2021 IT Audits

Kevin Armstrong, Admin Svcs Mgr
Audit Committee
August 8, 2021

SILICON VALLEY
CLEAN ENERGY

Three Audits covering different areas

Three Separate Audits are underway / planned for 2021

1) Information Technology Audit

- Currently in Process – expected completion in September 2021

2) Advanced Metering Infrastructure Audit

- Results due to CPUC by April 2022; expected start in Nov / Dec 2021

3) Security Review and Gap Assessment

- Currently in Process – expected completion end of year 2021

Information Technology Audit

Hutchinson and Bloodgood

via

Abbott, Stringham, Lynch

- Voluntary Audit focusing on current practices, including IT controls, policies, and outside penetrations / hacking
- SVCE in its Fourth Consecutive Year
- Audit RFP process conducted in early 2021, with firm awarded contract in March 2021
- Preliminary findings available now, with final report expected in September

Advanced Metering Infrastructure Audit

Abbott, Stringham, Lynch

- CPUC Mandated Audit of Customer Meter Data
- Occurs every 3 years; current period is 2019 – 2021
- Results due to CPUC in April 2022
- Project launch targeting Nov / Dec 2021, to get ahead of the CCA queue

Security Review and Gap Assessment

Securicon

- First Assessment of this type conducted by SVCE
- More forward-looking than traditional IT audit, focusing on potential future threats, including ransomware, phishing, and other cybersecurity issues.
- Additional focus on human behavior / security, in addition to technical countermeasures

Next Steps

- The following updates today are informational, and staff welcomes Committee feedback.
- Upon conclusion of the IT Audit and Security Assessment, staff will prioritize measures.
- FY21-22 Budget has a set-aside for Cybersecurity improvements.
- Staff will share remediations confidentially with the Board, given security concerns around public disclosure of specific countermeasures.

SECURICON
Information Security Solutions

Security Review & Gap Assessment for

SILICON VALLEY CLEAN ENERGY

www.securicon.com

Agenda:

- Security Review Scope
- Security Review Methodology
- Remediation recommendation (TBD)
- Key Takeaways (TBD)

Security Review Scope

- As determined during our initial scoping call with Silicon Valley Clean Energy (SVCE) on May 4, 2021, Securicon's primary objective was:

    1. *Identify & document critical vulnerabilities that could lead to reduced integrity, confidentiality, or availability of your critical data.*
    2. *Conduct network device & architecture review*
    3. *Conduct security program review*
    4. *Provide gap analysis using NIST and other industry standards.*

Security Review Methodology

- *Network Architecture Review*
- *Security Program Review*
- *Program Briefing & Gap Analysis*

