SILICON VALLEY CLEAN ENERGY

Information Technology Update

Audit Committee
June 5, 2019

Agenda

01

Agenda

AMI Audit Presented by Abbot, Stringham & Lynch.

02

Agenda

General IT Audit Results

03

Agenda

Discussion of responses to Cybersecurity RFI

04

Agenda

Data Security 2.0

1. AMI AUDIT

SILICON VALLEY
CLEAN ENERGY

aslcpa.com | @aslcpasv

Silicon Valley Clean Energy Authority

Agreed-upon Procedures Report on

AMI (Covered) Data Privacy and Security

For the Period through December 31, 2018

AGREED-UPON PROCEDURES

1. Abbott, Stringham & Lynch, CPAs (ASL) – Introduction of Firm and Team
   - Steve Carter, Partner – ASL
   - Patrick Ngai, Audit Manager – ASL
   - Steve Nessen, Partner – Hutchinson & Bloodgood, CPAs (H&B)
   - Chris White, Partner – H&B
2. Scope of Engagement – 2 components as addressed in CPUC Decision 12-08-045
   - Written Policies and Procedures
   - IT Focus
3. Overall Report Findings – Steve Carter, CPA
4. IT Discussion – Chris White and Steve Nessen
5. Q & A

AMI DATA IT REVIEW

Regulatory

Automated Meter Infrastructure (AMI) audit required by CPUC triennially

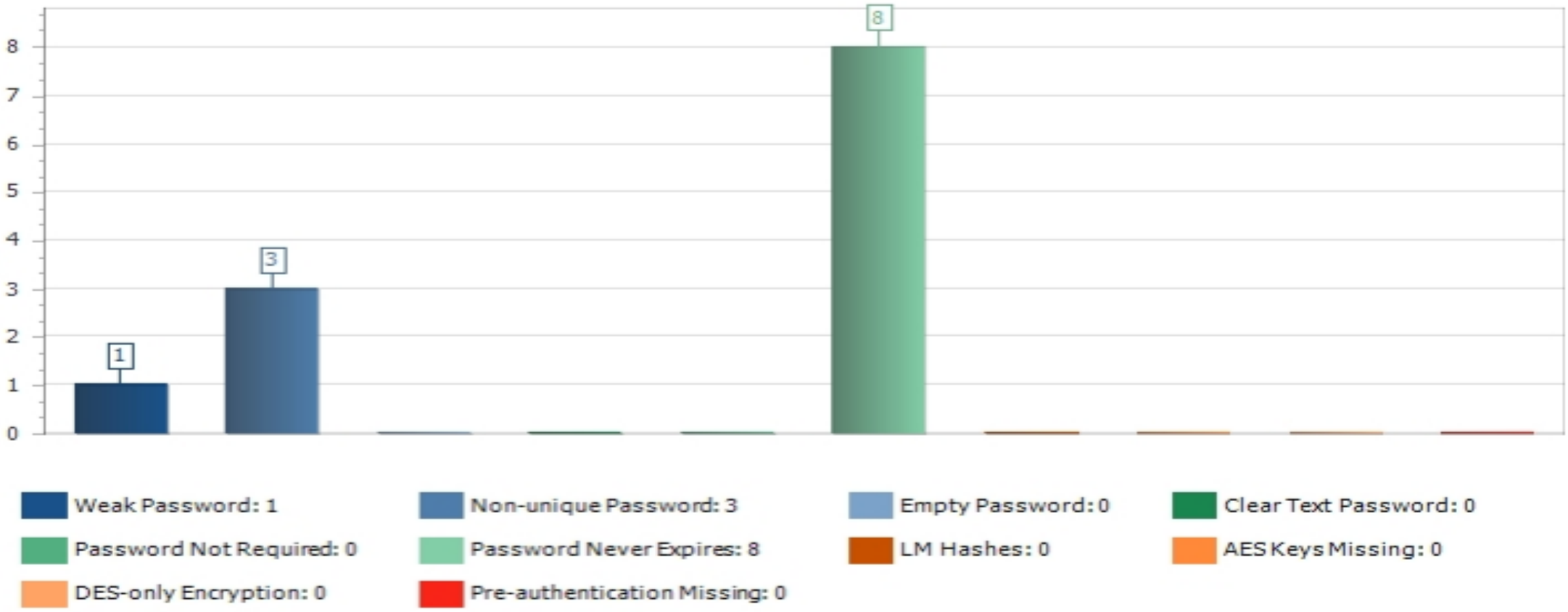
Focus

AMI specific IT controls related to the acquisition, storage and processing of AMI related data

