A Holistic Approach to Cybersecurity: Mapping the NICE Workforce Framework to the Critical Infrastructure Cybersecurity Framework

Anne Kohnke, PhD
Assistant Professor of IT
akohnke@ltu.edu

Lawrence Technological University
College of Management
21000 West Ten Mile Road
Southfield, Michigan 48075
248.204.3085

Abstract - The need for a high degree of interconnectivity poses many challenges to organizations to adequately protect and defend their infrastructure from sophisticated cyber-attacks. External and internal attackers have caused substantial losses to organizations, not only in exposing embarrassing emails and incurring financial costs, but to the reputations that never recover. Hackers employ a variety of techniques and strategies to steal financial data, intellectual property, and expose sensitive information. They range from individual attackers, to activist groups, to teams of well-funded criminal enterprises, to full-time attackers employed on behalf of nation-states. If an organization does not have an IT cybersecurity program and security controls in place to handle threats, they will pay the price in costly data breaches and inevitable legal issues. However, cybersecurity is a relatively new discipline that is often referred to by a variety of names such as information assurance, information security management, and risk management activities. The demand for cybersecurity professionals to address the increased level of threats is being hindered by the absence of a common language or lexicon to understand the work and skill requirements for IT security positions. It is critical that organizations of all sizes have an understanding of the tasks, knowledge, skills, and abilities to develop an effective security program. This study evaluated two cybersecurity frameworks created by NIST, namely the National Initiative on Cybersecurity Education (NICE) Cybersecurity Workforce Framework 2.0 and the Cybersecurity Workforce Framework issued by Presidential Executive

Order 13636. We provide an in-depth mapping and discussion of the NICE Cybersecurity Workforce Framework 2.0 tasks to the CSF Framework functions and categories to provide a comprehensive understanding for cybersecurity professionals to develop and implement an effective IT security program.

Keywords

Cybersecurity, IT Governance, NICE Cybersecurity Workforce Framework, CSF Framework

1. INTRODUCTION

Computerized systems and the information they process are so tightly bound within the fabric of our society that their reliability, confidentiality, integrity, and availability of the information in which they process must be totally trustworthy in order to enable the fundamental structures of our society. For instance, one only has to imagine the impact on national security if military defense information was leaked to our adversaries. The problem lies in the fact that the knowledge that is required to assure reliable and consistent protection of cyber assets changes as rapidly as the technology evolves. As a result, most people view the practices involved in ensuring cybersecurity as an opaque set of activities and requirements that few can truly understand or apply. As a consequence, electronic infrastructure in many organizations is riddled with vulnerabilities that have underwritten a significant number of criminal and national security exploits over the past decade (PRC, 2014). For instance, according to the non-profit Privacy Rights Clearinghouse there have been one billion records lost in the past 10 years (PRC, 2014). Keep in mind that those losses only comprise the outcome of breaches that were reported and since most organizations are reluctant to publicize security failures that number is most likely underrepresented (PRC, 2014).

2. THE EMERGING FIELD OF CYBERSECURITY

The issues associated with cybersecurity can be dated to the advent of the Internet which was made commercially available in the mid-1990s. Accordingly, the entire profession has a less than twenty year lifespan. In that time cyber-crime, cyber-espionage and even cyber-warfare have become visions with real consequences. Consequently, until there is a single commonly accepted definition of the field and the profession it is unrealistic to assume that our way-of-life is adequately protected. Yet, even with its newfound national prominence, there is still a lot of disagreement about what legitimately constitutes the right set of actions to prevent harmful, or adversarial actions. Cybersecurity is at best an ill-defined field, which is subject to a range of interpretation by numerous special interest groups (Burley, Eisenberg, & Goodman, 2014). Since there has been heretofore no clear definition of the field the profession and the actual protection of computers and information tends to be characterized by a long track record of hit-and-misses.

The confusion about what constitutes the proper elements of the field or the profession of cybersecurity originates from concepts from a number of disciplines. Some content from a variety disciplines might reasonably fall within legitimate boundaries and includes such diverse areas as:

- Business management – which contributes concepts like security policy and procedures, disaster recovery and continuity planning, personnel management, contract and regulatory compliance.
- The traditional technical studies of computer security, such as computer science, contribute knowledge about ways to safeguard the processing of information in its electronic form.
- Likewise, knowledge from the field of networking adds essential recommendations about how to safeguard the electronic transmission and storage of information.
- Software engineering adds the necessary system and software assurance considerations like testing and reviews, configuration management, and lifecycle process management.
- Law and law enforcement contribute important ideas about such topics as intellectual property rights and copyright protection, privacy legislation,

cyber law and cyber litigation, and the investigation and prosecution of computer crimes

- Behavioral studies address essential human factors like discipline, motivation, training, and certification of knowledge.
- Even the field of ethics, with its consideration of the personal and societal implications of information use and information protection, as well as codes of conduct contribute something to the discussion.

All of these areas could potentially bring something to the overall aim of information protection. As such, it would seem logical to incorporate the principles and methods from each area into the total body of best practice for cybersecurity. Nonetheless, there is still discussion about where the line ought to be drawn, or where the focus within those boundaries ought to be.

3. A HOLISTIC APPROACH

The term "holistic" can be used to describe what has to happen in order for a security solution to be airtight. However, there are a number of systemic and cultural challenges that must be addressed. First, most of the current crop of cybersecurity professionals specializes in some vertical aspect of the field and do not necessarily approach things holistically. There are models that define personal requirements for practitioners within specific silos of practice. These include the common body of knowledge (CBK) for the Certified Information System Security Professional (CISSP) and the Information System Audit and Control Association's (ISACA) Control Objectives for IT (COBIT). Specifically, ISC2s CISSP certification and ISACA's Certified Cybersecurity Manager (CISM) provide a perfectly acceptable CBK for cybersecurity professionals (Whitman & Mattord, 2012). However, they are totally different and competing models, in the commercial space, and therefore they are not considered to be a commonly accepted basis the profession.

