Technology Summary

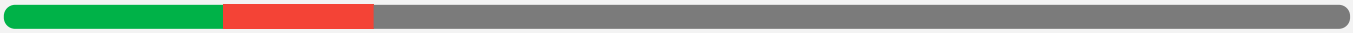
Zorg Industries

Alignment as of: 07/23/2020

Created: 07/23/2020

Overall alignment score

59%



24 Aligned 0 Marginal 17 Vulnerable 104 N/A

Alignment overview

Center For Internet Security Controls 7.1	59%
CIS Control 1: Inventory and Control of Hardware Assets	0%
CIS Control 2: Inventory and Control of Software Assets	67%
CIS Control 3: Continuous Vulnerability Management	–
CIS Control 4: Controlled Use of Administrative Privileges	50%
CIS Control 5: Secure Configuration for Hardware and Software on Mobile/Laptops/Workstations/Servers	100%
CIS Control 6: Maintenance Monitoring and Analysis of Audit Logs	0%
CIS Control 7: Email and Web Browser Protections	100%
CIS Control 8: Malware Defenses	67%
CIS Control 9: Limitation and Control of Network Ports Protocols and Services	100%
CIS Control 10: Data Recovery Capabilities	75%
CIS Control 11: Secure Configuration for Network Devices such as Firewalls Routers and Switches	100%
CIS Control 12: Boundary Defense	50%
CIS Control 13: Data Protection	0%
CIS Control 14: Controlled Access Based on the Need to Know	100%
CIS Control 15: Wireless Access Control	100%
CIS Control 16: Account Monitoring and Control	33%
CIS Control 17: Implement a Security Awareness and Training Program	83%
CIS Control 18: Application Software Security	–
CIS Control 19: Incident Response and Management	25%
CIS Control 20: Penetration Tests and Red Team Exercises	–

Alignment details

Center For Internet Security Controls 7.1

24 | 0 | 17 | 104 | 59%

CIS Control 1: Inventory and Control of Hardware Assets

0 | 0 | 2 | 6 | 0%

1.4 Maintain Detailed Asset Inventory

Review ID: 171610 Engineer: Brian Dappolone (07/23/2020) VCIO: Brian Dappolone (07/23/2020)

Question: Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all hardware assets, whether connected to the organization's network or not.

Why we are asking: Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

Business analysis: This item has been added to the strategic roadmap and will be a point of discussion at our next meeting.

Technical analysis: The customer does not have an up to date inventory of all hardware assets located inside and outside of the main facility.

1.6 Address Unauthorized Assets

Review ID: 171610 Engineer: Brian Dappolone (07/23/2020) VCIO: Brian Dappolone (07/23/2020)

Question: Ensure that unauthorized assets are either removed from the network, quarantined, or the inventory is updated in a timely manner.

Why we are asking: Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

Business analysis: This item has been added to the strategic roadmap and will be a point of discussion at our next meeting.

Technical analysis: Along with the lack of an asset inventory, unauthorized assets are not removed or noted as removed.

CIS Control 2: Inventory and Control of Software Assets

2 | 0 | 1 | 7 | 67%

2.1 Maintain Inventory of Authorized Software

Review ID: 171610 Engineer: Brian Dappolone (07/23/2020) VCIO: Brian Dappolone (07/23/2020)

Question: Maintain an up-to-date list of all authorized software that is required in the enterprise for any business purpose on any business system.

Why we are asking: Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

Business analysis: This item has been added to the strategic roadmap and will be a point of discussion at our next meeting.

Technical analysis: An up to date software list is not available.

2.2 Ensure Software is Supported by Vendor

Review ID: 171610 Engineer: Brian Dappolone (07/23/2020) VCIO: Brian Dappolone (07/23/2020)

Question: Ensure that only software applications or operating systems currently supported and receiving vendor updates are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.

Why we are asking: Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

Business analysis: None

Technical analysis: Software is supposed by the vendor and updated regularly.

2.6 Address unapproved software

Review ID: 171610 Engineer: Brian Dappolone (07/23/2020) VCIO: Brian Dappolone (07/23/2020)

Question: Ensure that unauthorized software is either removed or the inventory is updated in a timely manner

Why we are asking: Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

Business analysis: None

Technical analysis: Software records are held and maintained by the administrative assistant.

