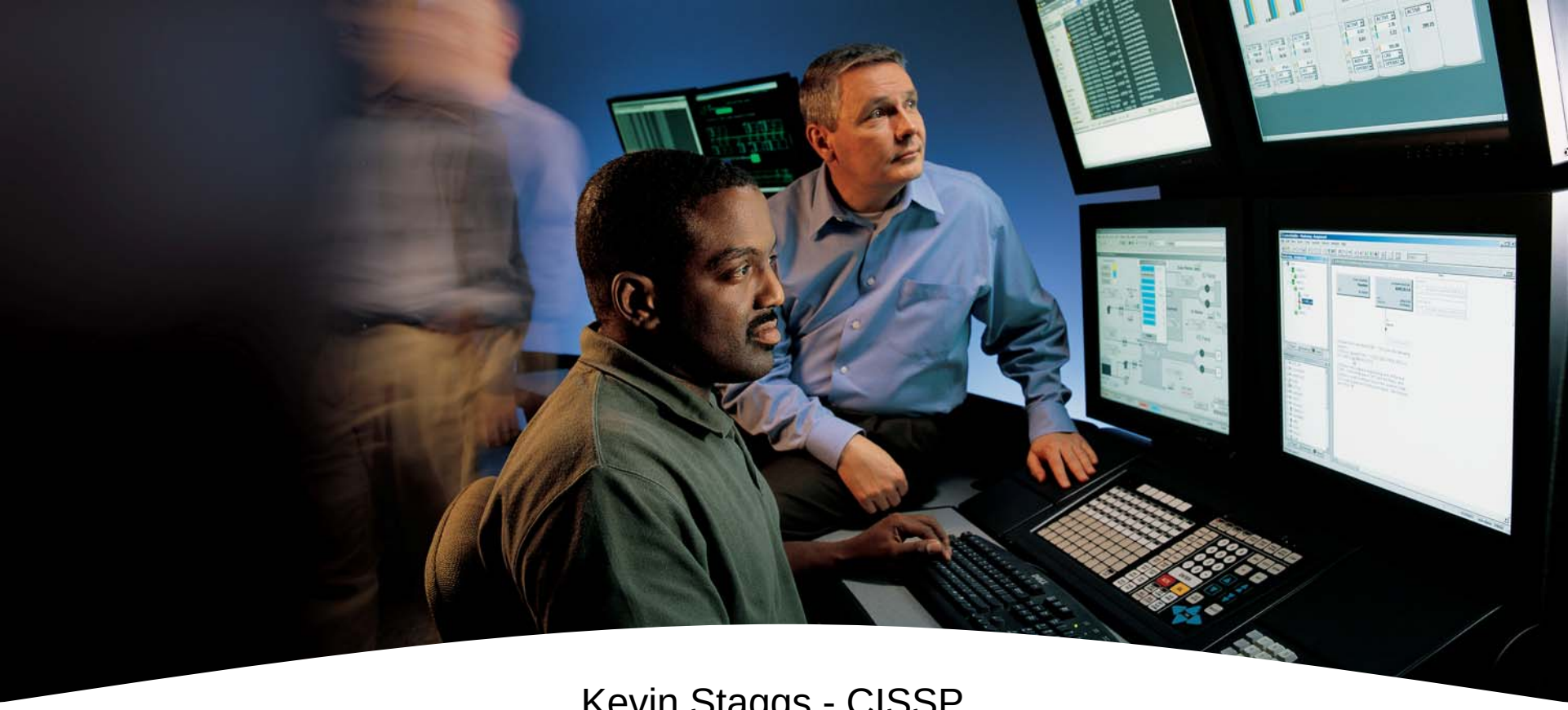


Kevin Staggs - CISSP

February 2, 2009

Patch Management

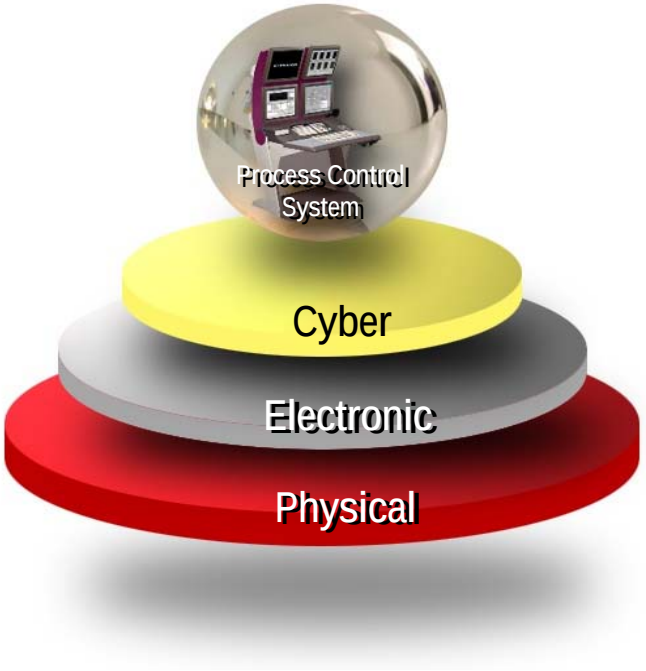
Honeywell

Topics

- Our philosophy
- Advice to our customers
- Patch qualification and management
- How we support our customers
- Industry needs
- Resources
- Summary