The National Initiative for Cybersecurity Education (NICE) workforce framework defines the complete set of roles that might reasonably be considered part of the cybersecurity workforce (NIST, 2014). Thus, in essence, the NICE framework defines the field of "cybersecurity." The NICE Cybersecurity Workforce Framework is an umbrella framework, in the sense that its intention is to define the complete set of competencies associated with cybersecurity work. However, the NICE framework goes a step further in that it also links those competencies to a group of common security roles and a set of functions associated with those roles (NIST, 2014). That gives individual practitioners a standard set of recommendations about the activities that should be implemented in order to fulfill the requirements of each of those roles.

The aim of the NICE Cybersecurity Workforce Framework is to establish the common taxonomy and lexicon to be used to describe all cybersecurity work and workers irrespective of where or for whom the work is performed" (NIST, 2014). The Framework is composed of seven general knowledge areas and thirty two distinct specialty areas. These Knowledge and Specialty areas define the range of activities that legitimately comprise the cybersecurity profession. In that respect NICE has become the first truly holistic definition of the field. The NICE Framework is composed of seven general Knowledge Areas that serve as an overarching structure for the field. Figure 1 (below) illustrates this:

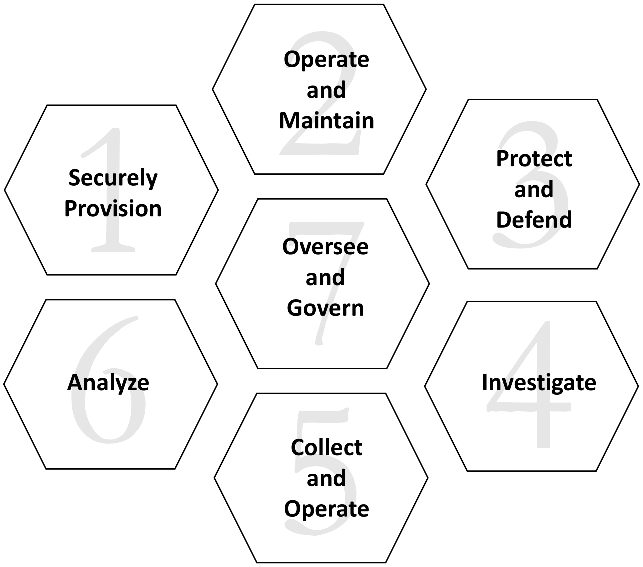


Figure 1: The NICE Cybersecurity Workforce Framework 7 General Knowledge Areas

There are thirty two Specialty Areas that accompany the seven general knowledge areas. Figure 2 (below) shows the 32 specialty areas associated with each of their respective general knowledge area:

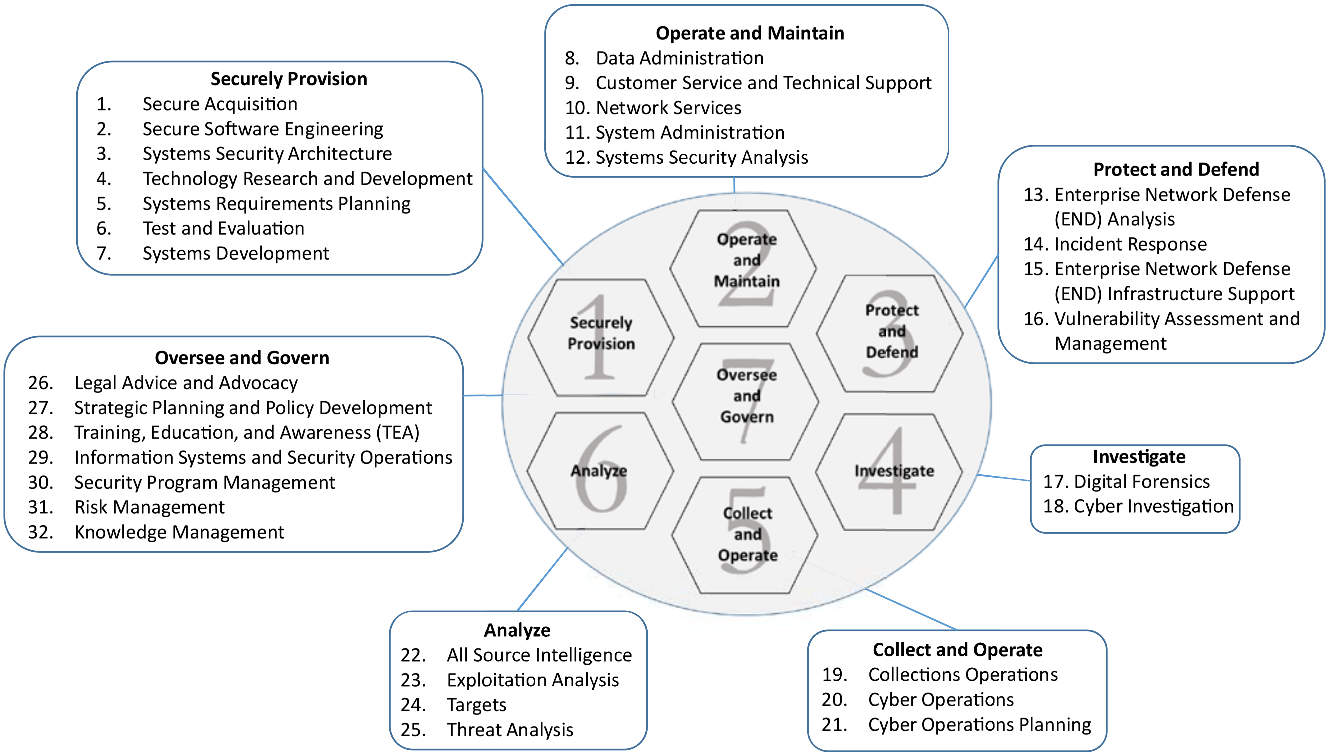

Securely Provision
1. Secure Acquisition
2. Secure Software Engineering
3. Systems Security Architecture
4. Technology Research and Development
5. Systems Requirements Planning
6. Test and Evaluation
7. Systems Development
Operate and Maintain
8. Data Administration
9. Customer Service and Technical Support
10. Network Services
11. System Administration
12. Systems Security Analysis
Protect and Defend
13. Enterprise Network Defense (END) Analysis
14. Incident Response
15. Enterprise Network Defense (END) Infrastructure Support
16. Vulnerability Assessment and Management
Investigate
17. Digital Forensics
18. Cyber Investigation
Collect and Operate
19. Collections Operations
20. Cyber Operations
21. Cyber Operations Planning
Analyze
22. All Source Intelligence
23. Exploitation Analysis
24. Targets
25. Threat Analysis
Oversee and Govern
26. Legal Advice and Advocacy
27. Strategic Planning and Policy Development
28. Training, Education, and Awareness (TEA)
29. Information Systems and Security Operations
30. Security Program Management
31. Risk Management
32. Knowledge Management
1 Securely Provision
2 Operate and Maintain
3 Protect and Defend
4 Investigate
5 Collect and Operate
6 Analyze
7 Oversee and Govern

Figure 2: The 32 Specialty Areas of the NICE Cybersecurity Workforce Framework

For each Specialty Area, a set of Professional Roles has been identified and associated with it. These roles fulfill the workforce requirements for that specialty area. Figure 3 shows the professional roles for the seven specialty areas within the Security Provision general knowledge area:

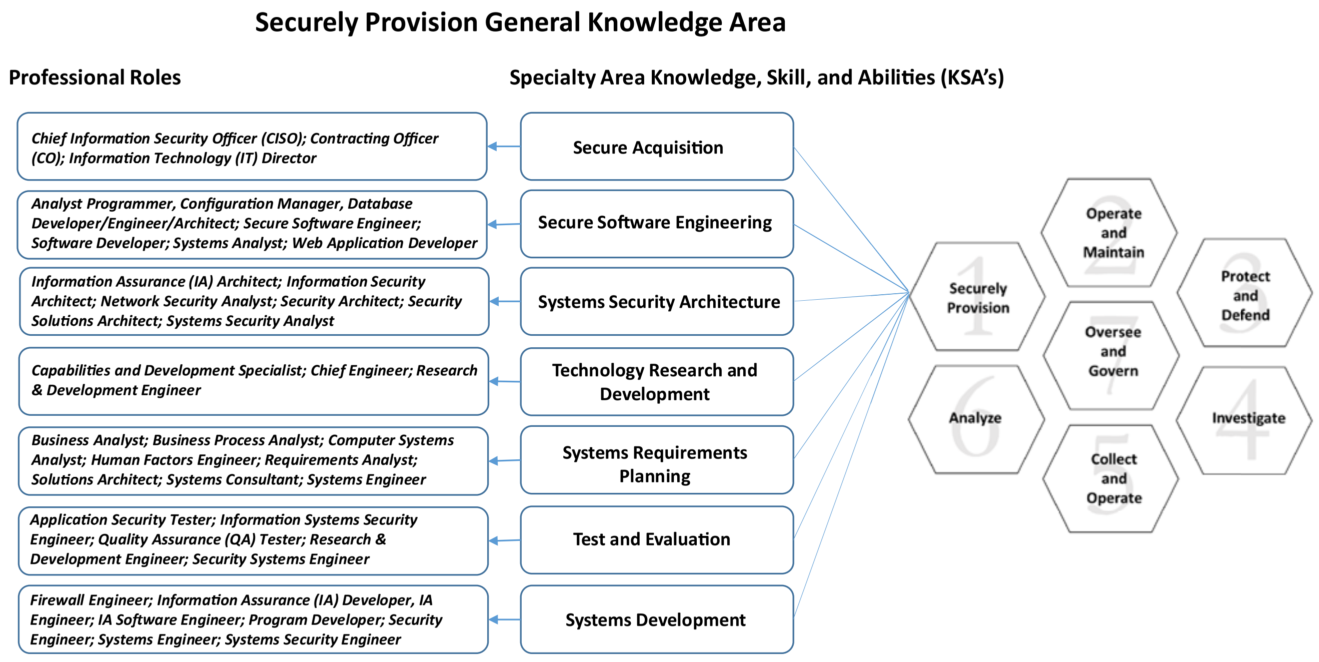
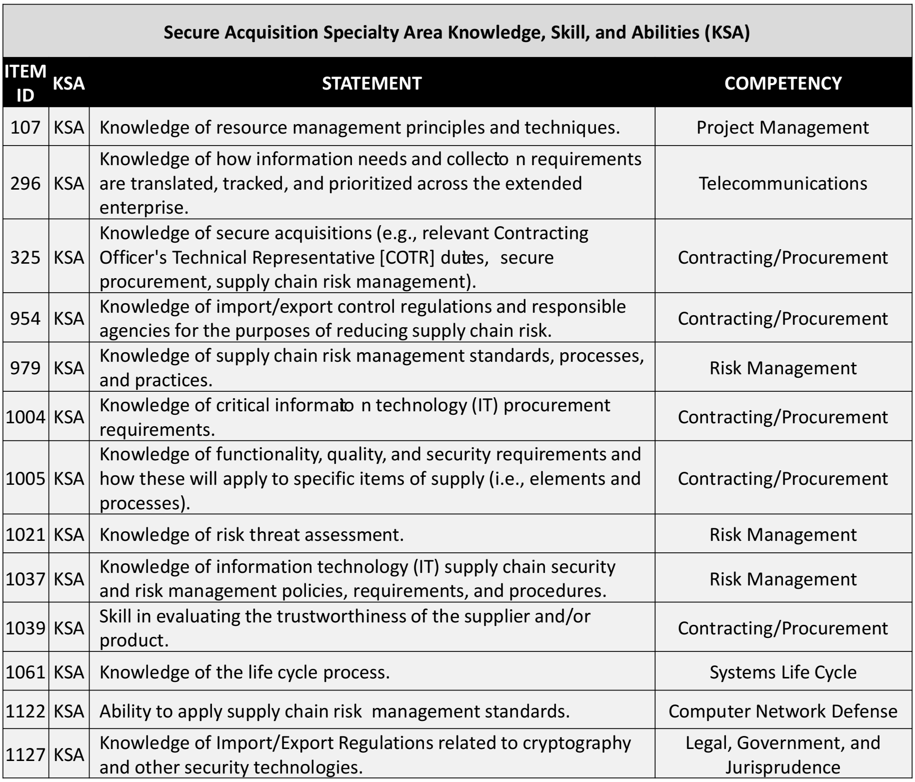