CIS Control 3: Continuous Vulnerability Management

0 | 0 | 0 | 0 | –

A review has not been completed for this category

CIS Control 4: Controlled Use of Administrative Privileges

1 | 0 | 1 | 7 | 50%

4.2 Change Default Passwords

Review ID: 171610 Engineer: Brian Dappolone (07/23/2020) VCIO: Brian Dappolone (07/23/2020)

Question: Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.

Why we are asking: The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

Business analysis: None

Technical analysis: As part of our amazing proactive services, passwords are changed when any new asset is deployed into a production environment.

4.3 Ensure the Use of Dedicated Administrative Accounts

Review ID: 171610 Engineer: Brian Dappolone (07/23/2020) VCIO: Brian Dappolone (07/23/2020)

Question: Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.

Why we are asking: The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

Business analysis: This item has been added to the strategic roadmap and will be a point of discussion at our next meeting.

Technical analysis: Admin accounts are not split for safety.

CIS Control 5: Secure Configuration for Hardware and Software on Mobile/Laptops/Workstations/Servers

1 | 0 | 0 | 4 | 100%

5.1 Establish Secure Configurations

Review ID: 171610 Engineer: Brian Dappolone (07/23/2020) VCIO: Brian Dappolone (07/23/2020)

Question: Maintain documented security configuration standards for all authorized operating systems and software.

Why we are asking: Establish, implement, and actively manage (track, report on, correct) the security configuration of mobile devices, laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

Business analysis: None

Technical analysis: This is something that we, the amazing and wonderful MSP, do on a regular basis.

CIS Control 6: Maintenance Monitoring and Analysis of Audit Logs

0 | 0 | 1 | 7 | 0%

6.2 Activate audit logging

Review ID: 171610 Engineer: Brian Dappolone (07/23/2020) VCIO: Brian Dappolone (07/23/2020)

Question: Ensure that local logging has been enabled on all systems and networking devices.

Why we are asking: Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.

Business analysis: This item has been added to the strategic roadmap and will be a point of discussion at our next meeting.

Technical analysis: Local logging was not something we thought was important and is not currently enabled. As part of the CIS review, we should enable this using Group Policy.

CIS Control 7: Email and Web Browser Protections

2 | 0 | 0 | 8 | 100%

7.1 Ensure Use of Only Fully Supported Browsers and Email Clients

Review ID: 171610 Engineer: Brian Dappolone (07/23/2020) VCIO: Brian Dappolone (07/23/2020)

Question: Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers and email clients provided by the vendor.

Why we are asking: Minimize the attack surface and the opportunities for attackers to manipulate human behavior though their interaction with web browsers and email systems.

Business analysis: None

Technical analysis: All browsers are Microsoft Edge or Google Chrome. We have disabled the installation of other browsers and Internet Explorer through Group Policy.

7.7 Use of DNS Filtering Services

Review ID: 171610 Engineer: Brian Dappolone (07/23/2020) VCIO: Brian Dappolone (07/23/2020)

Question: Use Domain Name System (DNS) filtering services to help block access to known malicious domains.

Why we are asking: Minimize the attack surface and the opportunities for attackers to manipulate human behavior though their interaction with web browsers and email systems.

Business analysis: None

Technical analysis: Use of the Umbrella platform for all of our clients.

CIS Control 8: Malware Defenses

2 | 0 | 1 | 5 | 67%

8.2 Ensure Anti-Malware Software and Signatures are Updated

Review ID: 171610 Engineer: Brian Dappolone (07/23/2020) VCIO: Brian Dappolone (07/23/2020)

Question: Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis.

Why we are asking: Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.

Business analysis: None

Technical analysis: AV and AM software and signatures is pushed through our RMM.

8.4 Configure Anti-Malware Scanning of Removable Devices

Review ID: 171610 Engineer: Brian Dappolone (07/23/2020) VCIO: Brian Dappolone (07/23/2020)

Question: Configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected.

Why we are asking: Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.

Business analysis: This item has been added to the strategic roadmap and will be a point of discussion at our next meeting.

Technical analysis: Removable device scanning is currently disabled due to speed concerns. We should look into possible quick scans or another solution to enable this efficiently.

8.5 Configure Devices Not To Auto-run Content

Review ID: 171610 Engineer: Brian Dappolone (07/23/2020) VCIO: Brian Dappolone (07/23/2020)

Question: Configure devices to not auto-run content from removable media.

Why we are asking: Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.

Business analysis: None

Technical analysis: This is configured through Group Policy.

