LATENT VULNERABILITIES

CRITICAL INFRASTRUCTURE PROTECTION
HSI Industrial Skills — Reliability Matters

Key Observations

Emergence of Latent Vulnerabilities

– Long-standing, higher risk issues evade detection, including inadequate monitoring and improper access management

Improved Internal Controls

– Entities have improved cyber security and internal controls

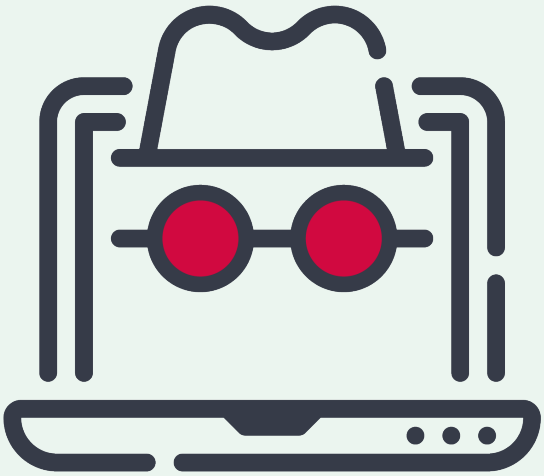
EXAMPLE 1
Physical Security
Ineffective alarm configurations left physical access points vulnerable

EXAMPLE 2
Electronic Access Failures
Unauthorized users accessing sensitive information due to failure of access controls

EXAMPLE 3
Shared Accounts Issue
Multiple users with unauthorized backend access due to a lack of understanding of the system's technical architecture

EXAMPLE 4
Patching Issue
Incorrect patch source identified

Suggestions for Improvement



Enhance Detective Controls:

– Allocate resources for developing, testing, and executing detective controls
– Ensure alarms and alerts function correctly

Conduct Regular and Sufficient Testing of Detective Controls:

– Test to ensure alarms and alerts from substations function from end-to-end

Periodically Scrutinize Design of Existing Controls:

– Think about scenarios the controls may not address

Conduct Appropriate Internal Audits and Assessments

– Perform targeted internal audits and assessments
– Train internal experts to search for latent vulnerabilities
– Use peer reviews to identify overlooked issues

Leverage Security Assessments:

– Use internal vulnerability assessments, third-party security assessments, and penetration testing to detect and correct vulnerabilities

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