Securely Provision General Knowledge Area
Professional Roles
Specialty Area Knowledge, Skill, and Abilities (KSA's)
Chief Information Security Officer (CISO); Contracting Officer (CO); Information Technology (IT) Director
Analyst Programmer, Configuration Manager, Database Developer/Engineer/Architect; Secure Software Engineer; Software Developer; Systems Analyst; Web Application Developer
Information Assurance (IA) Architect; Information Security Architect; Network Security Analyst; Security Architect; Security Solutions Architect; Systems Security Analyst
Capabilities and Development Specialist; Chief Engineer; Research & Development Engineer
Business Analyst; Business Process Analyst; Computer Systems Analyst; Human Factors Engineer; Requirements Analyst; Solutions Architect; Systems Consultant; Systems Engineer
Application Security Tester; Information Systems Security Engineer; Quality Assurance (QA) Tester; Research & Development Engineer; Security Systems Engineer
Firewall Engineer; Information Assurance (IA) Developer, IA Engineer; IA Software Engineer; Program Developer; Security Engineer; Systems Engineer; Systems Security Engineer
Secure Acquisition
Secure Software Engineering
Systems Security Architecture
Technology Research and Development
Systems Requirements Planning
Test and Evaluation
Systems Development
1 Securely Provision
2 Operate and Maintain
3 Protect and Defend
4 Investigate
5 Collect and Operate
6 Analyze
7 Oversee and Govern

Figure 3: The Security Provision General Knowledge Area with associated Specialty Areas and Professional Roles

Each Specialty Area also itemizes a set of KSAs and competencies associated with that particular Specialty Area. Figure 4 (below) illustrates the Knowledge, Skills, and Abilities (KSAs) identified for the Secure Acquisition Specialty Knowledge Area:



Secure Acquisition Specialty Area Knowledge, Skill, and Abilities (KSA)

ITEM ID	KSA	STATEMENT	COMPETENCY
107	KSA	Knowledge of resource management principles and techniques.	Project Management
296	KSA	Knowledge of how information needs and collection requirements are translated, tracked, and prioritized across the extended enterprise.	Telecommunications
325	KSA	Knowledge of secure acquisitions (e.g., relevant Contracting Officer's Technical Representative [COTR] duties, secure procurement, supply chain risk management).	Contracting/Procurement
954	KSA	Knowledge of import/export control regulations and responsible agencies for the purposes of reducing supply chain risk.	Contracting/Procurement
979	KSA	Knowledge of supply chain risk management standards, processes, and practices.	Risk Management
1004	KSA	Knowledge of critical information technology (IT) procurement requirements.	Contracting/Procurement
1005	KSA	Knowledge of functionality, quality, and security requirements and how these will apply to specific items of supply (i.e., elements and processes).	Contracting/Procurement
1021	KSA	Knowledge of risk threat assessment.	Risk Management
1037	KSA	Knowledge of information technology (IT) supply chain security and risk management policies, requirements, and procedures.	Risk Management
1039	KSA	Skill in evaluating the trustworthiness of the supplier and/or product.	Contracting/Procurement
1061	KSA	Knowledge of the life cycle process.	Systems Life Cycle
1122	KSA	Ability to apply supply chain risk management standards.	Computer Network Defense
1127	KSA	Knowledge of Import/Export Regulations related to cryptography and other security technologies.	Legal, Government, and Jurisprudence

Figure 4: Knowledge, Skills, and Abilities (KSAs) identified for the Secure Acquisition Specialty Knowledge Area

The NICE Cybersecurity Workforce Framework is intended to be applied in the public, private, and academic sectors. Use of the Framework does not require that organizations change organizational or occupational structures. In fact, the Framework was developed because requiring such changes would be costly, impractical, ineffective, and inefficient. Thus the Framework can be applied to situations across all types of settings and environments.

