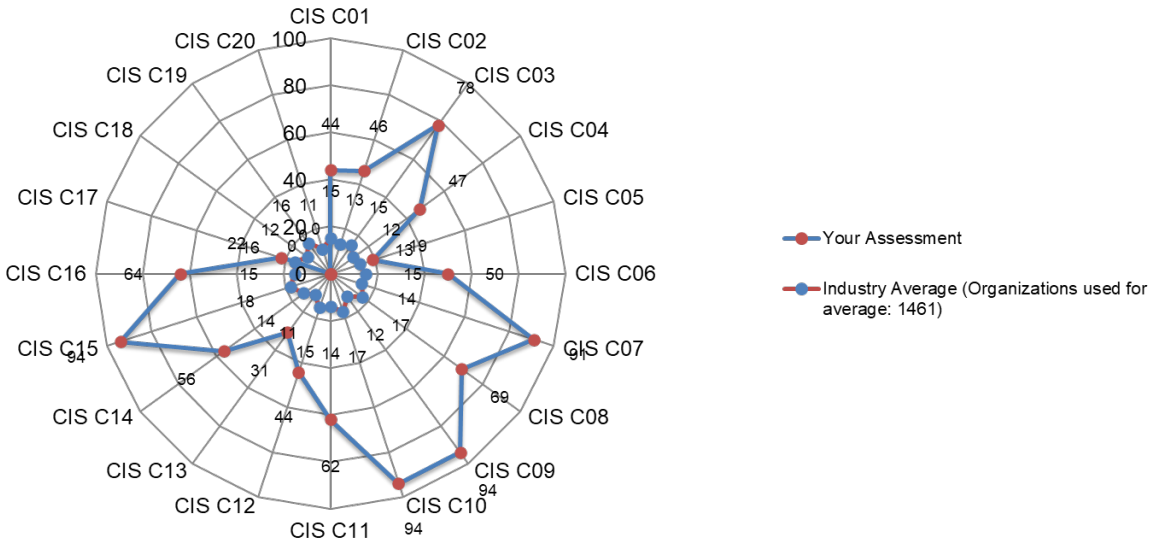
On September 21, 2020 Sajay Rai and Dr. Joe Adams of Securely Yours LLC (SY) performed an onsite survey of Client A's cyber security posture using the Critical Controls from the Center for Internet Security (CIS). Team members used the Controls Self-Assessment Tool (CSAT), an online assessment that catalogs maturity based on the 20 Critical Controls. The CIS Critical Security Controls are a recommended set of actions for cyber defense that provide specific and actionable ways to stop today's most pervasive and dangerous attacks. A principal benefit of the Controls is that they prioritize and focus a smaller number of actions with high pay-off results*. The team focused only on Implementation Group (IG) 1, this survey was conducted using the sub controls identified in Implementation Group 1, which covers the most important "cyber hygiene" activities. We recommend a follow up to examine maturity on Implementation Groups 2 and 3.

The purpose of this survey was twofold: 1) provide a snapshot of Client A cyber assessment posture; and 2) develop an annual plan for cybersecurity improvements.

Based on the survey results for CIS Controls, Implementation Group 1, Client A has better than the Industry Average benchmarks in the CSAT database in most control areas. (see Figure 1) and has a few priority items to tackle in order to improve their cyber security posture.



Survey Results

Each control area has an at-a-glance color code to indicate maturity. The basic color code: green = good | red = needs improvement

Note: summary is based on consideration of the 43 sub controls in Implementation Group 1. For a complete picture, additional follow up on Implementation Groups 2 and 3 is recommended.

Findings and Action Plan

Priority areas of potential improvement were noted:

- CC 17 Implement a security awareness and training program
  - Report: The security policy requires the existence of security awareness and training program but this program has not been initiated yet.
  - Recommendation: Develop and rollout a security awareness and training program which addresses all the controls requirement in CC17.

