The 3 Steps to Secure Process Systems

1. **Stakeholder engagement**
   - Understanding and Vision
   - Backing
   - Combined Know-how

2. **A dedicated security programme**
   - People, process & technology
   - Standards & Tools
   - Assurance/Monitoring

3. **A new mind-set**
   - Engineering thinking in IT situations
   - Get the vendors on-side
   - Acting together (Industry standards, test labs, shared learning)
“Lame Excuses”

- We do not use digital technology
- It's not connected to the corporate network
- It's never happened
- Plus all the IT systems ‘lame excuses’ “Writing Secure Code”, Michael Howard & David LeBlanc, Microsoft Press:
  - No one will try that attack
  - Why would anyone do that?
  - We’ve never been attacked
  - We’re secure – we use encryption
  - We’re secure – we use ACLs
  - We’re secure – we use a firewall
  - We’ve reviewed the code – there are no security bugs
  - We know it’s the default but the administrator can turn it off
  - If we don’t run as administrator, stuff breaks.
IT Security in an engineering environment

Will organisational scope allow the right experts to work together?
### Dedicated Security Programme

<table>
<thead>
<tr>
<th>Segment:</th>
<th>BU</th>
</tr>
</thead>
<tbody>
<tr>
<td>Good Segregation</td>
<td>Yes No No Yes Yes Yes Yes Yes Yes No Yes No</td>
</tr>
<tr>
<td>Good Three Tier Architecture</td>
<td>Yes No No Yes Yes Yes Yes Yes Yes No Yes Yes</td>
</tr>
<tr>
<td>Good AV</td>
<td>Yes No No Yes Yes Yes Yes Yes Yes No No Yes No</td>
</tr>
<tr>
<td>OS Patching</td>
<td>Yes No Yes No Yes Yes Yes Yes Yes Yes No No No</td>
</tr>
<tr>
<td>Contingency Planning</td>
<td>No No No No No No No No No No No No No No</td>
</tr>
<tr>
<td>Training</td>
<td>Yes Yes Yes Yes Yes Yes Yes Yes Yes Yes Yes Yes No</td>
</tr>
</tbody>
</table>
This Product is designed, developed and manufactured for general use, and is suitable without limitation for use in general office environments, for personal use and for household use.

It is **NOT** designed, developed and manufactured for use in environments bearing extremely high risk potentials like fatal risks or dangers, which require extremely high safety measures, and which could otherwise lead to death, personal injury, severe physical damage or other similar losses. Such environments include without limitations, use in:

- **nuclear power** facility control,  - **airplane control**,  
- **air traffic control**,  - **mass transport** operation control,  
- **life support**, and - **weapon launching** control.
Software License 2

- 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
The IT environment challenges

- Features vs. security requirements
- Cost drivers away from bespoke software & Code re-use
- Hard to predict dynamic IT vs. deterministic design
- Enormous code sizes
- ‘Re-boot’ mentality
- Dealing with legacy
- Security Entropy
- Using people who know what they are doing
Professional Security Expectations

• Security staff need to be accountable & have decision making roles.

• Professionals not just “advisors”.

• Is a bridge designed by a project manager?

• Would the surgeon wake you to ask your opinion?
Engineering Approaches

- Understand
- Analyse
- Build
- Operate/Test
- Measure

Risk Assessment/Policy
Security Techniques
Secure Development Lifecycle
Repeatable testing (ISA) /Pen Tests vs. SIL
Monitoring Systems - (Log)[C]

All to standardised & repeatable processes

See: ANSI/ISA-99.00.01-2007
and ISA Security Compliance Institute
www.isa.org/ISASecure
Questions?

Email: paul.dorey@bp.com