CYBER SECURITY LABOR SHORTAGES AND SKILL GAPS

CRITICAL INFRASTRUCTURE PROTECTION

HSI Industrial Skills — Reliability Matters

Key Observations

Industry Challenges

– The shortage of cyber security professionals has risen by 12.6% annually

REPORTED BY **70%** OF POWER ORGANIZATIONS – **CYBER SECURITY STAFF SHORTAGE**

CURRENT THREAT LANDSCAPE IS VIEWED BY **79%** OF ORGANIZATIONS AS THE **MOST CHALLENGING** IN THE PAST FIVE YEARS

Impact on CIP Reliability Standards

– Noncompliance is often linked to staff turnover and ineffective transition planning

– Insufficient resources and tools for new and existing staff to manage complex security needs

Challenges

Large Entities

– Complex systems and multiple roles create challenges in defining responsibilities and ensuring effective management

– Examples of failures include inadequate password management and failure to inventory accounts

Small Entities

– Limited resources can lead to disruption from the loss of a single employee

– Less capacity to manage all aspects of cyber security

Suggestions for Improvement

Reassess HR Strategies

Enhance recruitment efforts and improve employee retention strategies

Resource Allocation

Ensure adequate resources for implementing new processes or controls

Vendor Technology

Engage appropriate personnel in vendor training and demonstrations

Create Commonalities

Standardize processes and technology across departments to increase staff versatility

Develop Talent

Mentor staff from within or hire and train new employees

Strategically outsource time-intensive tasks to better use staff core skills

Succession Planning

Develop and document detailed succession plans for key staff roles

Implement both **short- and long-term** plans to manage critical tasks

Leverage NERC Resources

Use available **training**, **workshops**, **webinars**, and **best practices** to enhance security and compliance skills

hsi

Based on the NERC report: **Critical Infrastructure Protection Themes and Lessons Learned**, released August 2024.