Orange County Transportation Authority
Cyber-Security Update

Security Program Remediation Plan

- Objective #1:

  Prevent and contain future attacks

- Objective #2:

  Enable security risk based management decisions

- Objective #3:

  Implement recommended security best practices

Progress-to-date

- Up-to-date patching on 30-day cycle
- Implemented and refining network segmentation
- Finished training – white phishing is next
- Extensive evaluations and testing
- Continue our migration into the cloud
- Looking at machine learning tools
- Testing two-factor authentication
- Reviewing industrial control systems
- Data loss prevention insurance has been renewed

Recent Threats – Meltdown and Spectre

- Exploits modern CPUs to access protected memory
- Sensitive information theft, such as extracting encryption keys or passwords from memory
- Servers, desktops, laptops, mobile devices, and cloud servers are vulnerable
- Meltdown will be patched as part of OCTA's normal patch cycle
- No fix yet for Spectre

Industrial Controls Review

- Review and solidify incident management process
- Findings:
  - Generally in good shape
  - Co-managed systems responsibilities need to be solidified
  - Segment ICS from corporate network
  - Definition of some policies and procedures pertaining to Scada systems
  - Risk management framework

Next Steps

- Phishing
- Implement Spectre vulnerability patch
- Review/Implement Industrial Control Recommendations
- Return to Finance and Administration Committee in 6 months