CIS Control 9: Limitation and Control of Network Ports Protocols and Services

1 | 0 | 0 | 4 | 100%

9.4 Apply Host-based Firewalls or Port Filtering

Review ID: 171610 Engineer: Brian Dappolone (07/23/2020) VCIO: Brian Dappolone (07/23/2020)

Question: Apply host-based firewalls or port-filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

Why we are asking: Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.

Business analysis: None

Technical analysis: Windows Firewall is enabled by default using Group Policy on all domain machines.

CIS Control 10: Data Recovery Capabilities

3 | 0 | 1 | 1 | 75%

10.1 Ensure Regular Automated Back Ups

Review ID: 171610 Engineer: Brian Dappolone (07/23/2020) VCIO: Brian Dappolone (07/23/2020)

Question: Ensure that all system data is automatically backed up on a regular basis.

Why we are asking: The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.

Business analysis: None

Technical analysis: Server data is backed up to a Datto device locally and uploaded to the cloud every evening.

10.2 Perform Complete System Backups

Review ID: 171610 Engineer: Brian Dappolone (07/23/2020) VCIO: Brian Dappolone (07/23/2020)

Question: Ensure that all of the organization's key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system.

Why we are asking: The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.

Business analysis: None

Technical analysis: System backups are included in the hourly Datto backups.

10.4 Ensure Protection of Backups

Review ID: 171610 Engineer: Brian Dappolone (07/23/2020) VCIO: Brian Dappolone (07/23/2020)

Question: Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.

Why we are asking: The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.

Business analysis: This item has been added to the strategic roadmap and will be a point of discussion at our next meeting.

Technical analysis: Backups are secured on the local device using encryption, but the server room door is never locked. We have attempted to get the client to install a proper door in the past without much success. We recommend getting a proper lock as a basic security need.

10.5 Ensure Backups Have At least One Non-Continuously Addressable Destination

Review ID: 171610 Engineer: Brian Dappolone (07/23/2020) VCIO: Brian Dappolone (07/23/2020)

Question: Ensure that all backups have at least one offline (i.e., not accessible via a network connection) backup destination.

Why we are asking: The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.

Business analysis: None

Technical analysis: They are locally stored on the Datto.

CIS Control 11: Secure Configuration for Network Devices such as Firewalls Routers and Switches

1 | 0 | 0 | 6 | 100%

11.4 Install the Latest Stable Version of Any Security-related Updates on All Network Devices

Review ID: 171610 Engineer: Brian Dappolone (07/23/2020) VCIO: Brian Dappolone (07/23/2020)

Question: Install the latest stable version of any security-related updates on all network devices.

Why we are asking: Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

Business analysis: None

Technical analysis: This action is performed by our RMM.

CIS Control 12: Boundary Defense

1 | 0 | 1 | 10 | 50%

12.1 Maintain an Inventory of Network Boundaries

Review ID: 171610 Engineer: Brian Dappolone (07/23/2020) VCIO: Brian Dappolone (07/23/2020)

Question: Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.

Why we are asking: Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.

Business analysis: None

Technical analysis: A network diagram and workflow diagram and updated and maintained with every 3 month TAM visit.

12.4 Deny Communication over Unauthorized Ports

Review ID: 171610 Engineer: Brian Dappolone (07/23/2020) VCIO: Brian Dappolone (07/23/2020)

Question: Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.

Why we are asking: Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.

Business analysis: This item has been added to the strategic roadmap and will be a point of discussion at our next meeting.

Technical analysis: The owner of the company refuses to close his open RDP port because he likes to work from home. There are other secure options and he does not seem interested in spending the money or causing any downtime.

CIS Control 13: Data Protection

0 | 0 | 3 | 6 | 0%

13.1 Maintain an Inventory Sensitive Information

Review ID: 171610 Engineer: Brian Dappolone (07/23/2020) VCIO: Brian Dappolone (07/23/2020)

Question: Maintain an inventory of all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located on-site or at a remote service provider.

Why we are asking: The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.

Business analysis: This item has been added to the strategic roadmap and will be a point of discussion at our next meeting.

Technical analysis: Not all information is categorized and stored.

13.2 Remove Sensitive Data or Systems Not Regularly Accessed by Organization

Review ID: 171610 Engineer: Brian Dappolone (07/23/2020) VCIO: Brian Dappolone (07/23/2020)

Question: Remove sensitive data or systems not regularly accessed by the organization from the network. These systems shall only be used as stand-alone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed.

Why we are asking: The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.