General IT controls (such as patch management, IT governance, backup-recovery)

ACTIVE DIRECTORY ACCOUNT REVIEW

Distribution Chart by Weakness Type

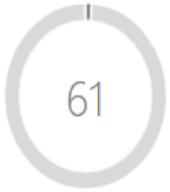


INTERNAL VULNERABILITY SUMMARY

CURRENT VULNERABILITIES

30	162	238	12
CRITICAL	HIGH	MEDIUM	LOW

EXPLOIT AVAILABLE

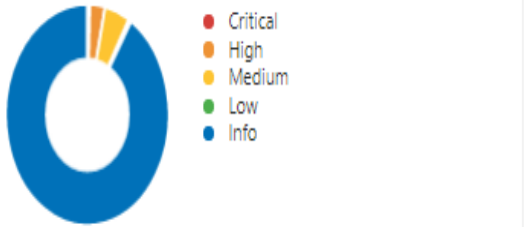


PUBLISHED OVER 30 DAYS AGO

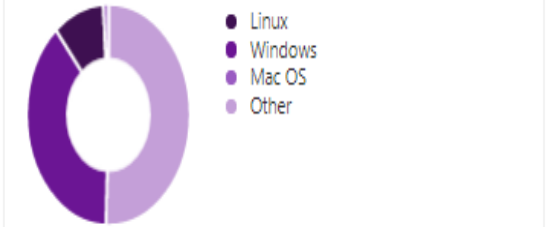
DISCOVERED USING CREDENTIALS

PUBLISHED SOLUTION AVAILABLE

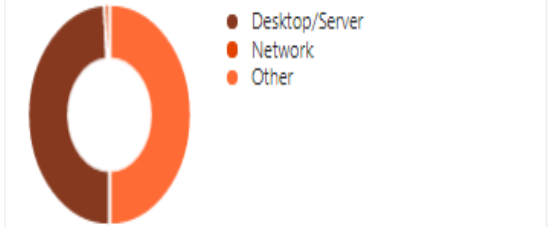
VULNERABILITIES



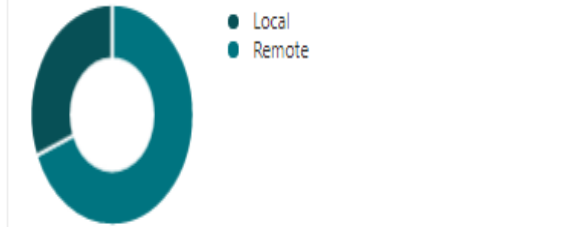
OPERATING SYSTEM



DEVICE TYPES



AUTHENTICATION



EXTERNAL VULNERABILITY SUMMARY

CURRENT VULNERABILITIES

CRITICAL	HIGH	MEDIUM	LOW
0	0	0	0

EXPLOIT AVAILABLE	PUBLISHED OVER 30 DAYS AGO	DISCOVERED USING CREDENTIALS	PUBLISHED SOLUTION AVAILABLE
0	12	0	0

RECOMMENDATIONS

- Active Directory (AD) accounts should be reviewed to ensure password settings match organizational policy
- Patch management for Microsoft and 3rd party software should occur weekly at a minimum
- Cloud-based data silos (Office 365, Box, etc.) should be reviewed to ensure appropriate security and audit logging are enabled
- On-going vulnerability testing and remediation should be part of overall IT management
- Vendor management policies should be improved to include appropriate documentation (SOC-2, independent security assessment) provided to SVCE.