4. THE CRITICAL INFRASTRUCUTRE CYBERSECURITY (CSF) FRAMEWORK

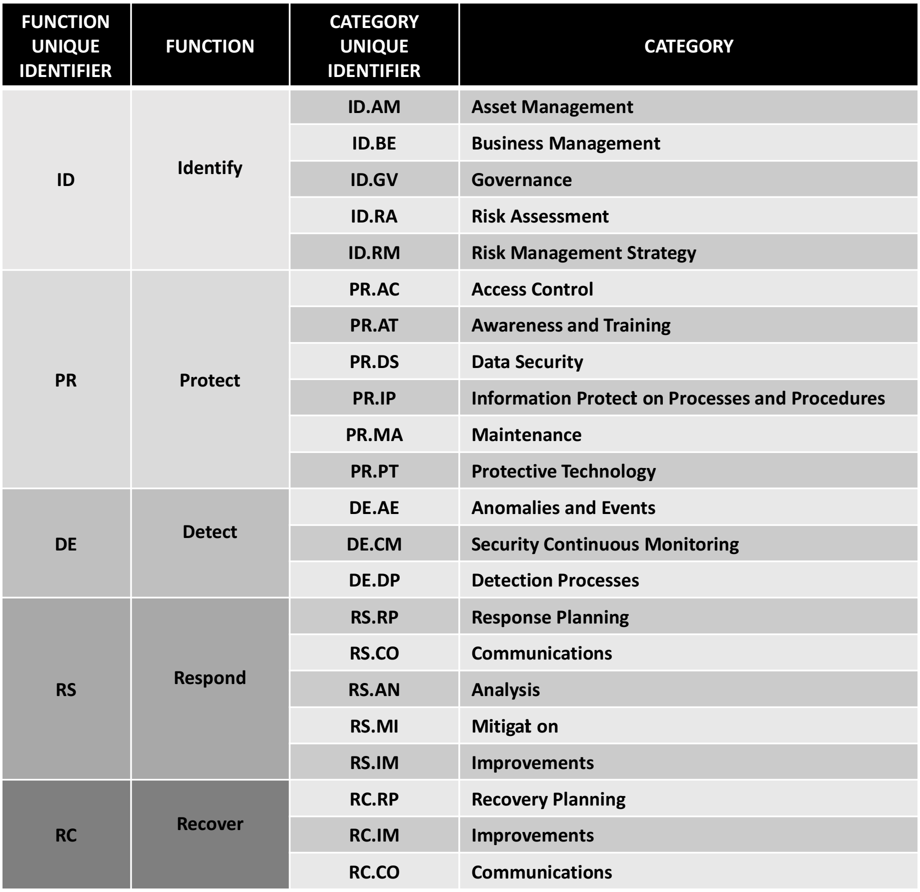
Although the workforce roles and KSAs have been standardized there is no description of a standard process to guide the work. That is where the National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity Version 1.0" (CSF), comes in (Executive Order 13636, 2013). The CSF Standard provides a specification of the basic functions necessary to implement a complete infrastructure protection system for cybersecurity. In simple, operational terms, the cybersecurity process involves nothing more than deploying and then ensuring a coherent set of best practices to protect all assets of value to a particular company. The problem lies in the term "best practice." As we saw with the elephant, everybody has their own definition of what constitutes best practice. So, the actions that one group might view as appropriate to secure an asset may not be seen quite as appropriate to another group. Therefore, it is essential to adopt a complete and commonly accepted framework of correct practice as a point of reference to guide any actions that an organization might take to protect its assets in the real-world. The ideal would be to have that framework authorized and endorsed by a universally recognized and legitimate third party.

In the case of cybersecurity, the best practice framework ought to encompass all of the legitimate actions necessary to ensure a reasonable state of reliable long-term security. Then, with respect to evaluating whether due care has been taken, it can be assumed that, if all of these practices are executed properly then the organization has met its legal and ethical obligations for information protection. Many other professions, such as the law, or medicine, have a commonly agreed upon definition of what it takes to meet the minimum standard of due care. Those help set the boundaries of ethical practice as well as guide the correctness of actions within those boundaries. Up to this point however, the problem for cybersecurity professionals is that that generally accepted framework didn't exist. So the research question became, "Can the best practice advice of the CSF framework be used to guide the deployment of the role, task, and KSA requirements of the NICE Model?" Ideally, a framework for good Cybersecurity practice would be universal in its application. Its correctness would be commonly accepted within the practitioner community. The model's recommendations would embody all of the currently understood correct actions for ensuring the confidentiality, integrity, availability, authentication and non-repudiation of information. Moreover, those recommendations would be expressed in a form that would allow a competent practitioner to tailor out a practical and economically feasible system that would protect all of the information of value under their care.

In day-to-day practice, the number of defenses that are weak or exploitable have been increasing over the past decade across the spectrum of government, business and academe due to the number and type of attackers growing in size and sophistication (PRC, 2014). In the 1990s, a typical attack was something like a criminal trespass or web-site defacement. The victims tended to be government institutions and attackers were inclined to be counterculture types who worked alone and on the fringes (Schmalleger & Pittaro, 2009). Now instead of being inspired by a desire to prove their art, attackers are motivated by financial gain and political ends. As a consequence, the old stereotypical image of the young adult conducting seventy-two hour hacks out of his parent's basement has been replaced by a much darker and more complex persona, one who is well organized and much more focused on making trouble. For instance, there are organized groups who perpetrate large-scale raids on financial institutions for the purpose of theft. The opportunities for financial gain from cyber-crime are so great now that established organized crime syndicates have taken to the business of electronic crime with the same zeal and enthusiasm as they did in the past with traditional physical crimes. However, this new criminal business does not involve guns and strong-arm tactics. Instead it involves all of the potential ways that information can be obtained and exploited, ranging from sophisticated hacking to dumpster diving.

