Industry 4.0

Moderator: Mike Assante, SANS Institute

Panelists:
David Foose, Emerson
Ernie Hayden, Securicon
Bryan Owen, OSIsoft
Industry 4.0

David Foose
Ovation Product Security Manager
2/22/2016
Current Observed Trends

- Everything has an IP
- Zero Borders
- Consolidation
Cloud/Virtualization

- For Control/Monitoring
- Cost
- Simulation
- Lifespan
- Micro Virtualization
- CIA Triad

Image Source: https://www.stickermule.com/marketplace/3442-there-is-no-cloud
Micro Generation

- Can physically affect the grid
- Control
- Updates
- Vendor Selection

Pervasive Sensing and Risk to ICS

Ernie Hayden CISSP CEH GICSP(Gold) PSP
Executive Consultant
www.securicon.com
Risk Implications of Pervasive Sensing

- #1 – Scalability
- #2 – Information Overload
- #3 – Scalable Response is Negatively Impacted
- #4 – Overreliance on Wireless Increases Hacking Opportunities
- #5 – Physical Attack of Sensors and Devices
- #6 – Cyber Security Supply Chain Injection
- #7 – Configuration Control and Management
- #8 – Subtle System and Sensor Interconnectedness Not Accounted for or Considered
- #9 – Weak Encryption Exposes Sensor Data and Infrastructure
- #10 – Real Sensors can be Substituted by False Sensors (Sybil Attacks)
THANK YOU!

University of Washington
College of Built Environments
Seattle, Washington
Capstone
Masters of Infrastructure Planning and Management (MIPM)

PERVERSIVE SENSING AND INDUSTRIAL CONTROL SYSTEM RISK IMPLICATIONS
By
Ernest N. Hayden CISSP CEH GIAC(Gold)
August 2015
Capstone Advisor: Barbara Endres-Popovskiy Ph.D.

If you’d like a copy of this paper please send an email to:
ernie.hayden@securicon.com
Industry 4.0
What’s your IoT Strategy?
Show me the Money!
Once we had control of one device, we had pretty much everything we needed...automatically begin spreading it’s update to other meters within range, setting off a chain reaction that wasn’t part of their feature set... we know, we added the feature to our malicious firmware update.

Technicians would spot the outage... and send out a remote firmware update to turn...his malicious software didn’t just turn off the power, it also deleted the firmware update feature....if it’s got the remote disconnect relay in it, ...enabled or not... it’s a real big, ugly issue.
## Security Feature Poverty Ladder (Example)

<table>
<thead>
<tr>
<th>Industry 4.0 Field Device Use Case</th>
<th>Data Integrity</th>
<th>Automatic Update</th>
<th>End to End Authentication</th>
<th>Open Port</th>
<th>Telemetry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indicator (Short Lived)</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Indicator</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Indicator Gateway/Mux</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Actuation</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Control Gateway/Mux</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td>✔</td>
</tr>
</tbody>
</table>
Questions?

Thank You