SILICON VALLEY CLEAN ENERGY

2. GENERAL IT AUDIT

SILICON VALLEY
CLEAN ENERGY

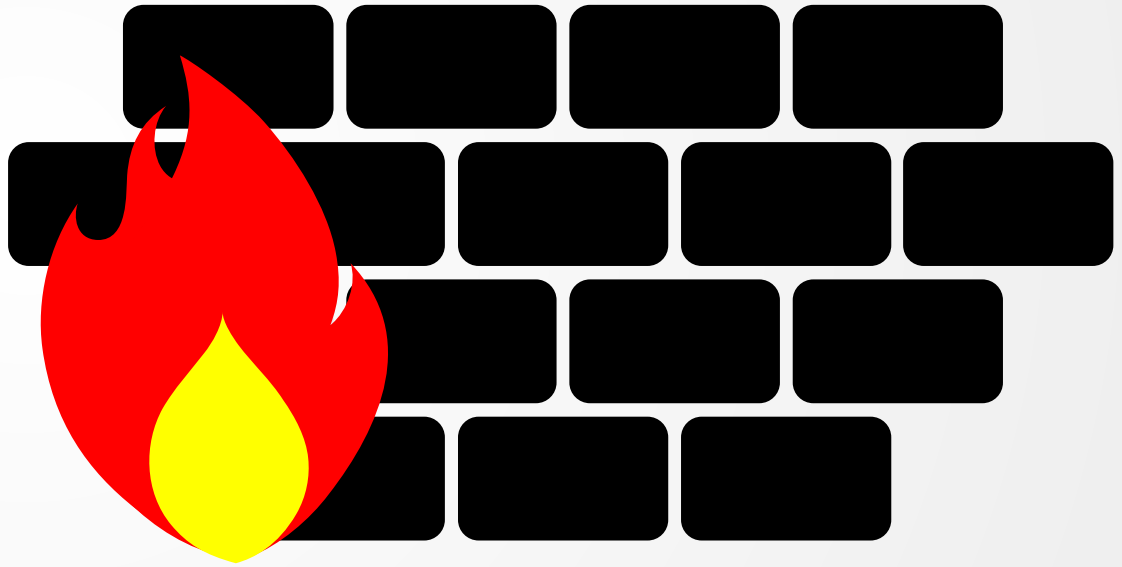
IT AUDIT

- SVCE commissioned Greycastle to perform audit of SVCE systems and policies
- Scope included:
  - Penetration Testing
  - External Vulnerability Assessment
  - Internal Vulnerability Assessment
- Rating scale:
  - **Low – Medium – High - Critical**

