Petronella
TECHNOLOGY GROUP

# Ransom Protection Checklist

For full protection from ransomware like Cryptolocker, make sure you have all these items in place.

☐ Have an Enterprise-Quality Backup System

- Do you have a good image backup system that you are 100% confident is working?

  Carbonite, DropBox, and many other types of cloud storage are not enough. Do you know about the weaknesses in your backup system?

- Are you using external USB hard drives or devices connected to a server to backup? If these devices are connected to the server, they can still get infected with the Cryptolocker and similar viruses.
- Are you backing up several times per day?
- Are you performing a restore test from backup at least monthly?

☐ Have a Modern Firewall

- Do you have a Unified Threat Managed Firewall? (http://en.wikipedia.org/wiki/Unified_threat_management)
- Do you have a Website Content Filtering Service?
- Do you have a firewall on your computer enabled?

☐ Have Modern Anti-virus

- Do you have a Cloud Antivirus and Antispam Filtering Service?

  Does your Cloud Antivirus/Filtering Service scan and filter links inside emails to ensure safety?

- Does your antivirus software integrate with your email client software and scan all incoming emails?
- Do you have Antivirus Software with Real-Time Heuristic Scanning (Anticipates new virus behavior) enabled?
- Do you have Antivirus Software that includes malware protection?
- Does your antivirus software automatically update itself at least every hour? If not, you should manually check for updates regularly.

Don't take chances.

Call for a free
**9-minute Cryptolocker Safety Review.**

**877.412.1112**

☐ Have a Process for Regular Updates

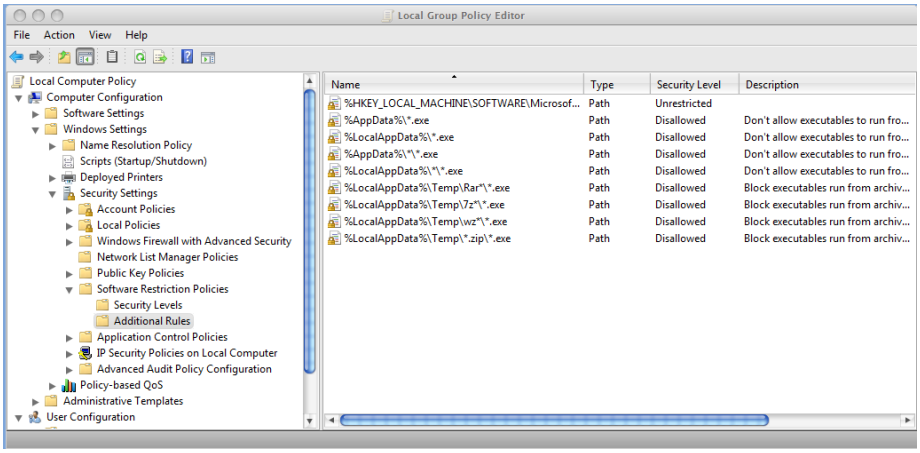
- Do you have a process to patch your operating system and applications? Reboot. Repeat. Keep checking and installing all patches until when you check again there are none left.
- Are you sure you're patching all Adobe software & Java?
- Are you sure you're using the latest web browser for Internet Explorer, Firefox and Google Chrome?
- Do you have Windows Update setup properly?

☐ Have an Employee Security Awareness program.

- Are your users aware of good security practices?
- Do your users notice email attachments that they weren't expecting or from people they don't know well? Do they know what to do next?
- Do you have an Employee Security Awareness program, and a quarterly lunch on security awareness?

☐ Implement Security Policies

- Do you use your computer with the administrator account?
- Do you have the right Software Restriction Policies (SRPs) to prevent the execution of certain programs through the use of group policy?
- Are the Cryptolocker SRP protection rules in place?



**Resources**

If you are a do-it-yourself person and want to do the work to protect yourself against Cryptolocker and other ransomware, below are resources with all the details. Be sure to complete all the steps.

- http://technet.microsoft.com/en-us/library/cc786941(v=ws.10).aspx
- http://www.bleepingcomputer.com/virus-removal/cryptolocker-ransomware-information - prevent

Ensure you are protected.

Call for a free

**9-minute Cryptolocker Safety Review.**

**877.412.1112**