# Preventing Ransomware [Checklist]

*Make sure you are covering as many attack angles as possible to minimize the possibility of a ransomware attack.*

## Software Appliances

- [ ] Make sure that every remote user logs in and works from a VPN.
- [ ] Firewall is properly installed and active.
- [ ] Use the latest generation endpoint protection measures. (Can also be combined with white-listing, real-time executable blocking, etc.)
- [ ] Create a dedicated anti-spam/anti-phishing system and communication plan
- [ ] Routinely run software updates (and patches) for all applications and the OS. Respond quickly to software vendor vulnerability alerts.

## Backup Solutions

- [ ] Implement a sophisticated backup solution. It can be either software-based or hardware-based, or a combination of the two.
- [ ] Perform regular testing of your recovery functions and several months of your data to ensure it's not already compromised.
- [ ] Check if your backup solution is covering all of your data, and if it can be easily accessed.

## Theft Prevention

- [ ] Track data movements via system logs
- [ ] Implement data encryption technologies
- [ ] Acquire and use extensive Data Leak Prevention (DLP) tools.
- [ ] Analyze your network traffic to search for unusual data movements
- [ ] Use the method of least permissions to protect your databases, folders, and singular files (Users' permission levels are commensurate with their ability to do their work.)

## Company Communication

- [ ] Regularly conduct simulated phishing attacks to test and educate your staff.
- [ ] Provide education and training about phishing emails and suspicious applications.
- [ ] Provide clear instructions on what to do if a malicious application or email is engaged by an employee.

**If you have questions or concerns about the vulnerability of your data, or need assistance in dealing with ransomware, please contact us: 616.244-2630 or info@trc-group.com**