

# Basic Cybersecurity Assessment Service

- Identify, remediate and secure your DeltaV System from cybersecurity risks
- Aligns with Emerson's cybersecurity best practices and standards
- Qualitative report allows for the planning and execution of cybersecurity remediation solutions



*The Emerson Basic Cybersecurity Assessment Service is an integral part of Emerson's three-step approach to effective cybersecurity "best practice" implementation and management.*

## Introduction

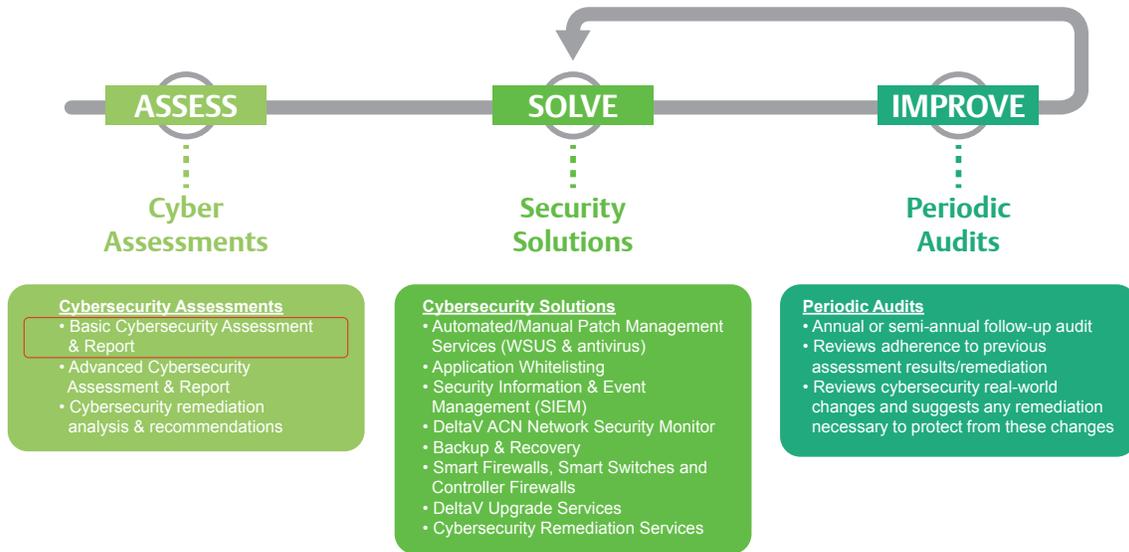
Effective cybersecurity solutions are not a "set them once and forget them" solution anymore. Every day more and more threats are launched at control systems from every direction and just knowing how malware can invade your system is but a small part of understanding how to deploy a "best practice" cybersecurity prevention system. Emerson's Basic Cybersecurity Management Service applies to Emerson DeltaV™ distributed control system (DCS), and provides expert consultation support for cybersecurity enrichment of process controls systems.

This Basic Cybersecurity Management Service is your initial control system cybersecurity review and assessment and will provide high-level insight into what parts of best practice cybersecurity standards that you have in place on your DeltaV DCS today. And, because every customer has their own

network architecture, Emerson utilizes your local DeltaV service representative to review, analyze and report back our findings on key cybersecurity best practices. Finally, we work in a collaborative framework with your site personnel to determine the best overall deployment of any Cybersecurity remediation, when necessary.

## Benefits

**Identify, remediate and secure your DeltaV System from cybersecurity risks:** The consequences of a successful breach/attack can cause serious damage to your plant, reduce or shut down production and even have safety and environmental implications. The results of this assessment will produce a report that will help guide you to some initial improvements that can be made and lay the groundwork for additional cybersecurity remediation.



**Aligns with Emerson’s cybersecurity best practices and standards:** Unaddressed control system hardening efforts, lack of effective user access policies and/or procedures, uncompleted or deferred software anti-virus and security updates and inadequate cybersecurity training for all personnel are all preventable cybersecurity vulnerabilities that have an effect on control system performance.

