



Cyber-CHAMP

A Cybersecurity Competency Health and Maturity Progression Framework

Most believe that cybersecurity's major problem is technical. However, human error most often causes the need for cybersecurity to protect systems. This means people are the biggest cybersecurity vulnerability.

In workforce development, the biggest gap is determining an organization's cybersecurity needs, optimal structure and a continuing education process necessary to develop and maintain a cyber-ready workforce.

The Cyber Competency Health and Maturity Progression Model (Cyber-CHAMP) was developed at Idaho National Laboratory to help organizations understand what they don't know and direct their cybersecurity resources.

BECOME INFORMED

The Cyber-CHAMP framework is a process that an organization can use to discover and establish a security target and training plan. The framework is divided into four modules that look at an organization's strategic alignment, security culture and workforce competencies.

The framework establishes a security target by performing the Trust module, which helps create strategic alignment between security initiatives and business goals. This module can be customized to follow specific energy or industry standards.

Once the security target is known, the next step in Cyber-CHAMP is to perform the Org module, designed to help the organization fully understand its security culture and cybersecurity needs.

Finally, with a solid understanding of business-aligned cybersecurity goals and a list of roles and responsibilities required to reach these goals, an organization can begin the Tech and Management modules to understand its workforce competency needs on an individual level.

Cyber-CHAMP builds security awareness, education, training and workforce competencies from both the business and individual perspective.

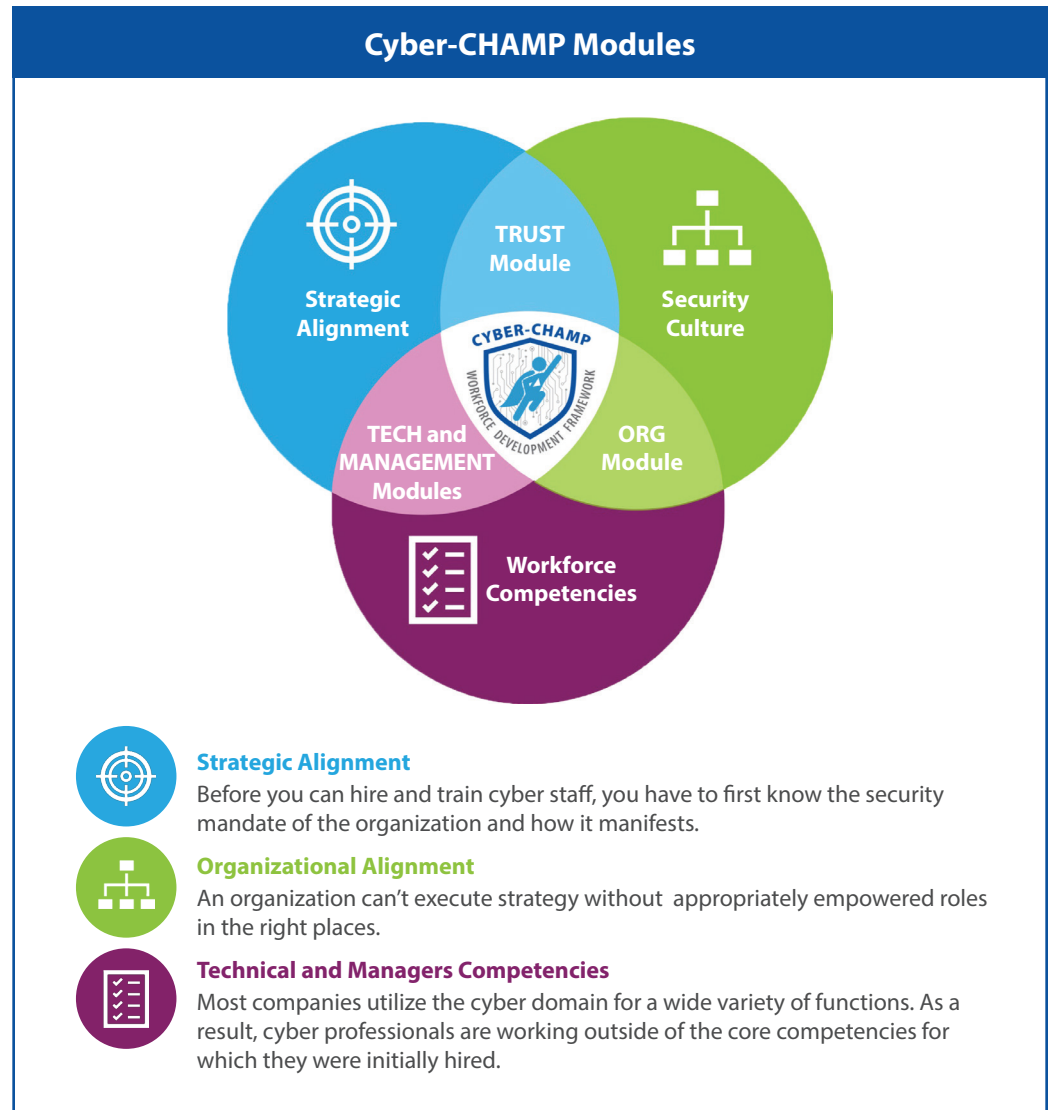
BENEFITS IN PRACTICE

This framework provides security learning pathways and priorities from the sea of available trainings and certifications. Cyber-CHAMP aligns managers and employees, while informing

human resource professionals on cyber roles and how to recruit for them. This understanding allows Human Resources and Managers to better assign job roles to cybersecurity positions. Using the Cyber-CHAMP framework, organizations can deconstruct their needs

and prioritize learning that provides cybersecurity skills to align with the organization and its standards of practice.

Battelle Energy Alliance manages INL for the U.S. Department of Energy's Office of Nuclear Energy.





FOR MORE INFORMATION


Technical contact
Shane Stailey
 208-526-1201
shane.stailey@inl.gov

Media contact
Ethan Huffman
 208-526-5015
ethan.huffman@inl.gov

www.inl.gov

- 

Strategic Alignment
 Before you can hire and train cyber staff, you have to first know the security mandate of the organization and how it manifests.
- 

Organizational Alignment
 An organization can't execute strategy without appropriately empowered roles in the right places.
- 

Technical and Managers Competencies
 Most companies utilize the cyber domain for a wide variety of functions. As a result, cyber professionals are working outside of the core competencies for which they were initially hired.

A U.S. Department of Energy
 National Laboratory