SILICON VALLEY CLEAN ENERGY

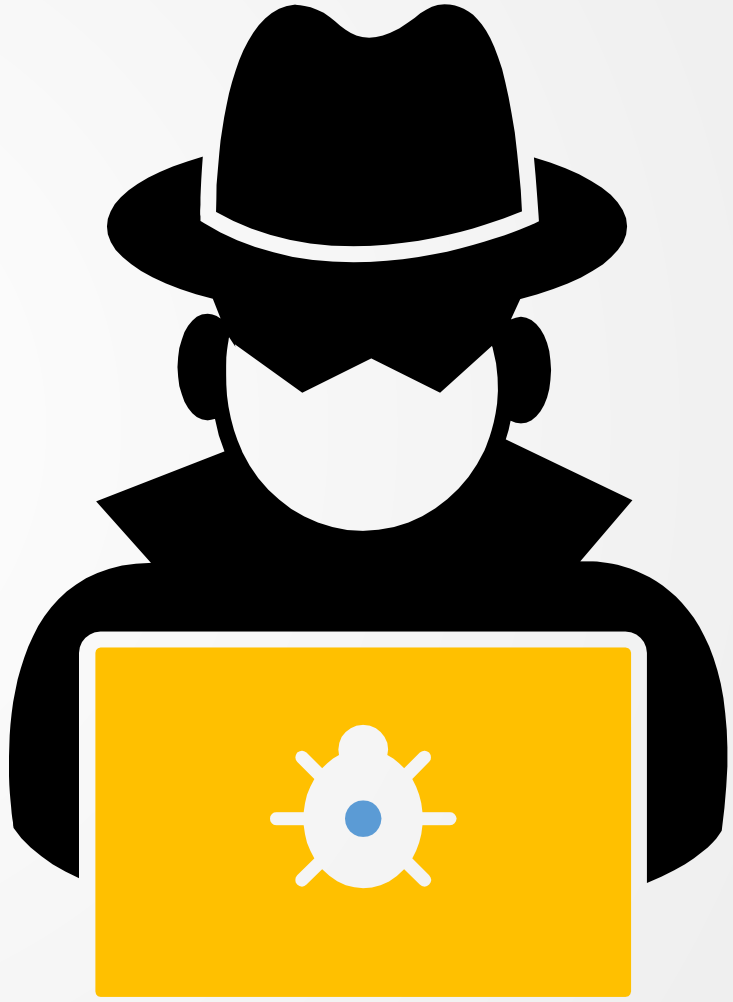
PENETRATION TESTING

- Simulate attacks and motives of cybercriminals
- Verify SVCE had the following practices in place:
  - Backup & Disaster recovery
  - Incident/Problem/ Change Management
  - Risk Mitigation
- **Result - LOW**
- Recommendations:
  - Continue to conduct regular penetration tests
  - Continue to conduct regular social engineering testing
  - Create and distribute security reminders



