

WORKFORCE DEVELOPMENT

IDENTIFYING NEEDS

- Identify your workload requirements.
 - Evaluate the complexity of your operations and the speed with which actions need to be executed.
 - Consider surge capacity needs and whether advanced technologies can help reduce the attack surface.
- Identify your workforce requirements.
 - Consider the competency, flexibility, and agility of the cybersecurity workforce in your organization.
 - Identify ideal reporting structures and highlight where multi-functionality is preferable.
- Define the required knowledge, skills, abilities, and competency of your workforce based on the roles they occupy and the business functions they support.
- Identify critical gaps in your organization's existing cybersecurity workforce.
 - Employ existing tools such as the NICE framework to guide internal assessments of roles and responsibilities.

IMPROVING EXTERNAL RECRUITMENT

- Strengthen job postings by writing clear, internally consistent job descriptions.
 - Use existing tools such as the NICE framework to highlight relevant skill sets.
- Gather data on recruitment through the application process, capturing types of applicants and previous work experiences.
 - Systematize data collection and share throughout company to prevent silo formation and support talent sourcing and development.
 - Evaluate recruitment data periodically to identify gaps in outreach.
- Rely on multiple indicators to assess candidate potential.
 - Consider implementing systematized hiring assessments.
 - Evaluate relevant degrees, certifications, and work experiences.
 - Avoid relying on one specific metric (e.g., a masters-level degree in engineering) when making hiring decisions.

ADVANCING INTERNAL TRAINING AND DEVELOPMENT

- Develop career maps that highlight advancement tracks for your cybersecurity workforce
- Identify pathways within your organization for retraining and repositioning talented staff into cybersecurity roles.
 - Consider potential nontraditional entry points into cybersecurity based on interest and ability.
 - Expand upskilling and retraining programs and incentivize transitions within your organization.
- Encourage internal training and independent learning.
 - Open opportunities for continued education and skill certification.
- Track data on workforce retention.
 - Evaluate retention data periodically to identify whether training and development programming is meeting employee needs.

Fundamental Approaches

Consider the following strategic approaches when developing a cybersecurity workforce.

1. **Expand the supply pipeline** producing new talent.
 - Do you have relationships with universities and technical colleges?
 - Do you offer cybersecurity internships or apprenticeships?
2. **Identify and match existing supply** with talent openings.
 - Is your human resources department effectively translating required skills into posted job descriptions?
3. **Retrain existing staff** to become part of the cyber workforce.
 - Is your organization leveraging existing talent by shifting resources to its cyber workforce?
4. **Reduce the demands** on your cyber workforce through technological innovation.
 - Do you have agreements with third-party service providers to create surge capacity during critical periods?
5. **Improve retention** of the current workforce.
 - Is your organization investing in talented team members?
 - Does your organization allow interested individuals to explore careers in cybersecurity?