COMMON FINDINGS IN OT CYBERSECURITY VULNERABILITY ASSESSMENTS

Lessons learned from thousands of on-site vulnerability assessments in OT environments

INTRODUCTION

Operational technology environments are increasingly targeted by cyber threats — and the most impactful risks are often hidden in plain sight.

Cyber breaches often begin with something small: an old computer tucked in the corner of a control room, a switch installed years ago and never updated or a shared password written on a sticky note near a terminal. These seemingly minor oversights can create significant risk to operational technology (OT), where every system is connected to production, safety and continuity.

Just a few years ago, many organizations paid little attention to cybersecurity. Today, companies across industries are prioritizing it and investing in risk assessments, skilled personnel, training and technology to enhance their cybersecurity posture.

Honeywell's professional services team conducts hundreds of Cybersecurity Vulnerability Assessments (CSVAs) each year across a broad range of settings — from industrial sites, such as chemical plants and refineries, to commercial facilities, including airports and hospitals. Every environment is unique, and cybersecurity strategies must be tailored to each site's specific operating conditions.

HONEYWELL RECOMMENDS CONDUCTING CSVAs ANNUALLY

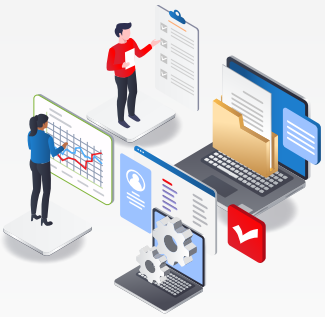
Regular assessments don't just identify vulnerabilities — they create a repeatable baseline that helps organizations measure progress, adapt to evolving threats and align cybersecurity investments with operational priorities.

WHAT IS A CSVA?

Provides a structured, risk-based understanding of an OT environment's cybersecurity posture so organizations can make informed, defensible decisions.

A CSVA is a holistic evaluation that examines weaknesses across three core areas: people, process and technology. It provides a comprehensive view of potential risks by assessing policies and procedures, physical and environmental security, network architecture, access control and asset vulnerabilities.

TYPICAL CSVA PROCESS



Collect data

Gather information on systems, network diagrams, policies, procedures, enforcement controls, assets, patches, firewall configurations, vendor access and more.

Identify weaknesses and vulnerabilities

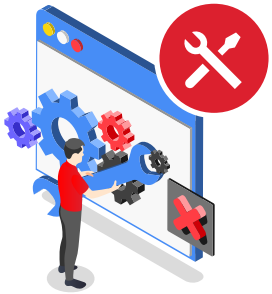
Analyze data and map findings to cybersecurity standards such as IEC 62443, NIST 800-53 Rev. 5, and NIST 800-82.

Develop priority remediations

Rank vulnerabilities by risk level and criticality to guide targeted mitigation and investment decisions.

CSVA Lifecycle

The CSVA lifecycle is a continuous, risk-driven approach to protecting critical applications and the infrastructure they support. Built on constant visibility and decisive action, the lifecycle enables organizations to identify, prioritize and close security gaps before they can threaten physical safety, operational uptime or business continuity. Rather than a one-time assessment, it's an evolving process that strengthens resilience as threats, technologies and operational demands change.



Maintain

Sustain improvements over time through governance, monitoring, documentation and periodic reassessment as threats, technologies and operations evolve.

Assess

Establish a clear baseline by identifying vulnerabilities, gaps and risks across people, processes and technology using industry-recognized cybersecurity standards.

Remediate

Prioritize and address identified risks through targeted actions that reduce exposure while balancing operational constraints, safety and business objectives.

The Power of Visibility

In complex sites, risk arises from how diverse systems, key operational components, and connected assets interact across the environment. A CSVA provides visibility across the entire operation, revealing hidden vulnerabilities and dependencies.

Typical Site Layout: International Airport

30 Buildings	**5** Control Rooms	**40** Servers
50 Applications	**4** Data Centers	**30** Workstations

Typical Site Layout: Chemical Plant

20 Buildings	**1** Control Room	**40** Servers
100+ Applications	**1** Data Center (1 Redundant)	**100** Operator Workstations

CSVA DELIVERABLES

A CSVA engagement typically results in:

- Detailed assessment report with in-depth analysis and tailored recommendations
- Briefing and presentation of findings for key stakeholders
- Mitigation roadmap outlining priority actions
- Optional post-engagement consultation and remediation support

CYBERSECURITY RISKS

It's critical to understand the factors that drive OT vulnerabilities.

PEOPLE

Cybersecurity vulnerabilities often originate from human behaviors and access practices. The following are common people-related findings identified during a CSVA:

- Control room doors left unlocked, allowing unauthorized physical access to critical devices
- Passwords visible or insecurely stored, such as taped onto equipment, left in plain sight or not changed from default vendor settings — often shared across multiple devices or systems
- Lack of defined access control, including outdated or incomplete lists of personnel authorized to access specific systems or areas
- Unrestricted access by vendors or internal staff to sensitive areas and devices increasing the risk of insider threats

HAVE YOU INTEGRATED PHYSICAL SECURITY CONTROLS INTO YOUR OT CYBERSECURITY STRATEGY?

