Introduction to

CYBER WORKFORCE DEVELOPMENT

CYBER-CHAMP AT A GLANCE

Executive Summary

Widespread cybersecurity talent shortages and skill gaps within the current workforce make it difficult for organizations to perform essential security functions. Over the last 10 to 20 years, securing information technology (IT) systems has been a priority for organizations. However, because technology is advancing so fast, all aspects of security are becoming more critical to business success. A few of these aspects include physical, IT, operational technology (OT), Internet of Things (IoT) and more.

Adversaries are aware of this increasing cyber footprint and are multiplying their cybersecurity attacks. An example of this might be a remote attack on an IT access control system that unlocks the front doors of an organization, compromising its physical security. With physical access adversaries can compromise industrial control systems (ICS) and their OT components because of a weak password on a building monitoring device. Operational technology and ICS systems are perfect targets for cybersecurity attacks because they could cause loss of life, physical injury, financial loss, damage to national security and impacts on public health. This security convergence requires that cybersecurity be looked at through a new lens. Rather than the more traditional view of cybersecurity being the sole responsibility of the IT department or chief information security officer, the responsibility for cybersecurity must be shared by everyone. This can be done through increased cybersecurity education, training and awareness based on an individual's roles and responsibilities within the organization.

Workforce development has many meanings depending on the lens through which it is viewed. Since 2003, Idaho National Laboratory (INL) has engaged in ICS/OT training programs. Since 2018, the Cybersecurity and Infrastructure Security Agency has asked INL to focus on research to better understand, define and standardize the cyber workforce development pipeline. This work has identified many cyber workforce development issues. This understanding has come from outreach, and direct engagement with industry, academic and government partners worldwide. As a direct response to this work, INL has identified the need for a methodology that can help organizations realize and resolve cyber workforce gaps.

The methodology INL has created is called Cybersecurity Competency Health and Maturity Progression, or Cyber-CHAMP. It is a framework, process, and collection of tools used to produce tailorable engagement plans to improve an organization's cyber workforce development. These engagement plans implement researched and validated workforce development business tools. Cyber-CHAMP can incorporate a wide variety of regulatory or nonregulatory cyber standards, models and frameworks. These can be national, international or voluntary. As a process, it will work for organizations of any size, type or industry sector. It is designed to help each organization understand and learn how to perform cyber workforce development according to their needs. As a set of tools, Cyber-CHAMP is built into four distinct software products, which are known as modules. They can be deployed individually, in series and as business needs dictate. The results of a Cyber-CHAMP engagement are organizational tools, metrics, measurements and road maps for cyber workforce improvement. This document will explain each piece of the Cyber-CHAMP model.

CYBER-CHAMP IS A FRAMEWORK, PROCESS, AND COLLECTION OF TOOLS USED TO PRODUCE TAILORABLE ENGAGEMENT PLANS TO IMPROVE AN ORGANIZATION'S CYBER WORKFORCE DEVELOPMENT.

INL Idaho National Laboratory

Cyber Workforce Development Structure

This document focuses on how an organization can use the Cyber-CHAMP framework, processes and tools to accomplish strategic business initiatives. The document covers the critical components of a Cyber-CHAMP workforce development evaluation. It highlights organizational security maturity targets and measured competency alignment for the organization and its individuals. The results of a Cyber-CHAMP assessment can deliver the business information an organization needs to understand and improve its security maturity.

These specific results are:

1. Understanding the organization's current cyber hygiene.
2. Understanding who is responsible for cyber tasking and duties.
3. Understanding organizational adjustments that may need to take place.
4. Understanding training recommendations for employees at all levels.

The results mentioned above can help an organization build a workforce that is more aware, competent and cyber-ready. To summarize, it is critical to view Cyber-CHAMP as a business management tool that takes the complex issues of cybersecurity workforce development and breaks them down into specific processes.

FRAMEWORK

Cyber-CHAMP is a framework built into two sections that work together to measure, track and improve the security maturity and competency of any organization. The first section, security operational readiness, as seen on the left side in Figure 1, helps organizations pinpoint where to start improving their cybersecurity program. The resulting measures for cybersecurity hygiene are measurements in observed security practices, documented plans and policies, and security program strategic direction.

PROCESS

Cybersecurity work roles, accompanying tasks, skills and knowledge are unique to every position. Organizations need help to achieve proper levels of operational readiness to detect, respond and mitigate cybersecurity vulnerabilities. This guide will walk stakeholders and future cyber champions through a surface-level, step-by-step process to implement Cyber-CHAMP in their organization.

CYBER-CHAMP IS A FRAMEWORK BUILT INTO TWO SECTIONS THAT WORK TOGETHER TO MEASURE, TRACK AND IMPROVE THE SECURITY MATURITY AND COMPETENCY OF ANY ORGANIZATION.

