Getting Off the Hamster Wheel of Testing

MODERATOR: Wendy Frank, Principal Cybersecurity, Privacy & Risk, PwC

PANELISTS:
- Diana Kelley
  Global Executive Security Advisor
  IBM Corporation
- Lisa Lee
  IT Examiner
  Office of the Comptroller of the Currency
- Latha Maripuri
  SVP and Global CISO
  News Corp
Agenda

- The Good, The Bad, and The Ugly
- Impact vs Effort
- Maturity Model of Testing
- Off the Wheel... Next Steps
Impact vs. Effort

- Pen Testing
- Phishing Exercise
- Integrated Code Scanning

- Basic Vuln Scanning
- Social Engineering

- Bug Bounty Programs
- Compromise Assessment
- Red / Blue / Purple Teams
- Threat Assessment
- IoT Testing

- "Rich" Network Vuln Scanning
- Continuous DAST
# Maturity Model of Testing

<table>
<thead>
<tr>
<th></th>
<th>Blissful Ignorance</th>
<th>Early Maturity</th>
<th>Threat &amp; Risk Testing</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Level 0</td>
<td>Level 1</td>
<td>Level 2</td>
</tr>
<tr>
<td>Asset Inventory</td>
<td>None</td>
<td>Basic</td>
<td>More complete</td>
</tr>
<tr>
<td>Vulnerability Scanning</td>
<td>None</td>
<td>Infrequent/via 3rd party</td>
<td>Regular but not often</td>
</tr>
<tr>
<td>Social Engineering</td>
<td>None</td>
<td>None</td>
<td>Basic</td>
</tr>
<tr>
<td>Phishing</td>
<td>None</td>
<td>Basic</td>
<td>Scenario testing</td>
</tr>
<tr>
<td>Physical Ethical Hacking (Pen Tests)</td>
<td>None</td>
<td>None</td>
<td>Entry point testing</td>
</tr>
<tr>
<td>Red Team</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Purple Team</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Application Testing</td>
<td>None</td>
<td>None</td>
<td>Basic</td>
</tr>
<tr>
<td>Threat Assessment</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Compromise Assessment</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
</tbody>
</table>

**Increasing Frequency**: 4

**Intensifying Scope**:
Off the Wheel…Next Steps

- Consider the cost benefit analysis
  - Testing expense
  - Remediation time
  - Training value
- Plan for the results
Off the Wheel...Next Steps

Evaluate your future testing strategy

- Understanding threat vectors/actors
- Variation of types
- Various channels
- Scope of work
- Frequency
- Using tests to train teams