# Is Your Control System Safe Against A Costly Security Breach?

*"A stable physical structure requires at least three main supports. Industrial cybersecurity is no different. Three pillars for effective cybersecurity system are: technology, policy and procedures, and people."*

**Dennis Brandl,**
**Control Engineering, July 2012**

## What if you could...

- Reference a roadmap that clearly highlights all your system's security weaknesses?
- Refer to a prioritized action list outlining how to fix those weaknesses?
- Bridge the gap between your IT department's and your plant control system's security policies?
- Clearly, easily spell out the resources you need to keep your control system secure?
- Get ongoing feedback and recommendations to ensure your system security stays up to date?

You rely on your process control systems' security measures to help you mitigate operations safety issues, unplanned system shutdowns, potential liabilities, loss of assets and brand reputation, and potential loss of life. Security breaches on a process control system can have disastrous impacts on process plants. Security measures you use on office data networks do not directly translate to process control or safety system networks.

For these reasons, it's increasingly important to carefully evaluate potential security vulnerabilities, verify that the process control system and external network connections are secured, and take appropriate steps to further harden the control system against potential threats.

## INCREASED INTEROPERABILITY CAN MEAN INCREASED VULNERABILITY

Control systems are increasingly adopting open standards and interoperable technologies to cater to demand for operational efficiency and up-time, improved project execution and timing, and to enable smart plants with predictive technology. Unfortunately, these standards also increase control systems' vulnerability to electronic attacks and infections via the internet, and from other external and internal network intrusions. Control systems vendors work to address these security vulnerabilities, but their efforts can only solve part of the problem. It is your responsibility to solve the remaining part by defining security policies and procedures, and implementing them across the control system.

## PLANNING FOR SYSTEM SECURITY MAINTENANCE ...WHERE TO START?

To keep your control system security strategy viable, effectively neutralizing security vulnerabilities and their potential impacts on your site you've got to keep it current. Identifying flaws or weaknesses in the control system's installation, operation, and management, is a crucial task, as these weaknesses can be exploited to violate the system's integrity or cybersecurity policy. Equally crucial is the task of devising ways to address these vulnerabilities with an efficient implementation plan. But control systems, unlike office networks, must run 24/7 and cannot always be disrupted for a patch or update as often as necessary. You can't simply announce a planned shutdown in a memo, saying that the servers will not be available during the night on a certain date. You've got to plan your control system downtime many months—or even years—ahead.

## CYBERSECURITY: HOW WORRIED SHOULD I BE?

Cybersecurity is not just an IT issue; it involves everyone who comes in contact with the process control system. Your plant management people probably know that cybersecurity can affect plant reliability and safety. And your corporate management people probably know that plant system security can affect the company's revenue and reputation. The question is: how much investment and manpower should you put into solving these problems?

EMERSON™
Process Management

## CYBERSECURITY INFORMATION EXCHANGE: KNOW WHERE YOU STAND

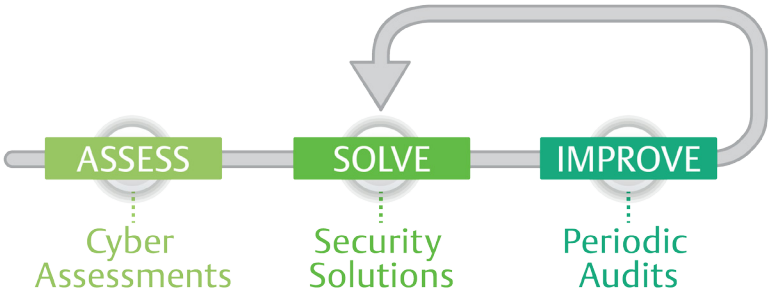
The Cybersecurity Information Exchange is a unique service that explores cybersecurity best practices as they relate to your facility. Together, we examine risks, mitigations and other issues specific to cybersecurity. This workshop equips you with the knowledge you need in order to move your control system security forward. The workshop aims to answer questions like: — "What are the most common threats to cybersecurity?" "What are some of the newer and evolving threats?" "What standards are available and which ones are right for my system?" "How are those standards implemented?" "What mitigations are typically implemented?" "What standard DeltaV system features can be used for mitigation?" and, "What are the risks in implementing security mitigations?"

## CYBERSECURITY CONSULTING/ASSESSMENT SERVICE

Emerson's Cybersecurity Consulting/Assessment Service establishes a baseline of your Emerson process control system perimeter and internal security conditions. This baseline will include a review of the installation and existing security procedures used to protect your process control system from internal and external threats. This baseline also reviews your present policies/procedures, control system drawings, best practices, network architecture and possible mitigation activities. From this baseline information a DeltaV cybersecurity assessment can identify control system security vulnerabilities and latent threats to your system. The assessment report will recommend prioritized mitigating actions to help you meet your site's control system cybersecurity integrity requirements.

## CYBERSECURITY FOLLOW-UP AUDIT SERVICES: IT'S A CONTINUOUS MAINTENANCE CYCLE

Emerson's Cybersecurity Management is a complete solution that fosters a continuous improvement and maintenance cycle. After the assessment and implementation of recommendations, an Emerson Systems Cybersecurity Consultant will follow up with regular audits. These can help preserve the integrity of your installed cybersecurity best practices and standards.




***"Management of the network is the key to security protection. As they say about Quality, business performance, and even about Life — Network Security is a journey, not a destination!"***

**Jim Pinto, Automation** Systems Cybersecurity, www.automation.com

For more information about Emerson's Security Solutions, contact your local sales office or visit:
**www.emersonprocess.com /cybersecurity**



EMERSON™
Process Management