Once cyber hygiene results are obtained, cyber competency alignment can be measured for the organization and its individuals from a security maturity perspective. This measurement is called competency health and it is the second section of the Cyber-CHAMP framework, shown on the right side of Figure 1. It is measured holistically by the organization, individually by technical contributors, and by those in leadership and management positions. More of these details can be found below in the Products/Tools section of this document. It is important to note that each piece of Cyber-CHAMP is built from several well-known models, frameworks and a lot of research. Having a framework allows the continual application and modification of pieces within the model. It is critical to understand that these two sections play together. See the Cyber-CHAMP Technical Guide for more details.

A game board illustrates the process of a Cyber-CHAMP engagement. There are five phases of the overall process. These are pre-engagement, engagement planning and development, engagement, results, and continuous monitoring. Each phase should ideally be completed in order as shown in Figure 2.

Figure 1: *Cyber-CHAMP framework.*

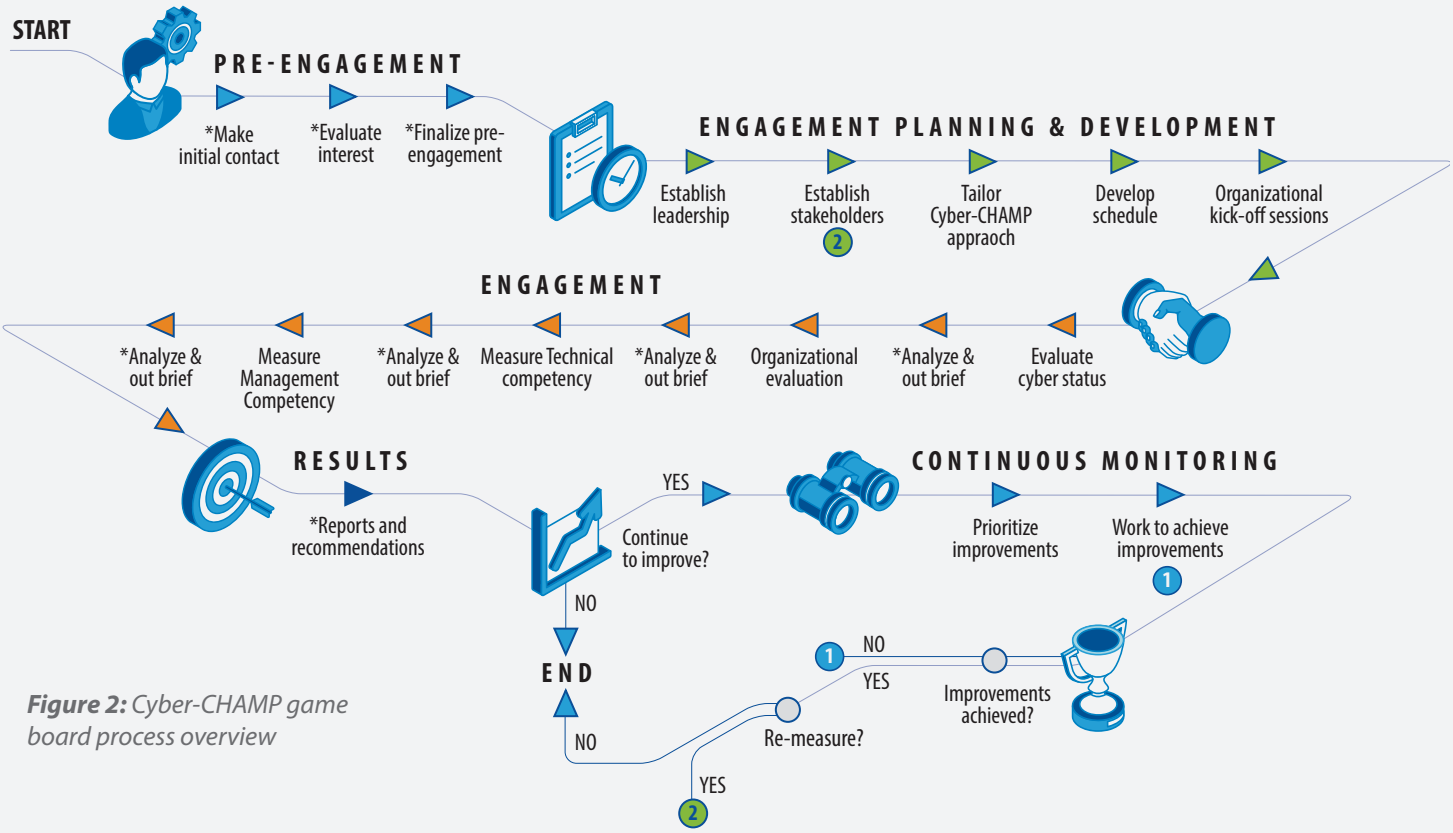

Figure 2: *Cyber-CHAMP game board process overview*

PRE-ENGAGEMENT PHASE

The pre-engagement phase has three steps. These are: make initial contact, evaluate interests and finalize pre-engagement. In the pre-engagement phase, the extent of the organization's interest in having a Cyber-CHAMP engagement is determined before moving on to the engagement planning and development phase. Organizations must complete all necessary documents in the pre-engagement phase before moving on.

