps actually implement it voluntarily.

Moreover, an approach that simply reacts to requirements or regulation has the potential to leave important assets at increased risk from attack.

5.4 Why can't I just follow my corporate cybersecurity standard?

If you are lucky enough to have one, the *Cybersecurity Framework* can be used as an adjunct to the currently existing corporate policy. A useful exercise is to conducts a "gap analysis", comparing existing company standards and practices to those recommended by the Framework. You may discover shortcomings of the current corporate policy and suggest improvements to it. The *Cybersecurity Framework* is not intended to replace your company's existing cyber risk policy.

5.5 Do I need to get started on one?

This is where the *Cybersecurity Framework* should shine. It has already done a great deal of the heavy lifting in considering the potential risks to your critical infrastructure and can easily be used to jump-start the development of the missing corporate standard in your organization.

Like existing Safety programs or Quality programs, your Cybersecurity program will need to be an evergreen process that recursively considers its objectives and the measures that have been and need to be taken to accomplish them. The *Cybersecurity Framework* document provides a convenient tool to help you establish your own program suited for your individual needs.

5.6 What happens if I'm not proactive?

The "elephant in the room" is the implied authority of regulatory agencies such as the Department of Homeland Security to impose regulations on critical infrastructure providers if they deem their voluntary efforts inadequate. The intent of the EO appears to be to encourage asset owners consider their cyber risk seriously and take effective measures to reduce that risk voluntarily, without the need for government regulation.

Not taking a preventative approach also has the potential to increase the risk of being impacted by a cyber attack.

6 How can I use NIST's *Cybersecurity Framework* to my advantage?

If you do not have an organizational cybersecurity policy or are involved in developing one, you will find the *Cybersecurity Framework* an excellent starting point.

6.1 Where do I begin?

The first step is to identify the state of your assets' cybersecurity risk by creating a current profile. The five functions described in the Framework Core provide a natural outline for anyone interested in understanding their own cybersecurity risk.

Starting with a risk analysis to determine whether your assets have any cybersecurity exposure and what the consequences of experiencing a cybersecurity event might be, document the current state of your assets. Then, given the information gleaned from this exercise, determine what the target state of your assets should be.

A gap analysis of the two profiles will show you what your cybersecurity program will need to address.