2021 IT Audit Results and AMI Review

Abbott, Stringham & Lynch
Certified Public Accountants and Business Advisors

Prepared by Steve Carter, Partner

HBCG

Prepared by Chris White, Partner

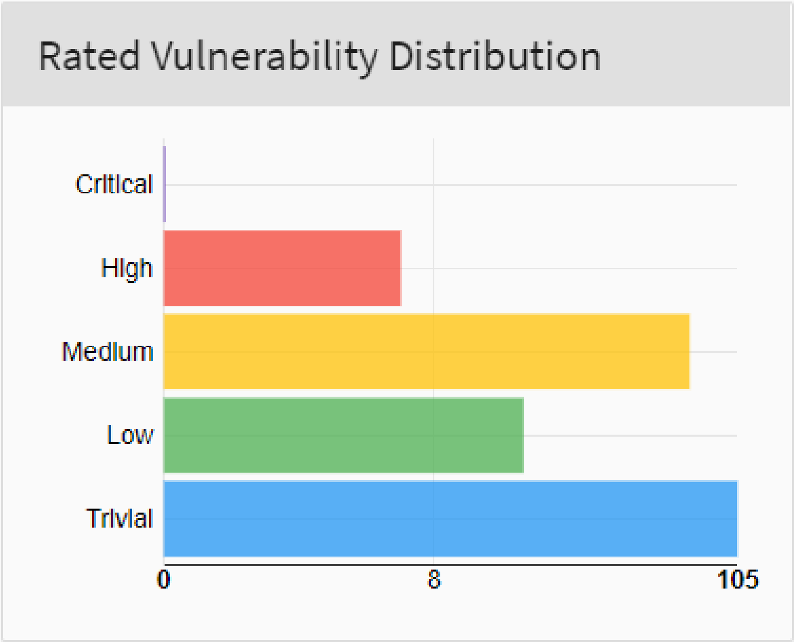
Security • Profit • Peace of Mind

IT Audit Scope

- Determine an appropriate control framework based on SVCE's size, scope, and industry.
- Evaluate SVCE's IT controls (technical and business) against the selected-and-customized framework.
- Internal and External Penetration Testing
  - Assume the perspective of a malicious actor and attempt to access the IT environment
  - Examines both external assets (websites and public IP addresses) and internal assets (workstations, servers, network devices)
- Vulnerability Assessment
  - Evaluate the configuration of key IT components including, but not limited to: Active Directory, Microsoft 365, PII/CPUC data storage, endpoint security, identity-access-and-authentication (IAM), network devices
- Information Security Program Evaluation
  - Evaluate SVCE's information security program (technical and business) against current best-practices, regulatory requirements, and the NIST CSF v1.1 framework.
  - Recommend adjustments and improvements to elevate SVCE's security posture
- Data Classification and Governance
  - Evaluate SVCE's data storage policies, procedures, and digital storage locations for appropriate user access controls with a special focus to AMI data.
- Policy and Procedure Review
  - Evaluate SVCE IT policies-and-procedures against NIST CSF v1.1 framework, AMI data requirements, and general best-practices.
  - Recommend adjustments and improvements to better reflect SVCE's technology environment, business practices, and post-COVID IT environments.

Preliminary Findings Summary

- Reviewed Email settings, DNS and SSL Certificates –advised remediations to strengthen
- Microsoft 365 is configured in accordance with recommended best-practices for security.
- Network devices are securely configured, maintained, and patched when needed.
- First-party patch management (Microsoft) is effective, Third-party patch management (Chrome, Adobe, Webex) is functioning, but needs improvement.
- User accounts are terminated in a timely manner.
- Configurations and policies such as Bitlocker encryption are effectively enforced.
- No critical vulnerabilities identified.



Preliminary Findings and Recommendations

- SVCE is better prepared than many CCAs of similar size or those affiliated with larger slow-moving municipality IT departments.
- SVCE maintains a healthy forward-looking information security approach, particularly regarding data security at third-party vendors (3PV) that is refreshing amongst organizations with access to PII.
- Storage and protection of AMI data is well-designed and executed. Depending on future growth and platforms, the additional use of SharePoint metadata and/or Azure Information Protection (AIP) should be considered to keep track of data sprawl.
- Third-party patch management is the area in greatest need of improvement, but this is true for most organizations. A number of cost-effective tools are available to address this.
- Policies, procedures, and governance documents should be reviewed annually or upon any major business or technology change to ensure they receive more frequent incremental updates than fewer “forklift” updates.
- Final report will be submitted at conclusion of audit.

Item 3
PRESENTATION

aslcpa.com | @aslcpasv

Abbott, Stringham & Lynch
Certified Public Accountants and Business Advisors

SVCE Audit Committee Presentation

By Steve Carter, CPA, CGMA, Principal

Wednesday, August 18, 2021

What Is an AMI Audit?

- AMI = Advanced Metering Infrastructure
- Determines gathering and use of Covered Information (CI) – information that can be used to identify an individual or business customer

Why We Do an AMI Audit?

- Is Covered Information properly identified and protected?
- Is CI used for Primary or Secondary Purposes?
- Review and test compliance with written policies and procedures around gathering, use, and disclosure of CI by SVCE
- IT Infrastructure in gathering, protection, and use of Covered Information – reviewed and analyzed
- To report upon compliance with CPUC's Order (Decision) involving Covered Information (CPUC Decision 12-08-045)

Time Frame for Audit

- Conducted every 3 years – Reporting Period is 2019-2021
- Audit will commence in November/December of 2021
- Report of procedures performed and findings - due date of April 30, 2022


Questions?
@aslcpasv
aslcpa.com