Prepare For A Cyber-Attack Now—Don’t Wait!

Karl Kispert, GRASSI & CO (May 15, 2018)

Things you can do now to help prevent ransomware attacks. Ransomware is a type of malicious software designed to block access to your computer system until a sum of money is paid.

Ransomware is a type of malicious software designed to block access to your computer system until a sum of money is paid.

According to Malwarebytes Cybercrime Tactics and Techniques 2018 Report, ransomware for businesses, of all sizes, is up 28%in the first quarter of 2018.

2018 ransomware attacks continue. A few examples are:

- The City of Atlanta – The mayor said we are “held hostage” as hackers demanded $51,000. It is not known if they paid the ransom, however the City had to pay $2.7 Million in emergency funding within a few weeks of the attack. Many services were disrupted and took weeks to restore.
- Hancock Health in Indiana had a hacker shut down all patient records and company emails. They did pay the $55,000 ransom as they felt, “we had no choice.”
- Erie County Medical Center in Buffalo, NY, the hackers wanted $30,000 – hospital officials refused to pay. Hackers wiped about 6,000 of the hospitals computers taking the staff about six weeks to get up and running again, and causing employees to have to keep handwritten records. Officials said it cost them $10 million to recover from the attack including money spent on hardware and software to rebuild the hospital's computer system, as well as overtime pay and lost revenue.

Things you can do now to help prevent ransomware attacks:

- Provide security awareness to anyone accessing your IT environment to prevent the number one cause: Phishing – Humans continue to be the weakest link. You need to go beyond training and make them aware so that it will become part of the security culture
- Back up your data daily – the best way to recover from a ransomware attack is to have backups ready to use when you are held hostage
- Patch software immediately - when fixes are made available, do not wait. Update your software so hackers cannot exploit a vulnerability
- Limit the number of people who can install software. Too many cooks spoil the broth. You need to trust that people are doing the right thing when installing and updating software
- Use a reputable antivirus software. AV is one step that will lower your chances of being attacked with ransomware

Security monitoring of your network must be in place. You MUST be aware of what is happening in your network and performing 24x7x365 monitoring, which will help ensure you are actively looking for the bad guys

- Who has access to what and why must be understood. A proper identity and access management program allows you to provide access to your critical applications by only those who should have it
- Use two-factor authentication. Gone are the days of just a single password. Having two forms, such as a password and a bio metric, to access your network is required to provide added assurance

While nothing is foolproof, taking preventive measures may help maintain your brand, ensure you retain your customers, and prevent a cyber-breach.

For more information or assistance with your Cyber and Information Security (CIS) Program, contact Karl Kispert, Grassi & Co.’s CIS Practice leader, at kkispert@grassicpas.com or 212-223-5037.

Links
[1] http://iitaly.org/files/global-ransomwarejpg-1