The purpose of the CSF framework is to enable managers and corporate end users to identify gaps in their security management infrastructure. This standard creates a comprehensive and persistent top-down process that will allow an organization to maintain effective security. The CSF framework provides a categorized set of cybersecurity outcomes and recommended controls for their achievement. It has three primary components: *Core, Profile, and Implementation Tiers*.

The *Core* is a hierarchical structure which consists of five risk control functions. Each Function is further broken down into Categories and Subcategories. Each Subcategory is further matched to Information Resources Examples of Information Resources are industry standards and guidelines, which, in combination provide a set of cybersecurity risk management best practices. Figure 5 illustrates this structure:



FUNCTION UNIQUE IDENTIFIER	FUNCTION	CATEGORY UNIQUE IDENTIFIER	CATEGORY
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Management
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protect on Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigat on
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Figure 5: The Critical Infrastructure Cybersecurity Framework (CSF)

The *Profile* provides organizations the ability to align their cybersecurity practices to their individual business needs. To do so, organizations create a Current Profile by measuring their existing programs against the recommended practices in the Framework Core. To identify a Target Profile, organizations employ the same Core criteria to determine the actions required to improve their cybersecurity posture. A comparison of the Current and Target Profiles will provide a roadmap to help make improvements. Figure 6 illustrates the seven step process on how an organization could use the CSF Framework to create either a new cybersecurity program or improve an existing one:

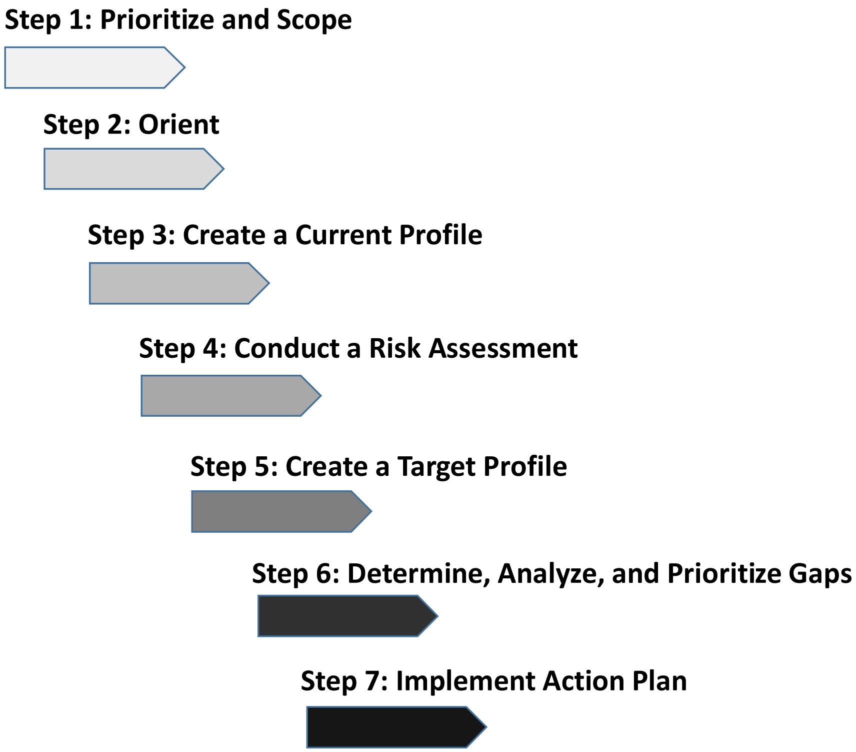
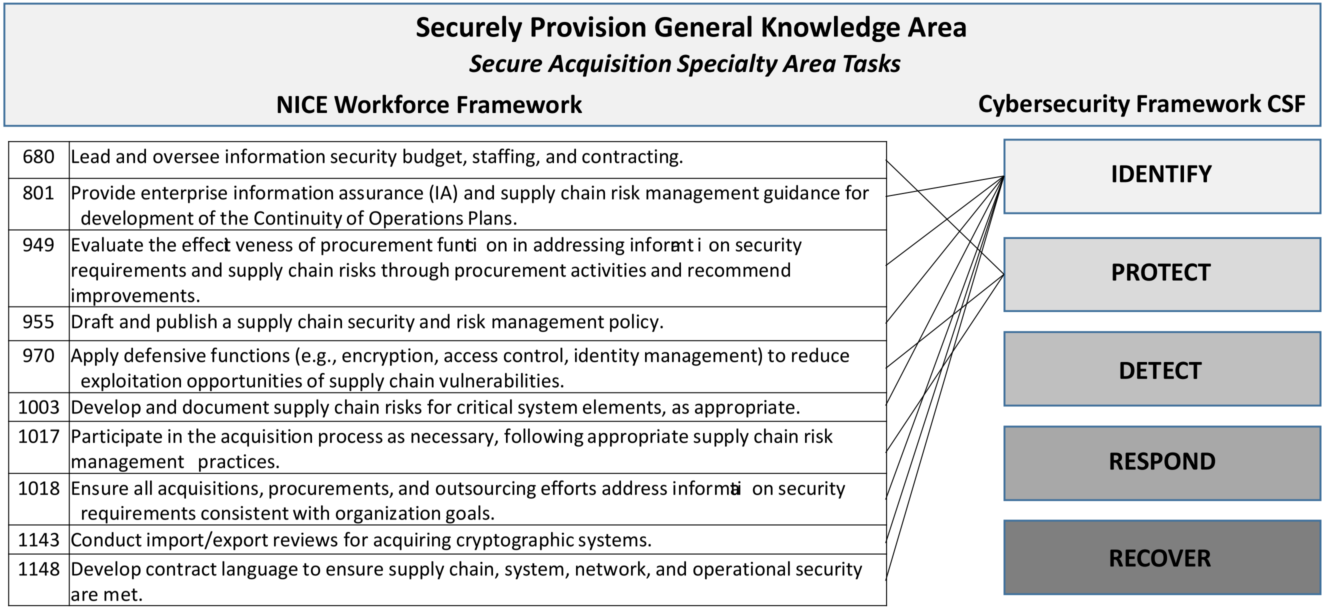