ENGAGEMENT PLANNING AND DEVELOPMENT PHASE

The engagement planning and development phase has five steps. These are: establish leadership, establish stakeholders, tailor Cyber-CHAMP approach, develop schedule and organizational kick-off session(s). In this section, the organization receives guidance from the engagement personnel about assembling a leadership team. The leadership team then compiles the information necessary to build an organizational profile. Then the organizational profile is built. Once the organizational profile is complete, the leadership team elects the organizational champion. The engagement team then trains the organizational champion in their roles and responsibilities for a Cyber-CHAMP engagement. The champion then identifies and recruits the necessary stakeholders. The champion, leadership team and any other stakeholders chosen collectively become the facilitation team. A Cyber-CHAMP approach for the organization can then be created, tailored and briefed to the stakeholders. A schedule for each subsequent step is then laid out into a timeline based on the organization's needs and resources.

ENGAGEMENT PHASE

The engagement phase has eight steps that are broken up into four separate modules. These modules are: evaluate cyber status, organizational evaluation, measured technical competencies, and measured management competencies. Each module has two steps. The first step is measuring and recording unique characteristics of the organization as outlined by each module. The second step involves analyzing, delivering a report, and giving an out-brief on the findings of each module. Each module is a process with a corresponding tool utilized to evaluate and assess the organization's cyber maturity and competency.

RESULTS PHASE

The results phase has one step, reports and recommendations. By this phase, the organization has gathered a lot of valuable data. This data now needs to be organized in a way that helps management make informed decisions on improvements moving forward. This will help increase the organization's strategic direction and alignment toward its overall goals.

CONTINUOUS MONITORING PHASE

The continuous monitoring phase has two steps. These are, implement improvements and work to achieve improvements. With a completed run through of the Cyber-CHAMP process, baseline measures for cybersecurity maturity, organizational alignment, and individual competency are established. From these baselines, a road map for improvement, with specific focus areas, can be identified for strategic risk management. The identified improvement now need to be prioritized and executed. By engaging in continuous monitoring, the organization's return on investment from the money spent on improvements can be assessed.

PRODUCTS / TOOLS

There are multiple products and tools used to complete Cyber-CHAMP, the majority of which are utilized during the engagement phase. The Trust module evaluates cyber status. The Org module evaluates the organization evaluation. The Tech module measures individual technical competencies. The Mgmt module measures individual management competencies. Please see Figure 3 below for reference.

Conclusion

The evolution of technology is making security increasingly difficult to achieve by the hands of just a few. From a security perspective, the convergence of IT and OT requires more hands on the deck. Cyber-CHAMP is both a workforce development framework and a business tool that helps organizations understand their current security posture and how it can be improved. This in turn helps management make better business decisions on how to achieve strategic direction. Cyber-CHAMP evaluations identify skills gaps that exist within an organization's workforce and provide individualized training plans to help close those gaps.

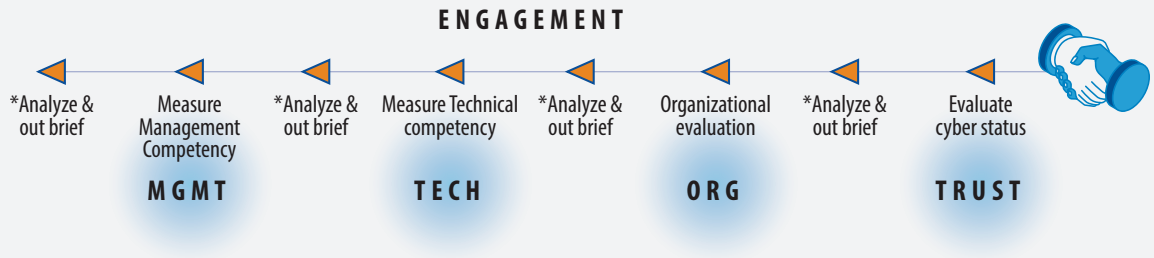

Figure 3: *The four modules of the engagement phase*

23-50417

Idaho National Laboratory