**Qualitative report allows for the planning and execution of cybersecurity remediation solutions:** The most basic cybersecurity assessment will form the foundation to assess and remediate cybersecurity vulnerabilities within your process control system. When considering the business value of the Basic Cybersecurity Assessment Service, the benefit of evaluating and remediating vulnerabilities that could lead to a cybersecurity breach versus the downtime costs that are associated with the discovery and removal of the breach are realized in several key areas:

- The Cost of Lost Revenue - Value of the Total Revenue lost during the cyber incident evaluation and repair period.
- The Direct Cost to Return to Operation - Cost of Unscheduled down-time, material, labor, overtime, off spec product and the start-up time required to begin operation.

## The Service

The effort to determine exactly what is required to proactively prevent an attack often can begin with a basic cybersecurity assessment at your site from your local Emerson-certified DeltaV service representative.

Emerson’s initial Basic Cybersecurity Assessment covers a wide range of cybersecurity related issues including:

- Review of the DeltaV network segmentation
- Review of existing cybersecurity policies and procedures in place
- Review of portable device policies (USB sticks, Portable CDs, etc.)
- Review of level of workstation and server “hardening” efforts (USB ports, personnel access policies, etc.)
- Review of user access policies and procedures including passwords and unused accounts
- Determination of O/S security update policies, procedures and enforcement
- Review of network physical security and perimeter protection “best practices”
- Review of data backup plans and data management procedures

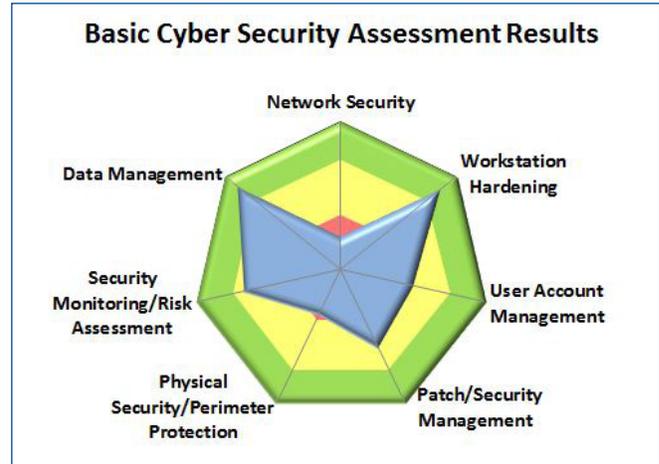
Your service representative will lead you through a series of questions/discussions aimed at determining the current state of cybersecurity readiness. These questions are grouped into 7 major categories’:

- Network Security
- Workstation Hardening
- User Account Management
- Patch/Security Management
- Physical Security/Perimeter Protection Management
- Security Monitoring/Risk Assessment
- Data Management

## The Report

Once this discussion has been completed, an analysis and findings report will be generated and reviewed with each customer. This will provide each customer with an initial assessment of the overall general cybersecurity health of that system. From there, remediation of the findings and closer assessments of specific findings will drive the next steps at any site.

Initially, a radar plot is developed from the results that will clearly show what cybersecurity elements are “in place and operational” as well as where the focus of cybersecurity remediation efforts might be directed. An example of a plot is shown below.



Within the final report, each of the seven key elements is individually explored, from what the goals were, what was covered and the specific findings. A final recommendation section focuses on the possible next step remediation for each of the findings for that section.

**Executive Summary**

Cyber security risk assessments are conducted to ensure that proper safeguards are present in the DeltaV system. The following radar chart graphically shows an overview of the cyber security readiness results for this system/site. The closer the blue plot area is to the outside edge of each of the 7 key elements, the better the results were for that section. From this chart, it should be clear which of the report elements any initial remediation focus should be on.

