

# Ransomware Attack Protection

## Security Best Practices



### Highest Priority: What MSPs should do now

#### Identify and Access Management

- Conduct an audit of all technology solutions, user accounts, and roles. Repeat this process on a quarterly basis (at least).
- Disable accounts upon employee technology offboarding, or update permissions and access upon role change.
- Disable inactive or underutilized employee accounts if they are unused or inactive for long periods of time.
- Use a password manager to create strong, unique passwords per technology solution and enable multi-factor authentication (MFA) on the password manager. Do not allow storage of credentials in a web browser.

- Protect any API keys in use.

- Use different keys for different integrations, rotating them periodically.
- Use IP restrictions where possible.
- Store keys securely.
- Enable MFA on all accounts that are allowed to via API keys anywhere they are configured for use.



## Network Access

- Restrict RDP access to LAN only - do not configure internet access to RDP.
- Use a VPN to restrict access to admin tools (RMM, Remote Access, etc.) Use MFA on the VPN.



## Patching Your Channel Technology

- Update all endpoints and technology software to versions that are free of known material vulnerabilities.
- Review vendor practices for discovery, patching, and notification of vulnerabilities.



## Protection of Local and Cloud Backups

- Act on your vendors' recommended guidance or best practices for the protection of your backup technology
- Move away from shared login accounts on appliances and technology portals.
- Enable MFA on access to technology portals and appliances.
- Store copies of backups offsite, or in an isolated network or file share location that is inaccessible from servers or workstations, thus making backups harder to access, encrypt, or destroy.
- Monitor and alert for backup deletion. Some vendors offer "soft" delete so backups are not immediately removed. Understand your vendors' capabilities.
- Test your backups. Determine how long it takes to do a restore, and set accurate expectations should the need arise.



# Lower Priority: Items to consider when expanding security best practices

## Identify and Access Management

- Monitor accounts for exposed credentials using free or commercial tools.
- Conduct phishing simulations and training campaigns for both MSP staff and clients
- Consider device trust or network IP whitelists for accessing technology portals and appliances.
- Avoid shared accounts. MFA is designed for a single user. As a result, it is difficult to manage shared accounts.
- Make sure techs follow your policies on storage and MFA for these tools!

## Network Access

- MSPs whose clients are an extension of the MSP's network should reconsider this design choice as one customer or MSP compromised = game over for all clients.
- Vendors that have site-to-site VPNs (L2Ls) into an MSP network to augment staff or technology should have their network security vetted and access controls on L2Ls should be tightly limited.
- Consider the time of day restrictions for access to RA VPN endpoints.



## Leverage Your Relationships to Gain Intelligence on Current Threat Environment

- Talk to your vendors about what they are seeing and what their road map is to address shifts in the cyber landscape.
- Partner with vendors and other MSPs to collaborate on how to best configure your technology to mitigate cyber threat risks.
- Join a peer group, and start discussions with other MSPs to learn about their best practices.
- If you've been attacked and your business has survived, share your knowledge.

## Cybersecurity Insurance

- Invest in cybersecurity insurance, but do not make the fact you have it public knowledge.
  - Extortion coverage should cover your business into the low to mid-six figures.
  - Verify that there are no wartime exclusions with your carrier.
  - Verify that the insurance carrier will pay for a preferred incident response and forensics provider, or become comfortable with and accept the one the carrier offers.
- Understand prior acts, exclusions, and timelines for each of these policy areas.
- Run an MSP ransomware attach tabletop scenario with the broker and carrier to understand the limits of coverage based on a real-world scenario.