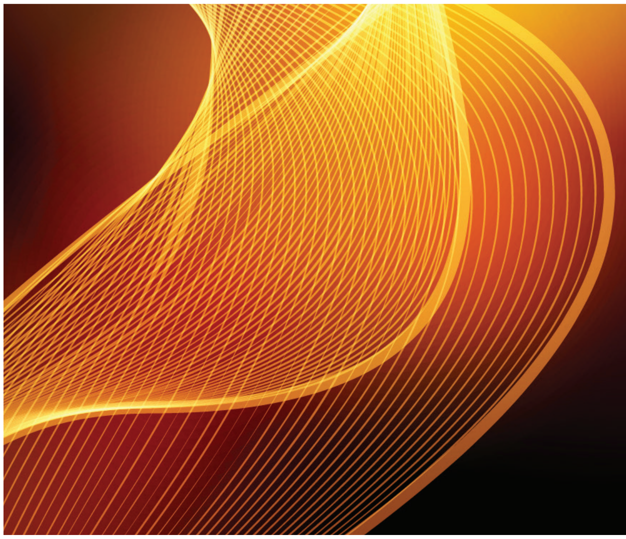


# Implementation Framework – Workforce Development and Management

*Melissa Kasan Ludwick*
*Troy Townsend*
*Jay McAllister*

*September 2013*

This material is based upon work funded and supported by ODNI under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of ODNI or the United States Department of Defense.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHEDON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

DM-0000620

# Implementation Framework – Workforce Development and Management

## Background

The Software Engineering Institute (SEI) Emerging Technology Center at Carnegie Mellon University studied the state of cyber intelligence across government, industry, and academia to advance the analytical capabilities of organizations by using best practices to implement solutions for shared challenges. The study, known as the Cyber Intelligence Tradecraft Project (CITP), defined cyber intelligence as the acquisition and analysis of information to identify, track, and predict cyber capabilities, intentions, and activities to offer courses of action that enhance decision making.

The characteristics of organizations and cyber intelligence capabilities varied among CITP participants. The SEI team worked with organizations just starting a cyber intelligence program, organizations with a robust, or advanced program, and others that were somewhere in between. An organization's cyber intelligence workforce – who to hire in leadership and analyst roles - emerged as a common struggle, regardless of the organizations size.

During CITP,  the SEI team learned of the differing demands of cyber intelligence analysts, typically based on the size of the organization or the maturity of their cyber intelligence program. Often, organizations did not have clear expectations for what the analyst's skills or competencies should be to best fit within their intelligence functions. Generally, organizations hired their cyber intelligence analysts by taking a non-technical analyst and providing them with training in cyber security, or by taking a technical practitioner and teaching them to look at the bigger picture and analyze technical data through a strategic lens.

The team also learned of the varied responsibilities of cyber intelligence leadership. Leadership was generally hired based on past intelligence experience, often from government positions. While these individuals have a vast amount of knowledge and experience, organizations need to be cautious and hire based on the maturity of their cyber intelligence function. Leadership requirements will differ for organizations just starting a cyber intelligence initiative versus organizations with an advanced function.

The Workforce Development Management Implementation Framework provides organizations with a guide to acquire the leadership, analysts, and tools appropriate for their cyber intelligence function.

