Cyber Security Awareness in the Digital Age

Presented by, Phil Bertolini, Deputy County Executive & CIO
Oakland County, MI

March 2018
Agenda

• Cyber Security Status
• How are we going to defend our data?
• CySAFE
• Cyber Security Challenges
Cyber Security Status

What have we done?
We have established an IT Security governance program based on industry best practices, built a team dedicated to the protection of Oakland County Systems and made IT Security our #1 Priority. Our strategy is a Defense in Depth approach. We use risk management processes and tools to analyze threats and vulnerabilities for services such as cloud services, vendor management and end point protections.

Where are we today?
We have been recognized as a top county in the United States when it comes to Information Security. We have recently added third party risk assessments, physical security assessments and further educated our teams on mitigating the top cyber threats.

Where are we heading?
We will continue to implement and enhance our controls based on the current threat landscape to ensure we operate securely and efficiently. Now that we have built our foundation we will refine our standard operating procedures and enhance our monitoring and metrics for the remainder of 2018.
How are we going to defend our data?
Minimizing Time, Cost, and Risk

While Maximizing Control and Meeting Compliance Standards
Roadmap 2014-2017

2014
- Build Governance
- Establish Risk Management
- Implement Quick Wins
- Educate IT and Users

2015
- Tool/Services implementation (IPS, BOT)
- Secure Access (2nd Factor Authentication, Remove admin rights)
- Software Development Life Cycle (SDLC)
- Third Party Management
- Business Integration

2016
- Managed and Automated Services
- Dashboards / Reporting
- Asset Inventory
- Pen and Vulnerability Testing

2017
- Audit Controls
- Business Continuity

CMMI
- 0-1
- 1-2
- 2-3
## CySoFE: Cyber Security Assessment for Everyone

<table>
<thead>
<tr>
<th>Control Category</th>
<th>2013 Q1</th>
<th>2014 Q1</th>
<th>2015 Q1</th>
<th>2016 Q1</th>
<th>2017 Q1</th>
<th>2018 Q1</th>
<th>2017 Q4 Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategy / Scope</td>
<td>0.22</td>
<td>2.22</td>
<td>2.44</td>
<td>2.44</td>
<td>3.00</td>
<td>3.0</td>
<td>3.0</td>
</tr>
<tr>
<td>Planning / Design / Configuration</td>
<td>0.56</td>
<td>1.33</td>
<td>1.56</td>
<td>1.78</td>
<td>2.89</td>
<td>3.0</td>
<td>3.0</td>
</tr>
<tr>
<td>Operations</td>
<td>0.67</td>
<td>1.55</td>
<td>2.09</td>
<td>2.27</td>
<td>2.91</td>
<td>3.0</td>
<td>3.0</td>
</tr>
<tr>
<td>Monitoring / Metrics</td>
<td>0.00</td>
<td>0.50</td>
<td>1.50</td>
<td>1.75</td>
<td>2.25</td>
<td>3.0</td>
<td>3.0</td>
</tr>
<tr>
<td>Response / Recovery</td>
<td>0.67</td>
<td>2.00</td>
<td>2.33</td>
<td>2.33</td>
<td>3.00</td>
<td>3.0</td>
<td>3.0</td>
</tr>
<tr>
<td>Control Category</td>
<td>2018 Q1</td>
<td>2018 Q2</td>
<td>2018 Q3</td>
<td>2018 Q4</td>
<td>2018 Q4 Target</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>---------</td>
<td>---------</td>
<td>---------</td>
<td>---------</td>
<td>----------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Strategy / Scope</td>
<td>3.67</td>
<td>3.67</td>
<td></td>
<td></td>
<td>4.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Planning / Design / Configuration</td>
<td>3.64</td>
<td>3.64</td>
<td></td>
<td></td>
<td>4.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operations</td>
<td>3.56</td>
<td>3.56</td>
<td></td>
<td></td>
<td>4.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monitoring / Metrics</td>
<td>3.00</td>
<td>3.33</td>
<td></td>
<td></td>
<td>4.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Response / Recovery</td>
<td>4.00</td>
<td>4.00</td>
<td></td>
<td></td>
<td>4.0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* Focus on improving Operations and Monitoring/Metrics for the remainder of 2018*
Benefits

• Prioritizes largest IT risk areas
• Trends progress
• Creates a Summary of Controls to explain current controls, exclusions and planned work
• Establishes RACI for all 35 controls
• Only takes 90 minutes
• FREE
Cyber Security Challenges

What challenges do we have?

Ransomware continues to be our biggest threat today. There are a low startup costs, minimum risks and high profit margins.

We continue to train our end users, add network protections such as blocked websites, harden our applications, servers and workstations and add more email protections to mitigate this threat. Lastly, we will further refine our Standard Operating Procedures (SOP) to prepare for automating labor intensive tasks.

What can you do?

Continue to be engaged and help improve our security culture and awareness across all our departments; Encourage employees to take the IT Security Training modules, be aware of Phishing emails and protect Oakland County data - both printed and electronic.
Cyber Security is Everyone’s Responsibility!