INL/MIS-22-70213-Revision-0

Cyber-CHAMP White Paper

March 2023

Sarah Pearl Lusk, Shane Dale Stailey

Changing the World's Energy Future

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

INL/MIS-22-70213-Revision-0

Cyber-CHAMP White Paper

Sarah Pearl Lusk, Shane Dale Stailey

March 2023

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

WHITEPAPER

Cyber-CHAMP

Org Module Guide

Made with VISME

Copyright 2021 Battelle Energy Alliance, LLC

NOTICE: This documentation was prepared by Battelle Energy Alliance, LLC, hereinafter the Contractor, under Contract No. AC0705ID14517 with the United States (U. S.) Department of Energy (DOE). NEITHER THE UNITED STATES NOR THE UNITED STATES DEPARTMENT OF ENERGY NOR THE CONTRACTOR MAKES ANY WARRANTY, EXPRESS OR IMPLIED, OR ASSUMES ANY LIABILITY OR RESPONSIBILITY FOR THE USE, ACCURACY, COMPLETENESS, OR USEFULNESS OF ANY INFORMATION, APPARATUS, PRODUCT, OR PROCESS DISCLOSED OR REPRESENTED THAT ITS USE WOULD NOT INFRINGE PRIVATELY OWNED RIGHTS.

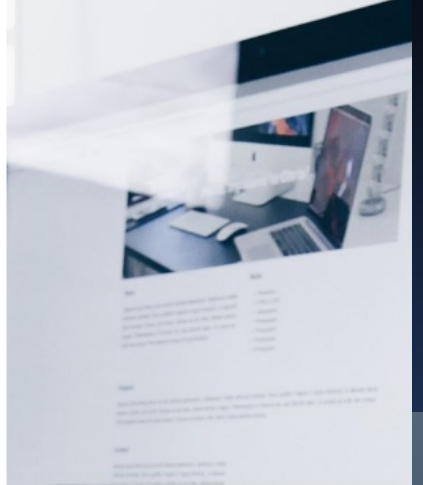
Made with VISME

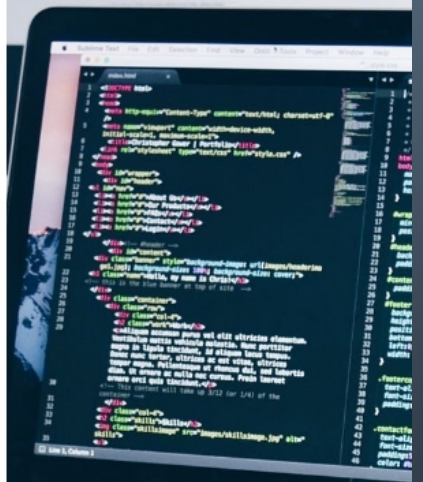
Table of Content

Made with VISME

Overview

Worldwide there is a tremendous shortfall in the cybersecurity workforce. By 2021, researchers have forecasted a deficit of 3.5 million cyber professionals. As workforce capabilities diminished, the world's cybersecurity threats have continued to multiply. Industrial control systems (ICSs) and their operational technology (OT) components became more vulnerable to attack and compromise. When an ICS is compromised, attackers can cause widespread impacts on national security, public health, and safety. This capacity makes ICSs attractive targets, with 90% of surveyed OT organizations reporting a damaging cyberattack in the last two years. To address the risk to ICSs, personnel must be competent in operational best practices and the latest threats. While frameworks for information technology (IT) cybersecurity education have





Made with VISME

How does your organization measure its cybersecurity state?

Many organizations cannot measure their ICS cybersecurity state and do not understand how to improve their personnel's OT workforce competencies. It is challenging to communicate the business case for developing a cyber-resilient workforce, even when deficiencies *have* been identified. With the ICS CYBER-CHAMP process, we can analyze individual businesses' cybersecurity maturity and workforce competency. Cyber-CHAMP can integrate data from individual business profiles to form an industry-based ICS cybersecurity workforce profile.

Made with VISME

Cyber-CHAMP Org Module

Cyber-CHAMP Model

The Cyber-CHAMP model is built to be performed and applied at the practitioner level, accounts from many technical (e.g., information, technology, cybersecurity) and managerial roles in an organization, and can be deployed by any size or type of organization. This model is based on sections and improvement categories, measurement areas, outputs, and results.

Mapping workforce roles

Cyber-Competency, Health, and Maturity Progression (Cyber-CHAMP) offers a holistic approach for IT and OT by bridging the ICS cybersecurity competency gap. ICS Cyber-CHAMP consists of five phases, one of which is creating an ICS cybersecurity workforce profile. Creating the ICS cybersecurity workforce profile includes mapping workforce roles and responsibilities to ICS functions and competencies.

Organizational competency health analysis

Cyber-CHAMP has carefully designed organizational competency health analysis to help organizations see problem areas within their cybersecurity team. The analyses help locate these problem areas and provide resources to improve the organization's defense against cyber-attacks. Once these holes are established, cyber-CHAMP provides up-to-date training resources that help build the organization's cyber professional skill sets for their specific job role and eradicate cyber security weak points.