## Implementation

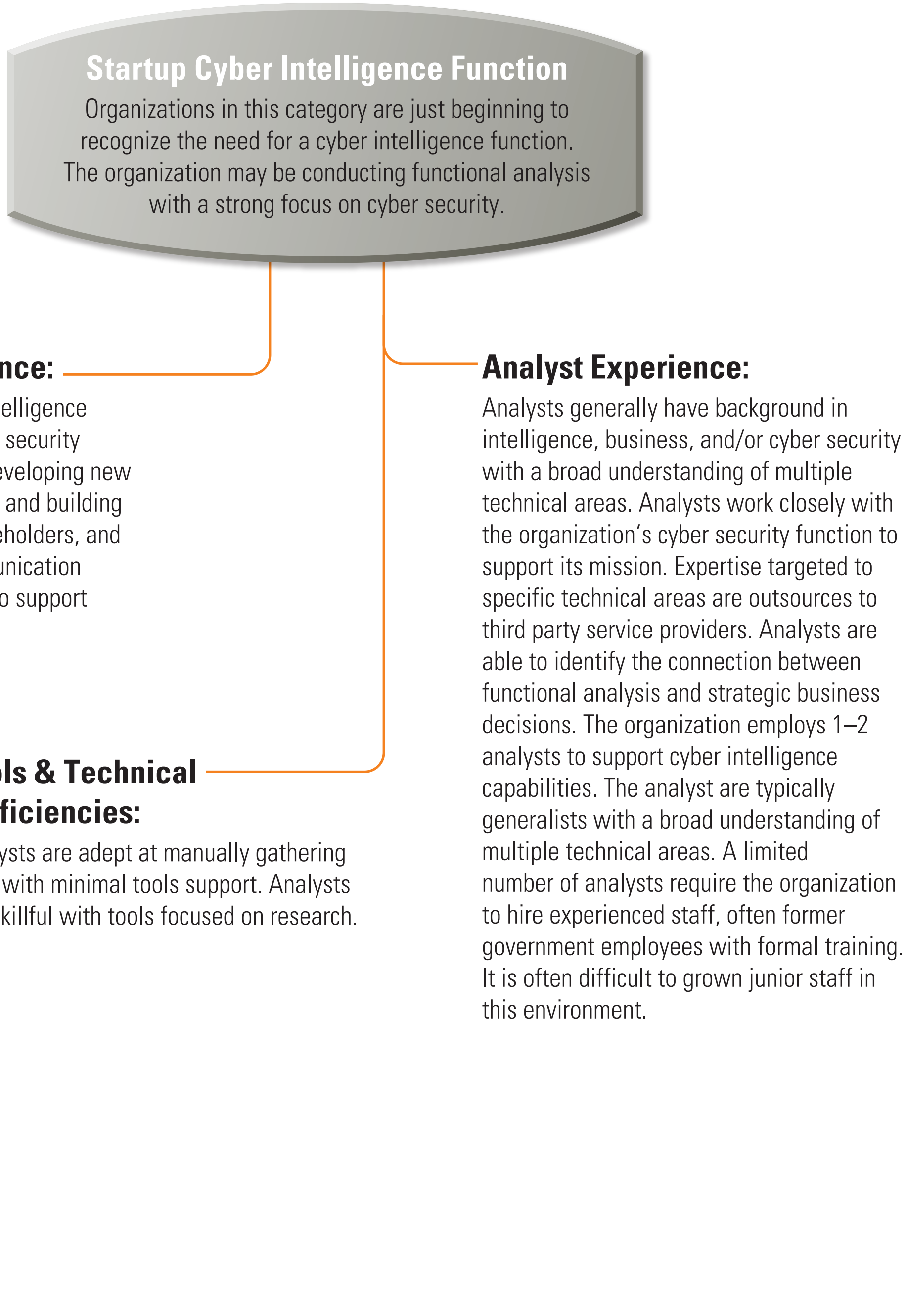
Here's how an organization can leverage the Workforce Development and Management Implementation Framework to develop and improve their cyber intelligence function:

1. Determine the profile that best describes your organization. The table below characterizes three different organizations by indications of targeted attacks and cyber footprint (comprised of environment and network size).

| Organization Profile | Organization A | Organization B | Organization C |
|---|---|---|---|
| Indications of Targeted Attacks | This organization has no indications of targeted attacks and is not in one of the government identified critical infrastructure sectors. | This organization has received some indications of targeted attacks and may be in one of the government identified critical infrastructure sectors. | This organization has received indications of persistent targeted attacks and is in one of the government identified critical infrastructure sectors. |
| Cyber Footprint | The organization utilizes cyber intelligence to predict and defend against attacks to its cyber footprint, comprised of a network with 25,000 nodes or less, and an external web and social media presence. The network does not contain third party connections and provides very limited external capabilities (i.e., no VPN, telnet, remote access, IDP). | The organization utilizes cyber intelligence to predict and defend against attacks to its cyber footprint, comprised of a network of 25,000 – 150,000 nodes, and an external web and social media presence. The external web presence does include some interactions with customers. Third party network connections are required for business operations, most notably, customer transactions and PII data. This organization may have an international network presence and allows its employees external network access - VPN, telnet, remote access, IDP). | The organization utilizes cyber intelligence to predict and defend against attacks to its cyber footprint, comprised of a network with more than 150,000 nodes, and a substantial external web and social media presence. The external web presence includes interactions and transactions with customers, and the organization hosts customers PII data. Third party network connections are required for business operations and are heavily integrated into the organization's network. This organization has a multinational presence and allows its employees external network access - VPN, telnet, remote access, IDP). |

2. Use the graphic below to establish and/or improve your organization’s cyber intelligence function.
   - Identify the current state of your organization’s cyber intelligence function
   - Identify the progression path for your organization’s cyber intelligence function
   - Use the graphic below to determine the leadership and analyst experience, tools, and technical proficiencies needed to establish and best grow your organization’s function

**The team recommends that companies fitting the “Organization A” description should be operating minimally at the Startup Cyber Intelligence Function. “Organization B” operating at the Established, or Advanced Cyber Intelligence Functions, and “Organization C” operating at the Advanced Cyber Intelligence Function.**



### Startup Cyber Intelligence Function

Organizations in this category are just beginning to recognize the need for a cyber intelligence function. The organization may be conducting functional analysis with a strong focus on cyber security.

