Why I Don’t Upgrade My Network

THE UPGRADE COULD MAKE OUR NETWORK UNSTABLE.

YOU CAN’T MAKE AN OMELET WITHOUT BREAKING SOME EGGS.

I INTERPRET YOUR FOLKSY RESPONSE TO MEAN I SHOULD UPGRADE THE NETWORK DESPITE THE RISKS.

NO, I’M SAYING I’LL BREAK YOUR EGGS IF THE NETWORK GOES DOWN.
Secure Network Refresh

Honeywell User Group 2017
Seth Carpenter/ Robert Alston
Agenda

• Introductions
• Safety Moment
• Secure Network Refresh Defined
• Identifying the Need for a Refresh
• Securely Refreshing a Process Control Network
  o Hardware Refresh
  o Software Refresh
  o Architecture Refresh
• Summary of Secure Network Refresh
• Wrap up / Q&A
How Do You Know if You Need a Network Refresh?

If you are still using one of these...

- IBM XT
- Cisco 1900

... you need a network refresh.
Secure Network Refresh Defined

• What it is?
  - Replacing out of date software and end of life hardware
  - Securing critical network infrastructure
  - Hardening of systems
  - Enabling migration of legacy components
  - Implementing secure communications
  - Updating network architecture

• What it is not
  - Experion upgrade
  - Controller upgrade
  - Release dependent
How Do You Know if You Need a Network Refresh?

If you are still using one of these…

… you **definitely** need a network refresh.
Foundation for ELCN/EUCN Migrations
Switch Obsolescence

• Announced End-of-Life (EOL) for many Cisco and other switches
  - Switches: 2900s, 2950s, 2960s, 3550s
  - Slower processing & interfaces
  - Some obsolete as of 2009
  - NOT UPGRADEABLE

• Big Issue: Security
  - Older switches do NOT support encryption
  - Configuration via Telnet only – IN THE CLEAR
  - Extremely vulnerable to TAKE OVER
  - New Switches & Routers support encryption for their communications and configuration files
  - Other manufacturer’s Switches & Routers that do not encrypt their configuration files and access should also be replaced

• Configurations of _upstream_ devices may also need to be checked as well
Router Obsolescence

- Routers were previously installed to support reliable connections
  - Routers today need more restricted configurations to strengthen security
  - Control of traffic between zones supports containment and protection
  - Router’s Access Control Lists define communication between networks

- Announced End-of-Life (EOL) for many Cisco Routers as well
  - Routers: 3560s, 3750s
  - Slower processing & interfaces
  - Some obsolete as of 2009
  - NOT UPGRADEABLE

- Same issues with security
  - Older routers do NOT support encryption
  - Configuration via Telnet only – IN THE CLEAR
  - Extremely vulnerable to TAKE OVER
  - New Routers support encryption for their communications and configuration files
  - Other manufacturer’s Routers that do not encrypt their configuration files and access should also be replaced

- Configurations of connecting devices should also be revisited
## FTE Qualified Cisco Switches and IOS

<table>
<thead>
<tr>
<th>Honeywell Model</th>
<th>Cisco Part Number</th>
<th>Qualified IOS (Latest First)</th>
<th>Cisco file name</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>15.2(2) E4</td>
<td><code>c2960x-universalk9-mz.152-4.E.bin</code> *</td>
</tr>
<tr>
<td>NE-SW224P</td>
<td>WS-C2960+24TC-L</td>
<td>15.0(2) SE9</td>
<td><code>c2960-lanbasek9-mz.150-2.SE9.bin</code> *</td>
</tr>
<tr>
<td>NE-SW248P</td>
<td>WS-C2960+48TC-L</td>
<td>15.0(2) SE9</td>
<td><code>c2960-lanbasek9-mz.150-2.SE9.bin</code> *</td>
</tr>
<tr>
<td>SI-296XN8</td>
<td>WS-C2960X-48TS-L</td>
<td>15.2 (2) E6</td>
<td><code>c2960x-universalk9-mz.152-2.E6.bin</code> *</td>
</tr>
<tr>
<td>NE-SW24G1</td>
<td>WS-C2960X-24TS-L</td>
<td>15.2 (2) E6</td>
<td><code>c2960x-universalk9-mz.152-2.E6.bin</code> *</td>
</tr>
<tr>
<td></td>
<td></td>
<td>15.2 (4) E</td>
<td><code>c2960x-universalk9-mz.152-4.E.bin</code> *</td>
</tr>
<tr>
<td>NE-SW312X</td>
<td>WS-C3750X-12S-S</td>
<td>15.0(2) SE6</td>
<td><code>c3750e-ipbasek9npe-mz.150-2.SE6.bin</code> *</td>
</tr>
<tr>
<td></td>
<td></td>
<td>15.0(2) SE4</td>
<td><code>c3750e-ipbasek9npe-mz.150-2.SE4.bin</code> *</td>
</tr>
<tr>
<td>NE-SW504S</td>
<td>IE-3000-4TC</td>
<td>12.2(55) SE9</td>
<td><code>ies-lanbasek9-mz.122-55.SE9.bin</code> *</td>
</tr>
<tr>
<td></td>
<td></td>
<td>12.2(55) SE3</td>
<td><code>ie-lanbase-mz.122-55-SE3.bin</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>12.2(50) SE2</td>
<td><code>ies-lanbase-mz.122-50.SE2.bin</code></td>
</tr>
<tr>
<td>NE-SW508S</td>
<td>IE-3000-8TC</td>
<td>12.2(55) SE9</td>
<td><code>ies-lanbasek9-mz.122-55.SE9.bin</code> *</td>
</tr>
<tr>
<td></td>
<td></td>
<td>12.2(55) SE3</td>
<td><code>ie-lanbase-mz.122-55-SE3.bin</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>12.2(50) SE2</td>
<td><code>ies-lanbase-mz.122-50.SE2.bin</code></td>
</tr>
</tbody>
</table>
Summary

- Replace out of date software
- Replace end of life hardware
- Secure critical network infrastructure
- Harden systems
- Migrate of legacy components
- Implement secure communications
- Update network architecture