Ransomware Checklist

Ransomware is a form of malware that keeps your data encrypted until ransom is paid. It comes in many variants (such as CryptoLocker, Petya, and WannaCry), but it's constantly evolving, making it very difficult to protect against. And although the average amount of ransom requested is $4,300, the average cost of downtime from a single attack can be as high as $46,800! So what should you do if you are hit by ransomware? Use this checklist to ensure you are taking the right steps:

☑ Shut down infected systems immediately

To avoid ransomware spreading, disconnect the infected device from any network it is on and turn off any wireless capabilities such as Wi-Fi or Bluetooth. Unplug any storage devices such as USB or external hard drives.

☑ Have an incident response plan

It's not if, it's when you have an incident. Make sure you have a clear plan and professionals to call to respond to cybersecurity incidents.

☑ Report the incident

You should let your organization know about the attack, but it's also important to report it to the FBI or your local authorities depending on where you are located. This is to help them gain an understanding of ransomware and its impact on victims.

☑ Evaluate your options

If you don't have a backup solution, your other options are to do nothing (lose your data) or decrypt your files using a 3rd party decryptor. If all else fails, you can pay the ransom, but beware of this option as it increases the chances that you'll be targeted again.

☑ Prevent future ransomware attacks

The first step in preventing future ransomware attacks is to educate your employees on cybersecurity awareness. You should also invest in endpoint security with a firewall or third party service that protects against ransomware. Finally, you should implement a business continuity plan. While business continuity can't prevent ransomware from attacking, it can prevent it from succeeding..

VISUAL EDGE IT™
SECURE TECHNOLOGY SOLUTIONS

www.visualedgeit.com | learnmore@visualedgeit.com