1. MSPNetworks has implemented various layers of protection to help minimize Cybersecurity vectors into your organizations data and IT systems. A listing of these layers are as follows

- We have worked with your organization to ensure server and network equipment exist in rooms with self-closing, locked doors, or in locked network cabinets.
- We have employed Sophos NGFW firewall's protecting the local area network at the edge. This also consists of Malware prevention, intrusion prevention and content filtering policies guarding traffic coming in and out of the network.
- In addition to the NGFW firewalls, we have industry leading software from Sophos to protect the Servers. Intercept X Advanced with EDR provides endpoint detection and response, anti-ransomware, exploit prevention, and managed threat response. In addition to these features, the endpoint protection works directly with the firewall to mitigate ransom-ware attacks and cryptos.
- We have deployed Webroot Secure Anywhere Antivirus to all workstations and macs. Webroot is configured for auto-quarantine/cleaning and creates a service ticket for issues that cannot be resolved.
- We have forced multi-factor authentication across the board for all organizational users using Office365/Gsuite to help mitigate phishing and other account compromises.
- Backups of data exist encrypted in motion as well as at rest. This is true for off-site backups. Local Backups are taken multiple times a day. Off-site backups are taken once a day.
- File access is controlled using Active Directory role-based permissions. AD account status is audited on a quarterly basis. Unused/stale accounts are purged to minimize attack vectors.
- Server and workstation updates are controlled by our RMM Platform which also reports on update failures and allows us to resolve update challenges in a quick manner.
- Barracuda Email Security Service protects against phishing, malware, ransomware, and other sophisticated, email-borne threats. Its multi-layered, cloud-hosted scanning engines include Barracuda Advanced Threat Protection, which combines behavioral, heuristic, and sandboxing technologies. This technology is applied to incoming email.
- Barracuda Essentials data loss protection and email encryption keeps sensitive data—such as credit card numbers, social security numbers, HIPAA data, and more—from leaving your organization. Content policies can automatically encrypt, quarantine, or even block certain outbound emails based on their content, sender, or recipient. This technology is applied to outgoing email.
- Dark Web Monitoring helps prevent a cybersecurity breach due to compromised employee credentials by monitoring the dark web in real time, and automatically alerting when it is time to change passwords because their credentials are up for sale on the Dark Web.
- MSPNetworks works with the admin team to deploy simulated phishing attacks and security awareness training campaigns to educate employees, making them the best defense against cybercrime.