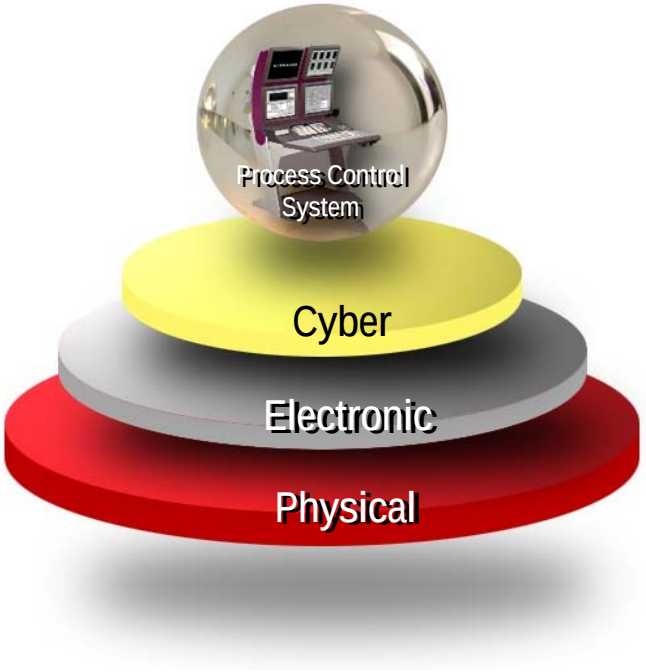
Our Philosophy

- Security and safety
  - Without security you cannot have safety
- Key Honeywell initiative
- Defense in depth
  - Security at more than just the perimeter
  - Built-in at every layer of the system
- Security is a journey not a destination
  - Policies and practices are key
  - Continuous security testing and improvements



Our Philosophy

- Security responsibility
  - End users
  - Vendors and system integrators
    - Work with their suppliers
    - Secure and test their systems
    - Work with their customers



Advice to Our Customers

- Physical access security is required to protect the system
- Reduce and secure entry points into the control system
- Perform regular security assessments
  - Security policies, procedures, and change management
- Perform regular backups and test restore capability
- Anti-virus software is necessary and must be kept up to date
- **System patches must be qualified and installed**
  - **Patch management**

Patch Qualification and Management

- Evolution of our program
  - From reactive to proactive
    - Three year evolution
    - Now program is fully proactive
  - People and equipment
  - Process
  - Communication and distribution

People and Equipment

- Dedicated teams
  - Security Steering Committee
  - SUIT – Security Update Investigation Team
  - Test team
- Dedicated test equipment
  - Multiple systems with multiple releases of software
  - Automated testing
- Dedicated teams and equipment required to succeed

Process

- SUIT process
  - Review all security updates for relevance
    - Microsoft
    - Other
  - Initiate testing of relevant updates
    - Automated rigorous regression testing
  - Review test results
  - Update qualification matrix

- Part of our lifecycle development process

Communication and Distribution

- Commitment of 7 day security update qualification
  - Most security updates qualified in 24 hours
  - Web site updated within 3 days
- Security update qualification status posted on public web site:
  - http://www.honeywell.com/ps
    - Click on Security & Other Updates
- Publish ISO image of all qualified security updates
  - Includes installation scripts
- Remote update server management

How We Manage Our Own Patches

- Be-ware alert advisory system
- Patches released through our Honeywell Solution Support On-Line system

How We Support our Customers

- Qualification of Microsoft WSUS
  - Configuration guidance for WSUS
- Security update qualification status posted on public web site:
  - http://www.honeywell.com/ps
    - Click on Security & Other Updates
- Remote update server management
- Security guidance with our Network and Security Planning Guide.

Industry Needs

- Support of multiple patch strategies
  - Multiple vendor support
  - Multiple patching needs
  - For Microsoft can be done with WSUS
- Support multiple patch types
  - Microsoft security updates
  - Antivirus definition files
- Make patching simple for the operators/end users

Resources

- Vendor guidance for patch management
  - Example can be found at http://www.honeywell.com/ps
    - Then click on Security & Other Updates

- Recommended Practice for Patch Management of Control Systems
  - From US Department of Homeland Security - Control Systems Security Program
  - http://csrp.inl.gov/Documents/PatchManagementRecommendedPractice_Final.pdf

- ISA SP99 Standards Committee – Manufacturing and Control Systems Security

Summary

- Control system safety requires a good security strategy
- Patch management is a critical element of any security strategy
- Control systems must be kept up to date
- Updates must be qualified by the vendors