

Security Management in Process Control: The 3 Waves of Adoption

**Dr Paul G Dorey
VP Digital Security & CISO
BP PLC**

The 3 Waves:

- ◆ **Adoption by the User/Operator**
- ◆ **Adoption by the System Integrator**
- ◆ **Adoption by the 'OEM' Supplier**

Back to Front?

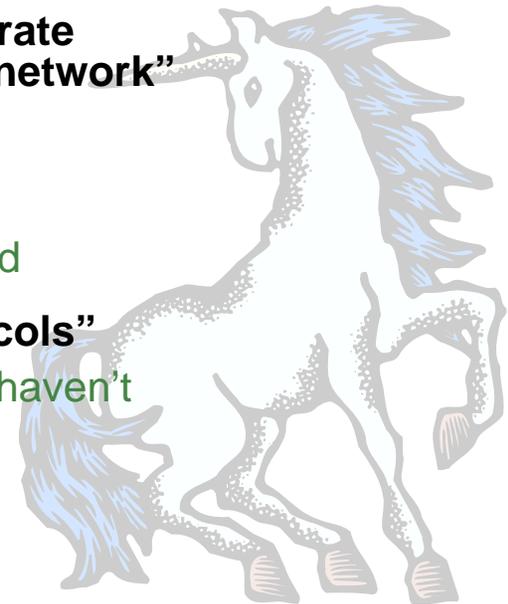
Wave 1: Background

- ◆ ***Oil and Gas companies have been interested in IT (Digital) Security since the mid '80s.***
 - *Information Broking, Operational Integrity*
 - *Trust in third party inter-connectivity*

- ◆ ***Reasonably mature IT Security functions within IT, BUT:***
 1. *Security risks do not respect organisational boundaries*
 - *Need Enterprise risk view, not business nor function limited*
 2. *Lack of **knowledge** of risk <> lack of risk*
 3. *Technology and use of technology, changes*

Common myths

- **“Our process control systems are safe because they are all isolated”**
 - Our survey says 89% are connected
- **“My networks aren’t connected, my server uses a separate network card to connect to the PCN and the corporate network”**
 - A great way to infect both networks
- **“Anti-virus can’t be applied”**
 - Supported by vendors in more cases than we expected
- **“Our system isn’t vulnerable as it uses propriety protocols”**
 - Shame they run over IP, and standard UNIX services haven’t been disabled
- **“Isn’t ACLs on a router as good as a firewall?”**
 - No !!
- **“I have a firewall, I’m safe”**
 - A support engineers enters the site and connects an infected laptop to your network
 - Your firewall allows HTTP to a badly patched webserver, and catches Nimda



Engaging the organisation

- **Needed management support**
 - Board-level (from the offset)
 - Business Stream management (quickly obtained)
 - Site management (took a little longer)
- **Needed engineers buy-in**
 - Protective of their environments
 - Believed that IT didn't understand process control issues / systems.
- **Global survey** to highlight the cyber-security challenge to management.
- **Engaged internal engineering communities/networks**
- **Created dedicated and targeted process control cyber security web-site**
 - One-stop shop for BP guidance & tools
 - Book reviews
 - News ticker
 - Feature articles
 - Links to further reading
- **Ensure that all information is given a process control interpretation:**
 - E.g. CERT vulnerabilities are reviewed with major vendors and specific advice released for major products



Wave 2: Background

- ◆ **Process Control & SCADA/DCS Vendors:**

- *Needed to break away from proprietary systems – cost/skills*
- *Adopted COTS technologies*
- *(Often) Did not have a background in security*

- ◆ **Customers:**

- *Liked the Cost Reduction & ease of integration*
- *Did not ask for security as part of the solution*

“Who will pay for the se~~X~~curity?”