Business analysis: This item has been added to the strategic roadmap and will be a point of discussion at our next meeting.

Technical analysis: Data resides on old desktops or filing cabinets the owner does not want to part with. It is recommended we find away to convince them to rid of these potential risks.

13.6 Encrypt the Hard Drive of All Mobile Devices.

Review ID: 171610 Engineer: Brian Dappolone (07/23/2020) VCIO: Brian Dappolone (07/23/2020)

Question: Utilize approved cryptographic mechanisms to protect enterprise data stored on all mobile devices.

Why we are asking: The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.

Business analysis: This item has been added to the strategic roadmap and will be a point of discussion at our next meeting.

Technical analysis: All hard drives are not encrypted by default. Windows 10 has the ability to enable BitLocker by default.

CIS Control 14: Controlled Access Based on the Need to Know

1 | 0 | 0 | 8 100%

14.6 Protect Information through Access Control Lists

Review ID: 171610 Engineer: Brian Dappolone (07/23/2020) VCIO: Brian Dappolone (07/23/2020)

Question: Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

Why we are asking: The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.

Business analysis: None

Technical analysis: All of these items are maintained by us, the best MSP on the planet.

CIS Control 15: Wireless Access Control

2 | 0 | 0 | 8 100%

15.7 Leverage the Advanced Encryption Standard (AES) to Encrypt Wireless Data

Review ID: 171610 Engineer: Brian Dappolone (07/23/2020) VCIO: Brian Dappolone (07/23/2020)

Question: Leverage the Advanced Encryption Standard (AES) to encrypt wireless data in transit.

Why we are asking: The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (WLANs), access points, and wireless client systems.

Business analysis: None

Technical analysis: All wireless access points require AES as the only encryption method.

15.10 Create Separate Wireless Network for Personal and Untrusted Devices

Review ID: 171610 Engineer: Brian Dappolone (07/23/2020) VCIO: Brian Dappolone (07/23/2020)

Question: Create a separate wireless network for personal or untrusted devices. Enterprise access from this network should be treated as untrusted and filtered and audited accordingly.

Why we are asking: The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (WLANs), access points, and wireless client systems.

Business analysis: None

Technical analysis: A guest network with only internet access is enabled on the company network.

CIS Control 16: Account Monitoring and Control

1 | 0 | 2 | 10 | 33%

16.8 Disable Any Unassociated Accounts

Review ID: 171610 Engineer: Brian Dappolone (07/23/2020) VCIO: Brian Dappolone (07/23/2020)

Question: Disable any account that cannot be associated with a business process or business owner.

Why we are asking: Actively manage the life cycle of system and application accounts - their creation, use, dormancy, deletion - in order to minimize opportunities for attackers to leverage them.

Business analysis: This item has been added to the strategic roadmap and will be a point of discussion at our next meeting.

Technical analysis: The owner's brother has an active account he uses when he isn't vacationing in Fhloston Paradise. He visits his vacation home there several times per year and works in the office when he is local.

16.9 Disable Dormant Accounts

Review ID: 171610 Engineer: Brian Dappolone (07/23/2020) VCIO: Brian Dappolone (07/23/2020)

Question: Automatically disable dormant accounts after a set period of inactivity.

Why we are asking: Actively manage the life cycle of system and application accounts - their creation, use, dormancy, deletion - in order to minimize opportunities for attackers to leverage them.

Business analysis: This item has been added to the strategic roadmap and will be a point of discussion at our next meeting.

Technical analysis: All but one account is disabled.

16.11 Lock Workstation Sessions After Inactivity

Review ID: 171610 Engineer: Brian Dappolone (07/23/2020) VCIO: Brian Dappolone (07/23/2020)

Question: Automatically lock workstation sessions after a standard period of inactivity.

Why we are asking: Actively manage the life cycle of system and application accounts - their creation, use, dormancy, deletion - in order to minimize opportunities for attackers to leverage them.

Business analysis: None

Technical analysis: This is enabled in Group Policy to 5 minutes.

CIS Control 17: Implement a Security Awareness and Training Program

5 | 0 | 1 | 3 | 83%

17.3 Implement a Security Awareness Program

Review ID: 171610 Engineer: Brian Dappolone (07/23/2020) VCIO: Brian Dappolone (07/23/2020)

Question: Create a security awareness program for all workforce members to complete on a regular basis to ensure they understand and exhibit the necessary behaviors and skills to help ensure the security of the organization. The organization's security awareness program should be communicated in a continuous and engaging manner.

