FUNDAMENTAL APPROACHES TO CYBERSECURITY WORKFORCE DEVELOPMENT

☐ Expand the supply pipeline.
  • Does your organization have relationships with universities and technical colleges?
  • Do you offer cybersecurity internships and apprenticeships?

☐ Identify and match existing supply with talent openings.
  • Is your human resources department effectively translating required skills into posted job descriptions?

☐ Retrain existing staff to become part of the cyber workforce.
  • Is your organization leveraging existing talent by shifting resources to its cyber workforce?

☐ Reduce the demand on your cyber workforce through technological innovation.
  • Do you have agreements with third-party service providers to create surge capacity?

☐ 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?

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 attack surface.

☐ Define the required knowledge, skills, abilities, and competency of your cybersecurity workforce based on the business functions they support.

☐ 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.

☐ 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.
**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 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 programs are meeting employee needs.
- Improve opportunities for continued education and skill certification.

**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.
  - Systematize data collection and share throughout the 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 when making hiring decisions.
- Gather data on recruitment through the application process.
  - Systematize data collection and share throughout the company to prevent silo formation and support talent sourcing and development.
  - Evaluate recruitment data periodically to identify gaps in outreach.

CarnegieEndowment.org