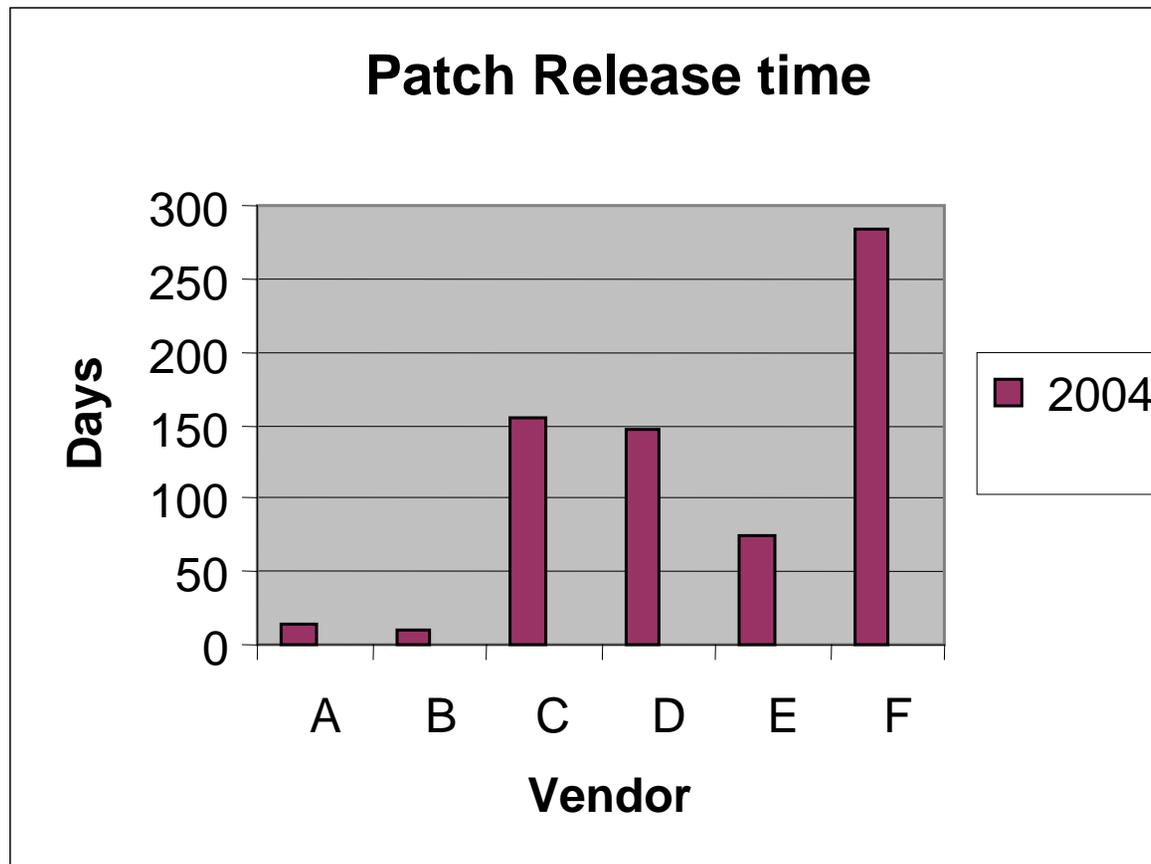
safety

Security Requirement

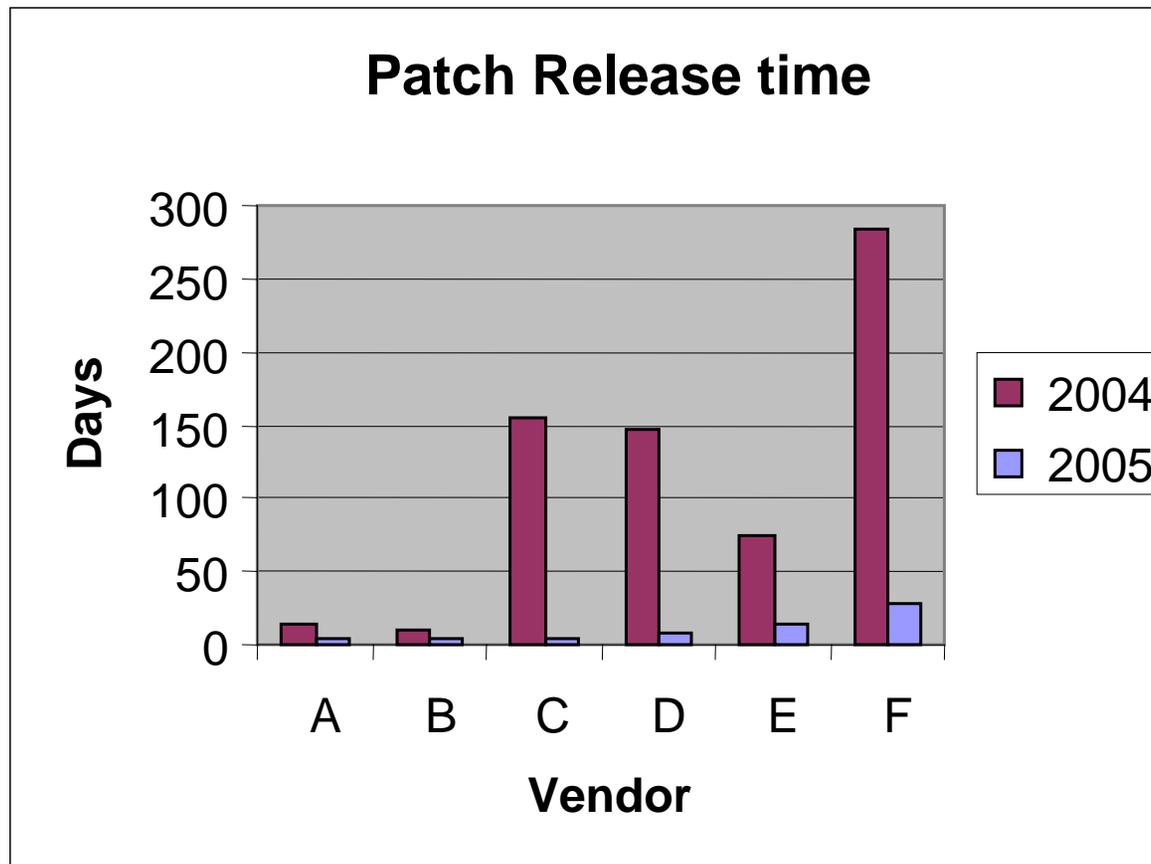
- ◆ Secure System Architecture & Component Design
- ◆ Security System/Component Testing
- ◆ Security Certification  ?
- ◆ Standards, Use Cases, Deployment Guides
- ◆ Security Support



System Integration Vendor League Table



System Integration Vendor League Table



Wave 3: Background

- ◆ **OEM (general IT) Suppliers:**
 - *May not be aware of use of their products in critical environments*
 - *Pleased with the additional income stream*
 - *(Almost) no understanding of security requirement*
 - *Poor security development practice*
- ◆ **Includes – IT Hardware, Operating Systems, Common Libraries, Databases, End User Tools, Middleware.....**

Software License

- XXXX and its suppliers provide the Software and support services (if any) AS IS AND WITH ALL FAULTS*, and hereby disclaim all other warranties and conditions, whether express, implied or statutory, including, but not limited to, any (if any) implied warranties, duties or conditions of merchantability, of fitness for a particular purpose, of reliability or availability, of accuracy or completeness of responses, of results, of workmanlike effort, of lack of viruses, and of lack of negligence, all with regard to the Software, and the provision of or failure to provide support or other services, information, software, and related content through the Software or otherwise arising out of the use of the Software.

* Their emphasis

General IT Requirements

- ◆ **Acceptance of use of technology in critical applications**
- ◆ **The ‘big win’ - A need for a step-change in system security & integrity, especially safety critical environments.**
 - Secure development approaches
 - Inherently secure development
- ◆ **Where next if the OEMs will not move to inherent security?**