### Leadership Experience:

The organization’s cyber intelligence leadership is typically more security minded with expertise in developing new initiatives, such as defining and building processes, identifying stakeholders, and establishing lines of communication throughout business units to support analyst collaboration.

### Analyst Experience:

Analysts generally have background in intelligence, business, and/or cyber security with a broad understanding of multiple technical areas. Analysts work closely with the organization’s cyber security function to support its mission. Expertise targeted to specific technical areas are outsources to third party service providers. Analysts are able to identify the connection between functional analysis and strategic business decisions. The organization employs 1–2 analysts to support cyber intelligence capabilities. The analyst are typically generalists with a broad understanding of multiple technical areas. A limited number of analysts require the organization to hire experienced staff, often former government employees with formal training. It is often difficult to grown junior staff in this environment.

### Tools & Technical Proficiencies:

Analysts are adept at manually gathering data with minimal tools support. Analysts are skillful with tools focused on research.

## Established Cyber Intelligence Function

Organizations in this category have begun to conduct functional analysis and may be conducting some strategic analysis. The organization may have some processes, stakeholders, and lines of communication identified, but continues to refine.

### Leadership Experience:

The organization's cyber intelligence leadership is mindful of both security and business operations. Leadership is accustomed to refining business processes and supporting established lines of communication throughout business units to aid in analyst collaboration.

### Tools & Technical Proficiencies:

Analysts in this organization are proficient with multiple tools and technical areas including:

- Data aggregators
- Social media monitoring
- Basic malware analysis
- Link analysis tools
- API injests
- Historical databases and reports
- Automation of functional data analysis (Splunk, Fire Eye)

### Analyst Experience:

This organization has an established cyber intelligence process with analysts conducting both strategic and functional analysis. Bi-directional lines of communication have been established with the security operations function and optimize intelligence gathering by sharing indications and warnings and utilizing trend and incident response data for analysis. Often the most labor intensive functions are outsourced to other organizations. The organization employs at least two analysts, with one analyst focused on strategic analysis and one analyst focused on functional analysis. Generally, these analysts have 5-10 years of experience and are proficient in multiple technical areas, but not an expert at any one subject. It's important for analysts to have domain and adversary expertise and be able to think strategically – positioning cyber into the context of the organization's mission.

## Adbvanced Cyber Intelligence Function

Organizations in this category recognize the need and value of a cyber intelligence program. The organization has clearly defined stakeholders and lines of communication. Processes are defined and appropriate.

### Leadership Experience:

The organization's cyber intelligence leadership drives the production of comprehensive intelligence. While the leadership is influenced by their technical expertise their focus is on risk to the business. Leadership is accustomed to executing established business processes and supporting external analyst collaboration across multiple sectors.

### Tools & Technical Proficiencies:

Analysts in this organization are proficient with multiple tools, mostly targeted to data correlation and technical areas including:

- Social media monitoring
- Supply chain analysis
- Comprehensive malware analysis
- Historical databases and reports
- Access to partner records (DHS, Red Sky, etc.)
- Automation of functional data analysis, Splunk, Fire Eye, etc.)

### Analyst Experience:

This organization has an established cyber intelligence process and most analysts are technical subject matter experts with a unique strategic vision regarding threats. Bi-directional lines of communication have been established with the security operations function and optimize intelligence gathering. This team is able to perform trend analysis and produce predictive, actionable products tailored to their stakeholders.

The organization employs at least five analysts, with analysts focused on strategic and functional analysis. Generally, the team is comprised of multiple subject matter experts with the ability to think strategically. Given the team's expertise and established processes, this organization's environment is ideal for growing junior staff.

### Indicators of Success

- Organizations are able to determine a profile that best describes them, either by indications of targeted attacks or by cyber footprint.
- Organizations starting a new cyber intelligence function are able to identify/craft the objective for the function.
- Organizations are able to utilize the guidance on key competencies, skills, and traits of an intelligence analyst to craft job descriptions and hire analysts needed to support the cyber intelligence function.
- Organizations are able to utilize the guidance on leadership to identify and hire the best person to lead the cyber intelligence function.
- Organizations are able to utilize the guidance on analyst experience and tools and technical proficiencies to identify the most competent staff and the tools needed to support successful analysis.
- Organizations are able to determine the progression path of their cyber intelligence function and use the guidance provided to identify the leadership experience, analyst experience, tools, and technical proficiencies to advance their cyber intelligence capabilities.