Honeywell frequently observes inconsistencies in how physical access is managed, which increases the potential for cyber and insider risks.

Consider:

- How do vendors, third parties, guests and visitors gain access to your facility and critical areas?
- Are access permissions and escort requirements clearly defined and enforced?
- Are control rooms, panels and network cabinets consistently secured?
- Are security cameras and monitoring systems active and regularly reviewed?
- Are physical security policies integrated into overall cybersecurity training and procedures?

PROCESS

Cybersecurity vulnerabilities often arise from gaps in policies, procedures and operational processes. Common process-related findings include:

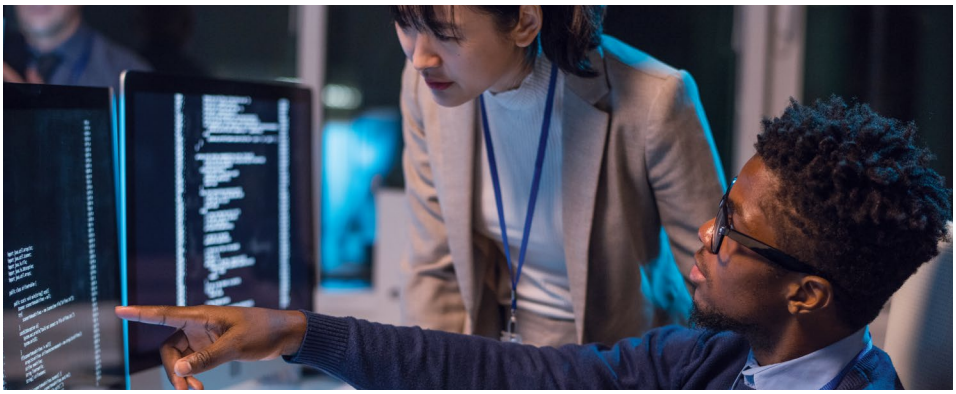
- Lack of controls for removable media, such as USBs, SD cards, keyboards and mice with unsecured ports that anyone can access
- Missing or incomplete network architecture documentation and absence of formal change management processes
- Undocumented incident response and recovery processes, leaving teams unsure of steps during a security event
- Unclear escalation procedures for remote access, including who is authorized to connect and under what conditions

DO YOU HAVE YOUR ACCEPTABLE RISK TOLERANCE QUANTIFIED?

Honeywell frequently observes undefined or inconsistent risk tolerance, making it challenging to prioritize mitigations effectively.

Consider:

- Have risk thresholds and acceptable exposure levels been formally documented?
- Are processes and controls aligned with these risk thresholds?
- Is there a consistent method for escalating and approving exceptions to policy?
- Are change management, incident response and recovery procedures regularly reviewed against the organization's risk tolerance?



TECHNOLOGY

Technology-related gaps can leave OT environments exposed to cyber threats. Common findings include:

- Multiple remote access tools from different vendors that are unmonitored and lack multi-factor authentication (MFA)
- Inadequate network segmentation, particularly for north-south traffic between OT and IT systems
- Firewall configurations need improvement, with temporary rules often left in place indefinitely
- Unmanaged Wi-Fi networks that are accessible beyond plant walls
- Lack of a comprehensive asset inventory, including firmware and patch levels
- Absence of continuous monitoring and intrusion detection capabilities within the OT network

HAVE YOU IMPLEMENTED ASSET DISCOVERY AND INTRUSION DETECTION TECHNOLOGY?

Honeywell often sees gaps in asset visibility and monitoring, leaving OT systems exposed to threats.

Consider:

- Are all OT assets inventoried and tracked for firmware, patches and configuration changes?
- Is intrusion detection implemented and monitored continuously across the OT network?
- Are unauthorized remote access tools and network connections actively identified and mitigated?
- Are firewall and segmentation policies regularly reviewed and enforced consistently?
- Does network architecture follow the Purdue Model for OT/ICS segmentation?

CONCLUSION

CSVAs help build a resilient and secure OT environment through ongoing assessment and targeted action.

CSVAs provide a critical point-in-time evaluation of your OT environment and should be conducted annually to track progress and ensure continuous improvement. Establishing a clear baseline is essential for securing remediation funding and aligning cybersecurity initiatives with leadership priorities.

Implementing CSVA recommendations can be time and resource intensive. Organizations typically follow a multiyear iteration, after which Honeywell performs a gap analysis to evaluate improvements and identify areas needing further attention. Cyber risks also evolve, so ongoing assessment is essential.

Beyond assessments, Honeywell offers a suite of complementary services to help organizations strengthen their OT security, including:

- OT penetration testing to evaluate whether your cybersecurity program can prevent or withstand a cyberattack
- Cybersecurity Hazard and Operability Study (HAZOP) assessments to understand how a cyberattack could impact operations and endanger personnel.
- Industrial network assessments to determine if your OT network is optimized to support operational requirements

By combining these services with regular assessments, organizations can proactively identify vulnerabilities, implement mitigations and build a more resilient OT environment.

Talk to Honeywell about scheduling an assessment to protect your operations and people.

Speak to an expert

For more information
www.honeywell.com

Honeywell
855 S Mint Street
Charlotte, NC 28202

THE FUTURE IS WHAT WE MAKE IT

Honeywell