CYBERSAFE SOLUTIONS

The Cost of a Ransomware Attack

A ransomware attack is like a digital hostage situation. Cybercriminals use a type of malware that encrypts or locks a user out of their computer network, keeping you from your data. The user only regains access to their files once a payment is made. In some cases, the victim may not get all their information restored, even after the money is sent, usually in the form of a cryptocurrency. As a scare tactic, attackers often give the victim a limited amount of time to pay.

Ransomware By The Numbers

- Experts predict there will be a ransomware attack on a business **every 11 seconds** by 2021
- Global ransomware damage costs will reach **$20 billion** by 2021
- In 2019, **205,280** organizations submitted files that were hacked in a ransomware attack – a **41%** increase from the year before
- Ransomware generates **over $25 million** in revenue for hackers each year
- Most companies take **nearly six months** to detect a data breach, even major ones
- In 2019, ransomware attacks cost the United States over **$7.5 billion**. Global damages cost organizations an estimated **$11.5 billion**

The Cost & Recovery of a Ransomware Attack

- Ransomware attacks cost businesses an average of $84,116.
- The file decryption process can take days to complete.
- This process must be completed by experts.
- 75% of businesses are without their files for two or more days. 30% of those are without them for five days or more.
- A few days of unavailable files often translates to weeks of lost productivity as the business recovers.

The Repercussions May Not End There

A new risk associated with ransomware is emerging that could make recovery more expensive for businesses. Cybercriminals are now downloading copies of the victim's files and threatening to release them publicly if the ransom isn't paid. This new complication brings forth the potential of 3rd party claims, as a result of a data breach.

Steps to Prevent A Ransomware Attack

Below are some best practices organizations can follow:

- Always consult in your trusted IT advisor and cybersecurity specialist
- Test your back up system to ensure a quick recovery; however, having a back up in place is not 100% reliable and a business should never count on them alone
- Understand what your risks are
- Develop Security Policies
- Provide employees with SOL Training and Simulated Phishing Tests
- Ensure you have implemented 24/7/365 network and endpoint security monitoring – the most critical step

About Cybersafe Solutions
Cybersafe Solutions is a state-of-the-art managed security provider, specializing in 24/7/365 network and endpoint monitoring services. They provide global clients SOC-as-a-Service through managed detection, response, and containment. Their team of certified specialists have more than 20 years of experience in the cybersecurity space and is ready to protect your most important assets.