**Round Rock Refining**

Round Rock, TX

System ID(s) {0001-xxxx-xxx}

5/13/2014

**Overall Evaluation:**

- **Positive:** *Good results evaluation. Continue to monitor.*
  - Data Management
  - Workstation Hardening
- **Neutral:** *Results are marginal. We suggest Customer evaluate each recommendation and implement accordingly.*
  - Security Monitoring/Risk Assessment
  - Patch Security Management
  - User Account Management
- **Concerning:** *Results are of concern. We suggest Customer evaluate each recommendation as a Priority and implement accordingly.*
  - Physical Security/Perimeter Protection
  - Network Security

Page 3 of 13

**5.0 Physical Security/Perimeter Protection Section**

One level of cyber security protection is simply to prevent physical access to equipment, ensuring that controllers and network equipment are mounted in locked enclosures. Another level of security is to install security perimeters or protective *cyber fences* within and around a system. Security perimeters provide a level of defense against confidentiality, integrity and availability compromises. Switches restrict physical connectivity while firewalls control traffic flows in and out of a network.

The Physical Security/Perimeter Protection Management section deals with the cyber security related “best practice” status of policies, procedures and enforcement techniques surrounding the appropriate use of firewalls, DMZ networks, unauthorized access/availability to controllers and network equipment, as well as locking down access to workstations.

**Findings:**

- 5a. Existence of perimeter firewall security policies, procedures and enforcement are indicated.
- 5b. The DeltaV workstation equipment protection appears to be satisfactorily locked or protected per DeltaV “best practice” security standards.
- 5c. The controllers and network equipment appear to be satisfactorily locked or protected per DeltaV “best practice” security standards.

**Recommendation(s):**

- 5a. Existence of perimeter firewall security policies, procedures and enforcement are indicated.
- 5b. The DeltaV workstation equipment protection appears to be satisfactorily locked or protected per DeltaV “best practice” security standards.
- 5c. The controllers and network equipment appear to be satisfactorily locked or protected per DeltaV “best practice” security standards.

## Assessment Service Availability

The Basic Cybersecurity Assessment Service offering for Emerson Process Management DeltaV control systems is available directly from your Emerson-certified Service representative.

The Lifecycle Services portfolio consists of service modules, each designed to address specific support requirements. These modules can be combined to customize a support program for your plant that is tailored to fit just right, meeting your support needs while providing value and peace of mind.

## Ordering Information

Description	Model Number
Basic Cybersecurity Assessment Service	Please Contact Your Local Emerson Sales Office

*This product and/or service is expected to provide an additional layer of protection to your DeltaV system to help avoid certain types of undesired actions. This product and/or service represents only one portion of an overall DeltaV system security solution. Emerson does not warrant that the product and/or service or the use of the product and/or service protects the DeltaV system from cyber-attacks, intrusion attempts, unauthorized access, or other malicious activity ("Cyber Attacks"). Emerson shall not be liable for damages, non-performance, or delay caused by Cyber Attack. Users are solely and completely responsible for their control system security, practices and processes, and for the proper configuration and use of the security products.*

To learn how comprehensive Cybersecurity Management Services address your cybersecurity needs, contact your local Emerson sales office or representative, or visit [www.emersonprocess.com/cybersecurity](http://www.emersonprocess.com/cybersecurity).

### Emerson Process Management

Asia Pacific: 65.6777.8211  
 Europe, Middle East: 41.41.768.6111  
 North America, Latin America:  
 T 1 (800) 833-8314 or  
 1 (512) 832-3774

[www.emersonprocess.com/cybersecurity](http://www.emersonprocess.com/cybersecurity)

©2016, Emerson Process Management. All rights reserved.

The Emerson logo is a trademark and service mark of Emerson Electric Company. The DeltaV logo is a mark of one of the Emerson Process Management family of companies. All other marks are the property of their respective owners.

The contents of this publication are presented for informational purposes only, and while every effort has been made to ensure their accuracy, they are not to be construed as warranties or guarantees, express or implied, regarding the products or services described herein or their use or applicability. All sales are governed by our terms and conditions, which are available on request. We reserve the right to modify or improve the design or specification of such products at any time without notice.