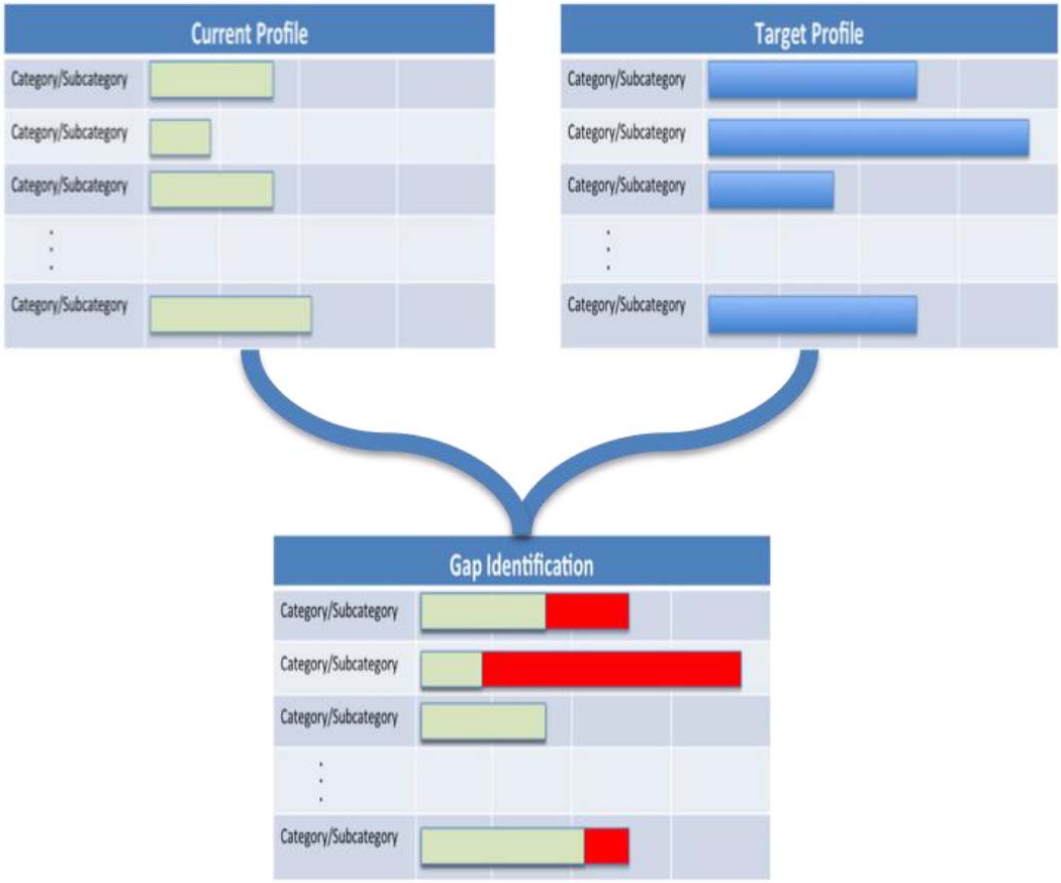

Figure 3 - Comparing Profiles

From the results of this assessment will flow the remainder of your cybersecurity program. Your organization's management will need to buy in to the changes required to mitigate the risks that were identified, allocate the necessary resources and establish priorities for implementing them. Follow the remaining recursive steps to advance the process.

6.2 How do I know what to do?

The Framework Core is not a checklist of activities to perform. Each individual case will have its own unique requirements. What the framework does is present key concepts that are known to help manage cybersecurity risk. It emphasizes the awareness, planning and communication that an organization should have in order to be effective at managing cybersecurity risk. The many standards and guidelines referenced in the Informative References are an excellent source for determining what comprise current best practices.

Assistance and advice on the selection of measures is available from a variety of sources. These include sector information sharing groups, standards bodies and professional consultants.

6.3 How does the "tier" concept affect my situation?

The tiering concept is similar to maturity levels that are used in various other management systems (e.g., Quality). The most effective approach is to use the tier descriptions to determine the desired state, based on an assessment of business needs and constraints.

The benefit is in having a semi-quantitative means of describing the organization's capability. In the words of the NIST document, the tier that will apply to you depends upon your "organization's risk management practices, threat environment, legal and regulatory requirements, business/mission objectives and organizational constraints."

6.4 How will I know when I am finished?

Like many other management processes (e.g., Safety, Quality), cybersecurity risk management is a continual process that is most effective when implemented in the form of a management system. Since the threat environment is always changing and the regulatory atmosphere is constantly evolving it would be presumptive to define a state of completion. However, like other PDCA processes, benefits continually accrue from the advancement of the process regardless of whether it can ever be considered finished.

7 Further Reading

- *Critical Infrastructure Security and Resilience*, Presidential Policy Directive 21 (PPD-21), The White House, February 12, 2013.
- *The Need to Know About Executive Orders: Much Ado About … Cybersecurity*, Leland E. Beck, Federal Regulations Advisor, February 18, 2013.
- *Executive Order 13636*, IT Law Wiki, February 19, 2013.
- *The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress*, Congressional Research Service, March 1, 2013.
- *Don't Reinvent the Wheel: Phil Agcaoili on the Cyber Security Framework*, Anthony M. Freed, TripWire, October 17, 2013.
- *The NIST Cybersecurity Framework – What is it and what does it mean to you?*, Ernest Hayden, Tofino Security, November 25, 2013.

Please send all comments and queries to research@berkanaresources.com or contact us at Berkana Resources Corporation, 700 Louisiana St, Suite 3950, Houston, TX 77002 (832)390.2694