The Org Module takes the data provided by an organization's cybersecurity professionals. It determines which job working groups and attached roles are responsible for cyber competencies. Researching the organizational STAE (Security Education, Training, and Awareness) program and comparing this to the NIST 800-50 models to discuss and provide the opportunity to align to cyber training best practices and recommendations.

Made with VISME

Mapping of workforce structure to security maturity and workforce competency levels

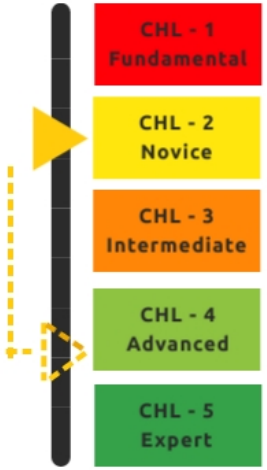
Cybersecurity Operational Readiness Maturity Level	ML-1	ML-2	ML-3	ML-4	ML-5
Security Competency Function	Awareness	Support	Maintain	Implement	Design
Engineering and Communications	X	X	X	X	X
Operation Technology	X	X	X	X	X
Management	X	X			
Support Staff	X	X	X		
Cybersecurity	X	X	X	X	X
IT Staff	X	X	X		

Made with VISME

Org, Risk, and Tech Module Metric/Measurement(s)

Based on the data provided in the organizational competency health analysis, your organization will be rated on a scale of one to five. One being poor or basic knowledge and five being expert knowledge. Cyber-CHAMP process life-cycle evaluation(s) 1-2 year. Increased competency health produces a significant gain in organizational security readiness, which impacts cyber hygiene and organizational cybersecurity functional level.

Individual and organizational measurements



CHL - 1 Fundamental

Basic Knowledge - The individual/organization has a common knowledge or an understanding of basic ICS cybersecurity techniques and concepts.

CHL - 2 Novice

Limited Experience - The individual/organization has ICS cybersecurity level of experience gained in a classroom and/or experimental scenarios or as a trainee on-the-job. Need help with most skills.

CHL - 3 Intermediate

Practical Application - The individual/organization can complete ICS cybersecurity task with competency as requested. Help from an expert is required at times but is usually performed independently.

CHL - 4 Advanced

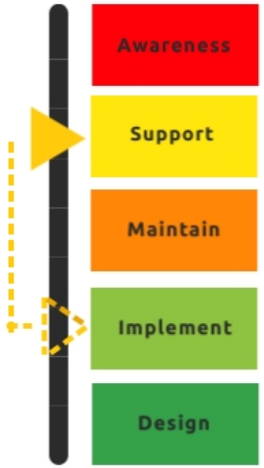
Applied Theory - The individual/organization can successfully complete ICS cybersecurity tasks with competency as requested. Help from an expert required at times, but usually perform independently.

CHL - 5 Expert

Recognized Authority - The individual/organization functioning as an expert in ICS cybersecurity and can provide strategic guidance, troubleshoot, and answer questions related to the ICS cybersecurity with expertise.

Made with VISME

Individual measurements



Awareness - Represents individuals who only need a level of cybersecurity concepts and understanding that are cognizant in nature. Contain simple knowledge or perceptions of security concepts.

Support - A knowledge of foundational security concepts and entry-level technical skill sets. An individual at this level may also have some tactical break-and-fix responsibilities.

Maintain - Competency is founded on functional security concepts. An individual can address tactical breaks, fix situations, and take a proactive, supportive role in identifying department technical needs.

Implement - Peers and leadership often consider these employees as SMEs in their field. They express complex technical concerns; ts effectively and are responsible for identifying technical needs across the organization.

Design - Individuals that understand the big picture and how actions affect system interoperability. Demonstrate strong presentation skills, possess strategic-planning skills, and manage large projects.

Conclusion

Organizational analyses and change recommendations reduce risk and increase cyber resilience. The more the different organizational elements work together, the better they can process information quickly and make inferences.

- **Cyber-informed business execution**: Security operational readiness measurements and competency progression metrics allow for improved business risk management/mitigation.
- **The cyber-aligned accomplishment of business aims and aspirations**: Organizational structure and education/training program are aligned for supporting cyber competency progression.
- **Cyber-competent business functions**: Organizational/Individual cybersecurity competencies and gaps are identified.
- **Cyber-ready workforce supporting information/operational support and connectivity**: Implementing education, training, and experience profiles to support all business systems with appropriate cybersecurity levels.
- **Cyber-ready business policy and plans**: Long-term monitoring of operational security readiness and competency progression milestones established and reflected in security policy and plans.

Cyber-CHAMP will help your organization achieve its security maturity level target by increasing your organizational security readiness. Provide continuous monitoring of plans and policies to increase your business's resilience. Developing and managing profiles will reduce organizational cyber risk. You maximize insurability and minimize supply chain risk by working to manage risk.

Organizations' competency paths and role alignments to industry standards will be updated and informed of the competency requirements needed to achieve desired security maturity. Cyber-CHAMP will provide technical and RISK management cyber training, education mapping, and work with you to increase your organization's ability to obtain and maintain a cyber-ready workforce. Individual training mappings form risk and learning profiles for an organization. These organizational risk and learning profiles combine to form sector profiles.

Made with VISME

Made with VISME

WHITEPAPER

Made with VISME