Step 1: Prioritize and Scope
Step 2: Orient
Step 3: Create a Current Profile
Step 4: Conduct a Risk Assessment
Step 5: Create a Target Profile
Step 6: Determine, Analyze, and Prioritize Gaps
Step 7: Implement Action Plan

Figure 6: Seven Step Process to Create a New Cybersecurity Program or Improve an Existing One

The *Implementation Tiers* help the organization understand how their current cybersecurity risk-management capabilities rate against the characteristics described by the framework. Tiers range from Partial (Tier 1) to Adaptive (Tier 4).

5. USING THE CSF AND NICE FRAMEWORKS TOGETHER

The CSF provides a categorized set of cybersecurity outcomes and recommended controls for their achievement. While the NICE framework defines the tasks required to carry out those control activities. The combination of the CSF and NICE framework can provide the "complete package" for managing cybersecurity risk. We have mapped all of the NICE specialty areas to the CSF Framework functions and created a total of 37 mapping documents. The following two figures (7 & 8) provide examples of 2 of the 37 documents in which tasks defined in the NICE secure acquisition and network services specialty areas are mapped to the CSF Framework function level:



Securely Provision General Knowledge Area

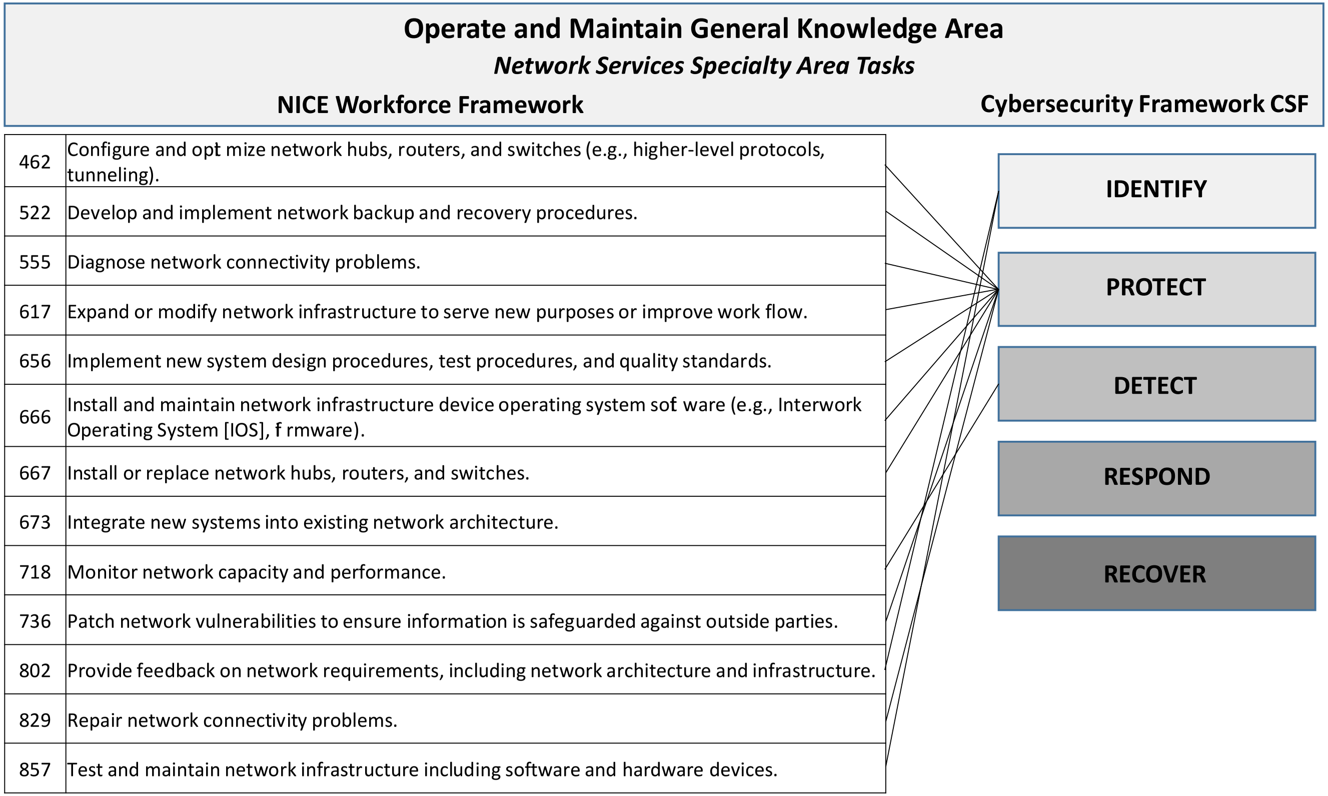
Secure Acquisition Specialty Area Tasks

NICE Workforce Framework

Cybersecurity Framework CSF

680	Lead and oversee information security budget, staffing, and contracting.
801	Provide enterprise information assurance (IA) and supply chain risk management guidance for development of the Continuity of Operations Plans.
949	Evaluate the effectiveness of procurement function in addressing information security requirements and supply chain risks through procurement activities and recommend improvements.
955	Draft and publish a supply chain security and risk management policy.
970	Apply defensive functions (e.g., encryption, access control, identity management) to reduce exploitation opportunities of supply chain vulnerabilities.
1003	Develop and document supply chain risks for critical system elements, as appropriate.
1017	Participate in the acquisition process as necessary, following appropriate supply chain risk management practices.
1018	Ensure all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals.
1143	Conduct import/export reviews for acquiring cryptographic systems.
1148	Develop contract language to ensure supply chain, system, network, and operational security are met.

Figure 7: NICE Secure Acquisition Specialty Area Tasks Mapped to the CSF Framework Functions



Operate and Maintain General Knowledge Area

Network Services Specialty Area Tasks

NICE Workforce Framework **Cybersecurity Framework CSF**

462	Configure and optimize network hubs, routers, and switches (e.g., higher-level protocols, tunneling).
522	Develop and implement network backup and recovery procedures.
555	Diagnose network connectivity problems.
617	Expand or modify network infrastructure to serve new purposes or improve work flow.
656	Implement new system design procedures, test procedures, and quality standards.
666	Install and maintain network infrastructure device operating system software (e.g., Interwork Operating System [IOS], firmware).
667	Install or replace network hubs, routers, and switches.
673	Integrate new systems into existing network architecture.
718	Monitor network capacity and performance.
736	Patch network vulnerabilities to ensure information is safeguarded against outside parties.
802	Provide feedback on network requirements, including network architecture and infrastructure.
829	Repair network connectivity problems.
857	Test and maintain network infrastructure including software and hardware devices.

Figure 8: NICE Network Services Specialty Area Task Mapped to the CSF Framework Functions