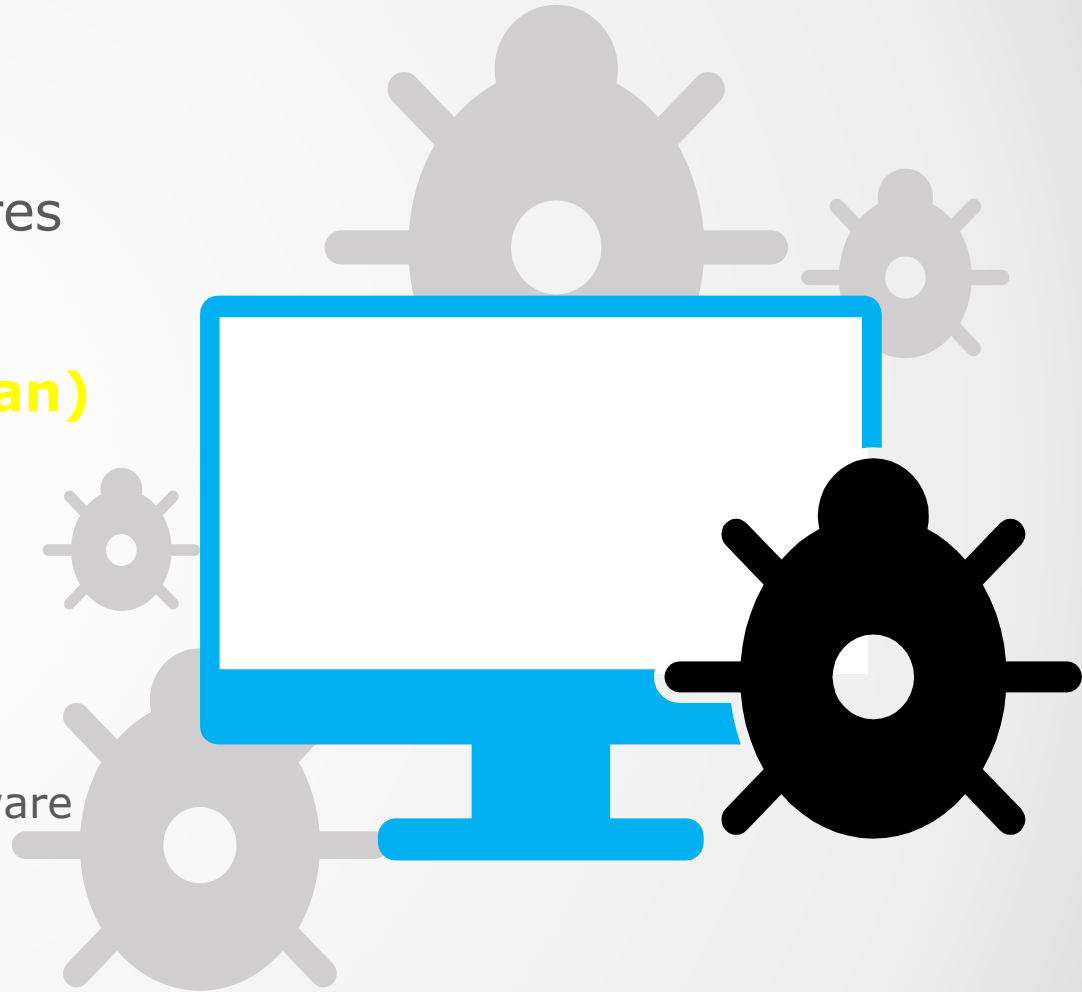
EXTERNAL VULNERABILITY

- Scan of outwardly facing hosts from the same perspective of any internal user (malicious or otherwise). Scans open ports and services.
- Scope of testing included:
  - Compare SVCE controls to industry standards
  - Identify vulnerabilities in SVCE's network, application, facilities and systems. Focus on regulatory and agency compliance.
- **Result - LOW**
- Recommendations:
  - Lock down access to only those that need network and system access
  - Patch and vulnerability management
  - Inventory and classify all assets based on business function (Asset Classification)



INTERNAL VULNERABILITY

- Evaluates the implementation of technical security controls for i.s., hosts and networks
- Intended to identify weaknesses in security measures and is essential component of overall security plan
- **Result – HIGH (1st scan) ----- MEDIUM (2nd scan)**
- Recommendations:
  - Implementation of a third-party software inventory
  - Ensuring Microsoft updates are fully applied
  - Remove or isolate outdated and/or unsupported software
  - Regular review of security bulletins and application of firmware
  - Consider regular vulnerability scanning schedule
  - Improve vulnerability process



INTERNAL VULNERABILITY

Category	Initial Assessment 3/19/2019	Rescan Assessment 5/19/2019	Cleaned
Total Critical Severity Vulnerabilities	33	8	25
Total High Severity Vulnerabilities	89	50	39
Total Medium Severity Vulnerabilities	160	51	109
Total Low Severity Vulnerabilities	9	10	+1
Total Vulnerabilities	290	119	171

ADDITIONAL FINDINGS

- Some web server and SSL vulnerabilities to be reviewed
- Server's anti-virus is turned off/missing
- Account Lock threshold is disabled, combined with a weak password, could allow dictionary attacks that would bypass alarms
- Accounts and Passwords
  - Some accounts need stronger passwords
  - Inactive accounts to be disabled
- Policies and Procedures
  - Consolidate amount of current policies
  - Develop new policies following accepted strategy

Blue = Remediated Black = Work in Progress

SILICON VALLEY CLEAN ENERGY

3. RFI RESPONSES

SILICON VALLEY
CLEAN ENERGY

RFI RESPONSES

- Staff released a Request for Information (RFI) on Cybersecurity
  - Received 3 responses
- Common themes included:
  - Strengthen vendor agreements
  - Audit current vendor contracts with a focus on data security and data handling
  - Engage CalCCA for buying power and industry streamlining

SILICON VALLEY CLEAN ENERGY

RFI RESPONSES

- Possible future RFP's to cover:
  - Information security risk assessment
  - Security awareness program
  - Incident response plan development
  - Security policy and procedure development
  - Vulnerability management program
- May collaborate with other CCA's
- FY 2019-20 budget to include increased funding for IT security

SILICON VALLEY CLEAN ENERGY

4. NEXT STEPS

SILICON VALLEY
CLEAN ENERGY

DATA SECURITY 2.0

- Strengthening IT Data Security Plan
- Customer Data
  - Re-organize all SVCE files in Box
  - Silo all customer data
    - Restrict access (IT assigns)
    - Scan workstations for customer data files currently on machine and remove
    - Encryption programs that lock/monitor files throughout lifecycle.

SILICON VALLEY CLEAN ENERGY

DATA SECURITY 2.0

- Policies:
  - Create new Data Protection/Security Policy
  - Create new AMI Data Privacy and Security Policy
  - Staff training and accountability
  - Update current IT policies
- Business Continuity
  - Identify vendors critical to operations and develop mitigation plan

SILICON VALLEY CLEAN ENERGY

THANK YOU

SILICON VALLEY CLEAN ENERGY