GETTING OVER A BAD ICS AUDIT

October 2018
Paul Piotrowski - GICSP, CISSP, CRISC, CBCP, CIPT
Automation Engineer – ICS Integrity
Presentation Context

- **Purpose**
  - Provide insight into common and not so common problems that can and do occur in ICS Audits. Share best practices to identify problems and promptly rectify them. How to move on from the final report.
  - Focus is on what can go wrong but the content can easily be used to plan a successful ICS audit.

- **Audience**
  - All ICS Cyber Security Professionals and Stakeholders
  - ICS Awareness Level Understanding

- **Content Source**
  - Personal Experience
  - Shell Auditor Colleagues
  - Christopher Humphreys – The Anfield Group
Most of us have seen an audit report that looks like this...

<table>
<thead>
<tr>
<th>Product Type:</th>
<th>Board Audit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Locations covered:</td>
<td>Your Site</td>
</tr>
<tr>
<td>Period of Fieldwork:</td>
<td>2 April – 16 April 2018</td>
</tr>
<tr>
<td>Date Issued:</td>
<td>FINAL</td>
</tr>
<tr>
<td>Audit Opinion:</td>
<td>UNSATISFACTORY</td>
</tr>
</tbody>
</table>

**EXECUTIVE SUMMARY**

The site Industrial Automation and Control System (IACS) controls are the heart of a production operating unit. Their specific function is to collect, display, transmit, monitor, control, optimize and store primary production data for the purposes of direct monitoring, control and safeguarding of plant operating processes. Due to increased connectivity of control systems and changes in technology, the number and sophistication of cyber security incidents, such as malicious attacks, viruses and unauthorized access to IACS systems, have increased significantly in recent years. This has led to an increasing need to secure IACS systems within the sites through risk-based controls.
Audit Reactions Will Vary...
But Wait - Other Bad Things Can Happen...

- **Scope Agreement**
  - What is being audited and how? - could lead to false assurance
  - What is your organization’s ICS definition?
  - Should the audit be performed at all?

- **Messaging**
  - Big picture focus; failure to convey impact in dollar value due to production deferment/shutdown
  - Findings and recommendations are not practical and/or feasible

- **Personality Conflicts**
  - Audit team and/or with stakeholders
  - No trust and/or credibility

- **Cultural Norm Missteps**
  - Deemed Offensive Behaviors
Other Bad Things Continued...

- **Operational Impacts**
- **Personal Health & Security**
  - Medical & family emergencies
  - Security of staff in and out of office
- **Logistic Fails**
  - Travel mix-ups/visas/equipment missing
  - Getting and staying where you need to be (i.e. helicopters)
  - Permitting & conflicting site priorities (i.e. cancellations)
  - Personal Protective Equipment not available or ready
- **Human Resource Noise**
  - Individuals leaving, joining, moving
How Do We Get Through It?

- Stay professional, truthful and transparent. Stronger as a team!
- Acknowledge errors, problems, successes. Apologize if needed
- Personal safety and health trumps any audit objective
- Identify problems early, escalate if required and rectify
- Cancel, postpone, change scope of audit if situation warrants it
- Be collaborating instead of confronting: educate, explain
- Overcommunicate during and after audit: regular updates, no-surprise meeting(s), issue discussion notes.
- If possible try to “purple team”, support each other post audit
Next Steps Post Audit & Final Thoughts

- Use the report as inflection point to get what YOU need organizationally
- Take the time to review the report through a different lens
- Take a “risk based” approach to discussion making
- Don’t point fingers and blame each other instead start fixing
- Be methodical and realistic in your remediation planning (don’t gold plate).
- Incorporate learnings into future audits and engagements

Final Thoughts

- There is no master playbook. Use the right tool for the right job.
- Compliance never equals security; any framework is floor not ceiling
- Remediation projects are complex: under promise, over deliver
Questions and Answers

“As question become more difficult where do you get answers?”

Number of Questions vs. Question Difficulty

Search Engines

ask a human