UNDERSTANDING RANSOMWARE IN 5 MINUTES

OVERVIEW

One of the fastest and newest growing threats to business data is Ransomware. This new threat can completely lock out your systems and demand a payment for the recovery of your data. The data is encrypted with a strong password which in most cases cannot be removed.

There is no single application or a technique that can prevent Ransomware. Instead, there are guidelines and data backup strategies that must be follow to reduce or even prevent Ransomware.

PREVENTION

The following guidelines should be followed at all times in order to protect the system against Ransomware.

- Utilizing UAC: UAC or user account control prevents users from accidently downloading malicious software. Any software installs must require an additional password or authentication process.
- Antivirus: While Antivirus application cannot detect 100% of the Ransomware, they do help. All systems must have fully up to date and active Antivirus installed.
- System Patches: All systems must be kept up to date via security updates and patches.
- Dual Destination Backup: Business must deploy a dual destination backup system, i.e BusinessBlackBox.com. This type of system can replicate critical data to local storage along with secure cloud storage.

AFTER THE INFECTION

After a Ransomware infection, your first task should be to locate and isolate the system that caused that infection. This system should then be properly repaired by an IT Engineer.

If your data is encrypted by Ransomware, your best bet will be to delete this data and restore the most recent copy from your backup. If you have deployed a BusinessBlackBox system, you will have the ability to restore data going back days or weeks based on your needs.