White Paper

Effective Use of Assessments for Cyber Security Risk Mitigation

Executive Summary

Managing risk related to cyber security vulnerabilities is a requirement for today's modern systems that use network communications to achieve the maximum benefits from system capabilities.

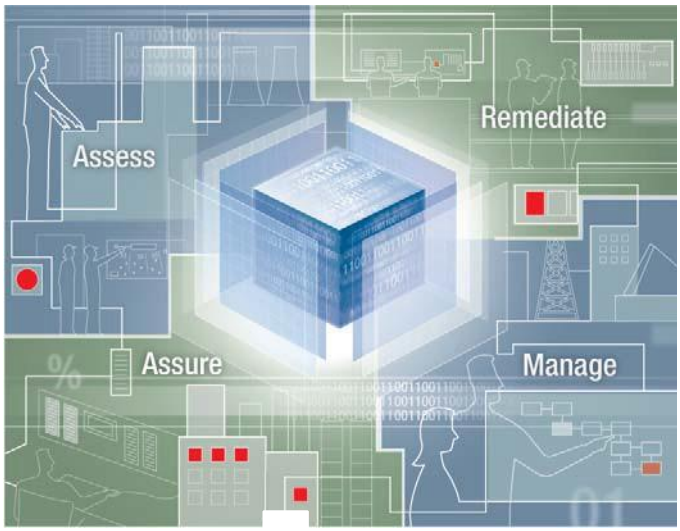
Malware intentionally or opportunistically affecting critical infrastructure is a real threat and most sites need and want an effective, manageable solution.

This paper discusses Honeywell's Cyber Security Vulnerability Assessment, the effectiveness of this type of assessment, and how it relates to the overall cycle of securing your critical infrastructure.

Table of Contents

Industrial Cyber Security

The ability to manage risk for control systems is nothing new. Industrial Cyber Security Solutions focus on protecting process industry facilities from the growing risk of industrial cyber security threats and vulnerabilities. The portfolio includes complete solutions, managed services, best practices, and support from Honeywell's global army of network and security-certified personnel that secure users' critical infrastructure and deliver a more predictable and safe environment – regardless of control system vendor or location. Often, control systems organizations find themselves insufficiently staffed to manage key elements, such as their network security program. The manpower shortfall is coupled, then, with increasing emphasis on uptime, availability, and reliability.



Industrial Cyber Security Lifecycle

The Industrial Cyber Security Lifecycle is on-going and logical in its approach, including:

- Assessing a specific area,
- Remediating any issues that are revealed,
- Continuing to manage those areas, using best practices, and
- Assuring that the system meets industry regulations or standards.

Cyber Security Vulnerability Assessment

The Cyber Security Vulnerability Assessment (CSVA) is a service that enables users to attain their security objectives, including:

- Following their industry's best practices, and
- Compliance with regulatory standards, such as ISA99, NERC CIP, CFATS, and ISO/IEC27001.

The CSVA uses a holistic approach that examines the three core facets of an organization's cyber security profile:

People	Process	Technology
• The cyber security awareness level in the organization • Adherence to existing security policies and procedures • Security program implementation training	• Current cyber security policies and procedures • Effectiveness of current policies and procedures relative to security and business requirements	• Cyber security technologies in use in the organization • The manner in which these technologies are configured and deployed

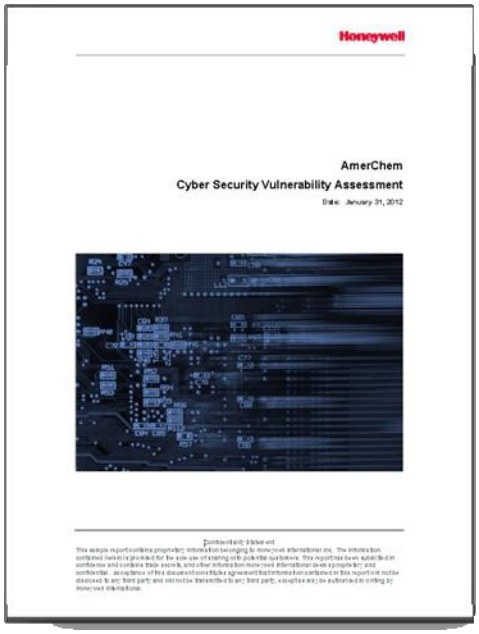
The CSVA service is performed on-site and a report is issued that contains:

- **Executive Summary** – documents the dates of the assessment, outlines the scope of the assessment, presents a summary of the findings (current risk level), and a brief summary of the Level 3 and Level 3.5 findings and recommendations, plus an overall rating for the site relative to cyber security practices.
- **CSVA Background Information** – confirms the dates of the assessment, participants, basics of the CSVA process, and information relative to previous assessments.
- **Network Design Summary** – describes the high-level design of the network architecture deployed at the site.
- **Detected Perimeters and Cyber Assets** – describes the information collected from the networks and devices, plus information collected from each cyber asset discovered.
- **Security Vulnerability Assessment** – summarizes the methods or technology used at the site and any security concerns or recommendations.

- **Findings** – describes all detailed findings that are the result of the CSVA.

Reviewing the outline of the areas addressed by the CSVA will help in understanding how effective use of the CSVA can mitigate cyber security risk. The assessment addresses:

- Good Security Practices
- Firewall Rules Assessment
- Ports and Services Assessment
- Patch Management
- Malicious Software Prevention
- Account Management
- Default Users
- Password Management
- Security Status Monitoring
- Security Logging
- Remote Administration & Management
  - Remote Interactive Access & Remote Control
  - Network Management
- Share Permissions
- Local Security Policy: Security Options


Honeywell

AmerChem

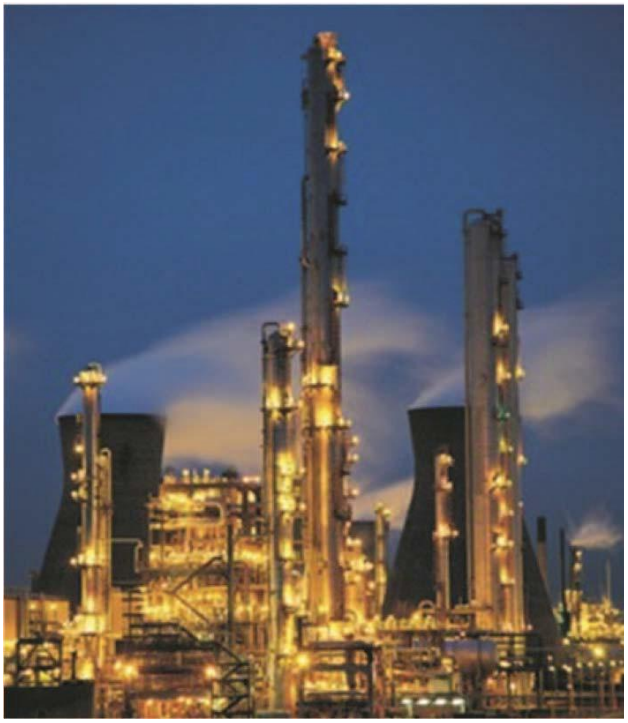
Cyber Security Vulnerability Assessment

The **Findings** section of the report relates directly to areas addressed by the assessment, with the results summarized by asset, vulnerability description, impact, likelihood of the vulnerability resulting in a security event, priority of the vulnerability, and ***actionable*** recommendations.

#	Asset(s)	Description of Vulnerability	Impact (1-5)	Likely (1-5)	Priority (1-5)	Recommendation
1	WEPEMSBOP-3	Switches do not have spanning tree feature enabled. This feature prevents communication loops from crashing the network.	2	3	3	Enable spanning tree feature
2	CEHM1-1A WEPIMARKV1 WEPITCPPLC HMI_2	All Windows machines are logged in using Administrator privilege accounts. This allows unrestricted access to the Operating System and its settings. Systems could be easily damaged by accidental or malicious user actions by anyone with access to the device.	2	3	4	Create new user accounts for the Operator's to use which is not a member of the local Administrators group. The suggested approach is a 'User' level account with restricted desktop environment only permitted to execute a minimum number of applications.
3	WEPEMSBOP-3	Switches have SNMP enabled with 'public' community string enabled. This allows unrestricted access to remotely administer the switch. The offender would have to have access to the network.	2	4	3	Disable the SNMP agent on the switches, or configure a non-default SNMP community string with a list of permitted managers.
4	CEHM1-1A HMI_2	The default guest user account is enabled, allowing anyone access to the machine locally at the console or remotely across the network without requiring login. With the default permissions of Windows, the Guest account has sufficient privilege to tamper with the Operating System.	4	4	4	Disable the guest account on all systems as it is not required for any applications.

Partial extract from sample CSVA Findings, which is included in the CSVA Report

Power Company Makes Effective Use of the CSVA in Mitigating Risks



A safety culture is ingrained in the everyday activities of power companies. These companies are very familiar with the aspects of physical security and safety in their installations. These companies are now finding that they need to extend their safety culture to embrace cyber security with the same level of focus and commitment.

Challenge

A forward-thinking US power company employed regularly recurring audits of various controls, systems and programs. However, when it came to a SCADA-based cyber security vulnerability assessment, the in-house audit team did not possess the specific combination of skill in process control experience and IT security risks. Site management realized they required a third-party expert with a unique combination of knowledge of the two worlds.

After contacting several consulting firms, the power company was unable to find a firm that was familiar with SCADA or other process control systems.

Solution

Honeywell was selected for the task due to expertise in both disciplines. The Industrial Cyber Security team possessed the experience and expertise that the power company required to review their SCADA system. The power company and Honeywell embarked on a collaborative review of the power company's process control systems and SCADA risk-assessment policies and procedures.

Results

During the risk assessment process, high-level risks were identified. This information was used to estimate, prioritize and coordinate ongoing risk-mitigation activities.

The power company received a high-quality, expert assessment with specific risk rankings to outline those areas for remediation that enabled the power company to:

- Assess their true risk,
- Abide by corporate standards for audit and review, and
- Prioritize the tasks they needed to execute.

"We needed access to cyber security experts with process control systems knowledge. Honeywell's team of experts was just what we needed to assess our SCADA system," commented the audit team lead of the US-based power company.

Gas Pipeline Operation Makes Effective Use of the CSVA in Mitigating Risks

This customer is one of the largest US-based utility companies, combining natural gas and electric utilities.

A gas utility's central control center continuously monitors flow rates and pressures at various points in its gas distribution system. Today's natural gas transmission and distribution systems are heavily dependent on computer technology, supervisory control and data acquisition (SCADA) systems to operate safely and efficiently.

Challenge

This utility company recognized the importance of the cyber security profile of its gas distribution pipeline and equipment. An operational incident underscored the need to provide better network management and data access. It had become clear that the company required unique expertise in cyber security for critical control networks.

Solution

This company had worked with Honeywell's Industrial Cyber Security team previously, and determined they needed help assessing and remediating the cyber security vulnerabilities of their gas distribution pipeline and equipment.

Results

Through the assessment, Honeywell's team documented the vulnerabilities in all facets of the customer's pipeline operation, interpreted and assessed the associated cyber security vulnerabilities, and provided a roadmap to mitigate risks. Included in this activity were:

- **Site and system assessment**—Review of particular site and system-specific vulnerabilities.
- **Policy and procedures assessment**—Review of current policy and procedure documents.
- **Compliance assessment**—Review of operations and processes against applicable compliance standards and best practices.
- **Security baseline**—Gauges progress against current status and operating model for security.
- **Risk assessment**—Identifies appropriate levels of security for each asset.

The final analysis included suggestions for improvement by order of importance, a project plan, and order-of-magnitude costs for budgetary purposes.

Going forward, Honeywell will assist the customer with further development, refining, and execution of their cyber security program.

"Thanks to Honeywell's cyber security expertise for industrial control and SCADA systems, along with its advanced assessment tools and techniques, we have addressed a wide range of potential risks to the safety, security and reliability of our natural gas distribution system," commented the SCADA Supervisor at the US-based natural gas pipeline company.

For More Information
Learn more about how Honeywell's Cyber Security Vulnerability Assessment can help to mitigate security risk at your site; visit our website www.becybersecure.com or contact your Honeywell account manager.

Honeywell Process Solutions
Honeywell
1250 West Sam Houston Parkway South
Houston, TX 77042

Honeywell House, Arlington Business Park
Bracknell, Berkshire, England RG12 1EB

Shanghai City Centre, 100 Junyi Road
Shanghai, China 20051

www.honeywellprocess.com

WP-14-01-ENG
November 2014