The NICE Workforce framework provides a strategic description of all of the elements of the cybersecurity field. It specifies all of the commonly agreed on activities and inter-relationships associated with good security into a single workforce model. Moreover, the NICE Workforce framework stipulates all of the requisite and commonly accepted workforce professional roles and practices necessary to carry out a complete set of cybersecurity activities. However, with cyber threats changing on nearly a daily basis; and with them, an organization's business environment and ability to meet new changing requirements; the ability to apply new risk strategies is critical. Well planned, developed, and documented strategies are applied to the vast array of levels of security needed in order to evolve and support business operations and risk, not simply as an effort in compliance of local, state, and federal regulations.

6. CONCLUSION AND DISCUSSION

The Framework for Improving Critical Infrastructure Cybersecurity (CSF), is a set of guidelines and practices also created by NIST, which provides government and non-government organizations a vital first step toward managing cyber-security risk. Moving forward, organizations need solutions that not only satisfy the NIST Cybersecurity Framework at the time of deployment but also enable continued security as threats and business requirements change and evolve. The conclusion can be made that the combination of the CSF and NICE Workforce framework provide the "complete package" in managing cybersecurity risk. The CSF provides a categorized set of cybersecurity outcomes and recommended controls for their achievement, while the NICE Workforce framework defines the tasks required to accomplish the control activities, in addition to defining the knowledge and skills sets necessary to perform those activities. A common framework for cybersecurity will also enable IT security managers to effectively communicate practices, goals, and compliance requirements with third party partners, service providers, and regulators. In particular, there should be a more meaningful, structured dialogue of cybersecurity priorities with third parties.

The Cybersecurity information assurance process has many facets. These have been standardized in the form of the NICE Workforce framework however, the Cybersecurity process has to be coordinated to be effective. That process can be standardized in the functions and controls of the CSF. The two NIST models can be combined into a single detailed prescription for implementing common best practice for cybersecurity. Together they can provide a standard, commonly accepted basis for creating true systematic cybersecurity responses in an organization. And although this may sound like a lot of effort, given the number of threats and hazards in cyberspace it would also seem like a comprehensive protection plan is a wise thing for any organization to develop and implement.

REFERENCES

[1] Burley, D., Eisenberg, J., and Goodman, S. E. (2014). "Would Cybersecurity Professionalization Help Address the Cybersecurity Crisis?" *Communications of the ACM*, Vol 57, No. 2, pp 24-27.

[2] Executive Order 13636, (2013). "Framework for Improving Critical Infrastructure Cybersecurity", *Federal Register*, Vol. 78, No. 33, Part III.

[3] ISO, (2014). *ISO/IEC 27000:2014*, International Standards Organization, Geneva

[4] NIST, (2014). "National Cybersecurity Workforce Framework", [online], National Institute of Standards and Technology, http://csrc.nist.gov/nice/framework/national_cybersecurity_workforce_framework_03_2013_version1_0_for_printing.pdf

[5] PRC (2014). "Chronology of Data Breaches Security Breaches 2005 – Present", [online], Privacy Rights Clearinghouse, http://www.privacyrights.org/data-breach

[6] Saltzer J. H. and Schroeder, M.D. (1974). "The Protection of Information in Computer Systems", *Communications of the ACM* Vol 17, No.7, pp 388.402.

[7] Schmalleger, F. and Pittaro, M. (2009). *Crimes of the Internet*, Prentice Hall, Upper Saddle River, N.J.

[8] Whitman, M.E. and Mattord, H.J. (2012). *Principles of Information Security*, Cengage, Boston.