- CC 19 Incident Response and Management
  - Report: Although a requirement listed in security policy, there is no Incident Response plan and procedure defined and implemented.
  - Recommendation: Define and implement an incident response program (sample incident response plan attached)

- CC 5 Establish Secure Configurations
  - Report: The Minimum Baseline Standards are not defined and the client does not follow any best practices for secure configurations.
  - Recommendation: Document and implement minimum baseline standards for key technologies (e.g. Windows Servers, Firewalls etc.).

- CC 1.4 Maintain Detailed Asset Inventory
  CC 2.1 Main inventory of authorized software
  - Report: Asset inventory in place for on-premises assets. Cloud inventory is missing.
  - Recommendation: Inventory all critical applications in the cloud. Identify the business and IT owners for the applications. Create a procedure to maintain the inventory.

- CC 16 Account Monitoring and Control

- Report: The Active Directory syncs with the Cloud ERP solution but the account maintenance of all other cloud applications is not performed.
- Recommendation: Perform access review of all cloud applications and remove any dormant or unauthorized users from these applications. If possible, integrate AD with these cloud applications for authentication and authorization.

Complete Survey Results

Control	Question No.	Question Title	Policy Defined	Control Implemented	Control Automated	Control Reported
CIS C01	1.4	Maintain Detailed Asset Inventory	Written Policy	Parts of Policy Implemented	Not Automated	Reported on Some Systems
CIS C01	1.6	Address UnauthorizedAssets	Written Policy	Parts of Policy Implemented	Automated on Some Systems	Reported on Some Systems
CIS C02	2.1	Maintain Inventory ofAuthorized Software	Written Policy	Implemented on Most Systems	Automated on Most Systems	Reported on Some Systems
CIS C02	2.2	Ensure Software isSupported by Vendor	Written Policy	Implemented on Some Systems	Parts of Policy Automated	Reported on Some Systems
CIS C02	2.6	Address UnapprovedSoftware	Written Policy	Not Implemented	Not Automated	Not Reported
CIS C03	3.4	Deploy Automated Operating System Patch Management Tools	Written Policy	Implemented on All Systems	Automated on All Systems	Reported on All Systems
CIS C03	3.5	Deploy Automated Software Patch Management Tools	Written Policy	Implemented on Most Systems	Automated on Some Systems	Reported on Some Systems
CIS C04	4.2	Change DefaultPasswords	Written Policy	Implemented on Most Systems	Automated on Most Systems	Reported on Most Systems
CIS C04	4.3	Ensure the Use of DedicatedAdministrative Accounts	Written Policy	Not Implemented	Not Automated	Not Reported
CIS C05	5.1	Establish SecureConfigurations	Written Policy	Not Implemented	Not Automated	Not Reported
CIS C06	6.2	Activate AuditLogging	Written Policy	Implemented on Some Systems	Parts of Policy Automated	Reported on Some Systems
CIS C07	7.1	Ensure Use of OnlyFully SupportedBrowsers and EmailClients	Written Policy	Implemented on All Systems	Automated on Most Systems	Reported on All Systems
CIS C07	7.7	Use of DNS FilteringServices	Written Policy	Implemented on All Systems	Automated on All Systems	Reported on All Systems
CIS C08	8.2	Ensure Anti-MalwareSoftware and Signaturesare Updated	Written Policy	Implemented on All Systems	Automated on All Systems	Reported on All Systems
CIS C08	8.4	Configure Anti-MalwareScanning of RemovableDevices	Written Policy	Implemented on All Systems	Automated on All Systems	Reported on All Systems
CIS C08	8.5	Configure Devices toNot Auto-Run Content	Written Policy	Not Implemented	Not Automated	Not Reported
CIS C09	9.4	Apply Host-BasedFirewalls or Port Filtering	Written Policy	Implemented on All Systems	Automated on All Systems	Reported on All Systems