Why we are asking: For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.

Business analysis: This item has been added to the strategic roadmap and will be a point of discussion at our next meeting.

Technical analysis: This is something we need to discuss with the client and determine the best course of action.

17.5 Train Workforce on Secure Authentication

Review ID: 171610 Engineer: Brian Dappolone (07/23/2020) VCIO: Brian Dappolone (07/23/2020)

Question: Train workforce members on the importance of enabling and utilizing secure authentication.

Why we are asking: For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.

Business analysis: None

Technical analysis: Training occurs every 6 months.

17.6 Train Workforce on Identifying Social Engineering Attacks

Review ID: 171610 Engineer: Brian Dappolone (07/23/2020) VCIO: Brian Dappolone (07/23/2020)

Question: Train the workforce on how to identify different forms of social engineering attacks, such as phishing, phone scams, and impersonation calls.

Why we are asking: For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.

Business analysis: None

Technical analysis: Training occurs every 6 months.

17.7 Train Workforce on Sensitive Data Handling

Review ID: 171610 Engineer: Brian Dappolone (07/23/2020) VCIO: Brian Dappolone (07/23/2020)

Question: Train workforce members on how to identify and properly store, transfer, archive, and destroy sensitive information.

Why we are asking: For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.

Business analysis: None

Technical analysis: Training occurs every 6 months.

17.8 Train Workforce on Causes of Unintentional Data Exposure

Review ID: 171610 Engineer: Brian Dappolone (07/23/2020) VCIO: Brian Dappolone (07/23/2020)

Question: Train workforce members to be aware of causes for unintentional data exposures, such as losing their mobile devices or emailing the wrong person due to autocomplete in email.

Why we are asking: For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.

Business analysis: None

Technical analysis: Training occurs every 6 months.

17.9 Train Workforce Members on Identifying and Reporting Incidents

Review ID: 171610 Engineer: Brian Dappolone (07/23/2020) VCIO: Brian Dappolone (07/23/2020)

Question: Train workforce members to be able to identify the most common indicators of an incident and be able to report such an incident.

Why we are asking: For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.

Business analysis: None

Technical analysis: Training occurs every 6 months.

CIS Control 18: Application Software Security

0 | 0 | 0 | 0 –

A review has not been completed for this category

CIS Control 19: Incident Response and Management

1 | 0 | 3 | 4 | 25%

19.1 Document Incident Response Procedures

Review ID: 171610 Engineer: Brian Dappolone (07/23/2020) VCIO: Brian Dappolone (07/23/2020)

Question: Ensure that there are written incident response plans that define roles of personnel as well as phases of incident handling/management.

Why we are asking: Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.

Business analysis: This item has been added to the strategic roadmap and will be a point of discussion at our next meeting.

Technical analysis: This is something that needs to be figured out.

19.3 Designate Management Personnel to Support Incident Handling

Review ID: 171610 Engineer: Brian Dappolone (07/23/2020) VCIO: Brian Dappolone (07/23/2020)

Question: Designate management personnel, as well as backups, who will support the incident handling process by acting in key decision-making roles.

Why we are asking: Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.

Business analysis: This item has been added to the strategic roadmap and will be a point of discussion at our next meeting.

Technical analysis: None

19.5 Maintain Contact Information For Reporting Security Incidents

Review ID: 171610 Engineer: Brian Dappolone (07/23/2020) VCIO: Brian Dappolone (07/23/2020)

Question: Assemble and maintain information on third-party contact information to be used to report a security incident, such as Law Enforcement, relevant government departments, vendors, and Information Sharing and Analysis Center (ISAC) partners.

Why we are asking: Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.

Business analysis: None

Technical analysis: Documentation is held in our office, the office of the best MSP in the universe.

19.6 Publish Information Regarding Reporting Computer Anomalies and Incidents

Review ID: 171610 Engineer: Brian Dappolone (07/23/2020) VCIO: Brian Dappolone (07/23/2020)

Question: Publish information for all workforce members, regarding reporting computer anomalies and incidents, to the incident handling team. Such information should be included in routine employee awareness activities.

Why we are asking: Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.

Business analysis: This item has been added to the strategic roadmap and will be a point of discussion at our next meeting.

Technical analysis: Does not occur.

CIS Control 20: Penetration Tests and Red Team Exercises

0 | 0 | 0 | 0 | –

A review has not been completed for this category