CIS C10	10.1	Ensure RegularAutomated Backups	Written Policy	Implemented on All Systems	Automated on All Systems	Reported on All Systems
CIS C10	10.2	Perform CompleteSystem Backups	Written Policy	Implemented on All Systems	Automated on All Systems	Reported on All Systems
CIS C10	10.4	Protect Backups	Written Policy	Implemented on All Systems	Automated on All Systems	Reported on All Systems
CIS C10	10.5	Ensure All Backups Haveat Least One OfflineBackup Destination	Written Policy	Implemented on All Systems	Automated on All Systems	Reported on All Systems
CIS C11	11.4	Install the Latest StableVersion of Any Security-RelatedUpdates on AllNetwork Devices	Written Policy	Implemented on Most Systems	Automated on Some Systems	Reported on Some Systems
CIS C12	12.1	Maintain an Inventory ofNetwork Boundaries	Written Policy	Implemented on Most Systems	Automated on Some Systems	Reported on Some Systems
CIS C12	12.4	Deny Communicationover Unauthorized Ports	Partially Written Policy	Parts of Policy Implemented	Parts of Policy Automated	Not Reported
CIS C13	13.1	Maintain an Inventory ofSensitive Information	No Policy	Not Implemented	Not Automated	Not Reported
CIS C13	13.2	Remove SensitiveData or Systems NotRegularly Accessed byOrganization	No Policy	Not Implemented	Not Automated	Not Reported
CIS C13	13.6	Encrypt Mobile Device Data	Written Policy	Implemented on All Systems	Automated on All Systems	Reported on All Systems
CIS C14	14.6	Protect Informationthrough Access ControlLists	Written Policy	Implemented on Some Systems	Automated on Some Systems	Reported on Some Systems
CIS C15	15.7	Leverage the AdvancedEncryption Standard (AES) toEncrypt Wireless Data	Written Policy	Implemented on All Systems	Automated on All Systems	Reported on All Systems
CIS C15	15.10	Create Separate WirelessNetwork for Personal andUntrusted Devices	Written Policy	Implemented on All Systems	Automated on All Systems	Reported on All Systems
CIS C16	16.8	Disable Any UnassociatedAccounts	Written Policy	Implemented on Some Systems	Automated on Some Systems	Reported on Some Systems
CIS C16	16.9	Disable Dormant Accounts	Written Policy	Implemented on Some Systems	Automated on Some Systems	Reported on Some Systems
CIS C16	16.11	Lock Workstation SessionsAfter Inactivity	Written Policy	Implemented on All Systems	Automated on All Systems	Reported on Some Systems
CIS C17	17.3	Implement a SecurityAwareness Program	Written Policy	Not Implemented	Not Automated	Not Reported
CIS C17	17.5	Train Workforce onSecure Authentication	Written Policy	Parts of Policy Implemented	Parts of Policy Automated	Parts of Policy Reported
CIS C17	17.6	Train Workforce onIdentifying SocialEngineering Attacks	Written Policy	Not Implemented	Not Automated	Not Reported
CIS C17	17.7	Train Workforce onSensitive Data Handling	Written Policy	Not Implemented	Not Automated	Not Reported
CIS C17	17.8	Train Workforce onCauses of UnintentionalData Exposure	Written Policy	Not Implemented	Not Automated	Not Reported
CIS C17	17.9	Train Workforce Memberson Identifying andReporting Incidents	Written Policy	Not Implemented	Not Automated	Not Reported
CIS C19	19.1	Document IncidentResponse Procedures	No Policy	Not Implemented	Not Automated	Not Reported
CIS C19	19.3	Designate ManagementPersonnel to SupportIncident Handling	No Policy	Not Implemented	Not Automated	Not Reported
CIS C19	19.5	Maintain ContactInformation ForReporting SecurityIncidents	No Policy	Not Implemented	Not Automated	Not Reported
CIS C19	19.6	Publish InformationRegarding ReportingComputer Anomalies andIncidents	No Policy	Not Implemented	Not Automated	Not Reported

FL Framework

https://www.cisecurity.org/controls/

Basic CIS Controls

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

Foundational CIS Controls

7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

Organizational CIS Controls

17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises