Ransomware: Should I Pay?

Ransomware is one of the fastest growing cyber-crimes because it's one of the most profitable. Unlike other malware that a hacker may or may not be able to monetize, ransomware is a direct path to getting paid through extortion.

The Ransomware Business Model
Today's sophisticated ransomware scams are based on a proven business model that often times will even come with tech support websites to make sure you get your data back.

The criminals know that if word got out that paying the ransom did not result in getting your files back, no one would ever pay.

There is no guarantee, however, that if you pay the ransom, you will get your files back as we don't have any credible data to work with. Most companies that have been hit with this attack don't want the word to get out, much less admit that they paid the ransom but didn't get their data back.

A couple of things are certain: paying the ransom is risky and absolutely encourages them to continue attacking others.

Before You Consider Paying
There are a number of steps you can take before you have to decide whether you should pay the ransom or not.

The easiest way to avoid having to pay the ransom is by having a solid backup that isn't connected to your computer or company network.

If you do have an uninfected backup that can be restored, removing the infection and the encrypted files is pretty easy to do by anyone with even moderate technical skills.

Which Ransomware Do You Have?
If you don't have a current backup, there may be tools available that can break the encryption if you were hit with one of the older or less sophisticated strains of ransomware that have been cracked.

A website called https://NoMoreRansom.org has created a repository of keys and applications that may be able to decrypt your files.

To help determine which strain you're infected with, you simply upload a couple of the encrypted files along with some of the details within the ransom demand note.

For security reasons, make sure to choose files that don't contain any sensitive personal or corporate information (picture files are usually a good choice to use for the upload test).

Protection Tip
First and foremost in protecting against this growing threat is the proper backup strategy.

Unfortunately, a traditional external backup drive isn't good enough because anything that's connected to your computer or is available through a network share will be encrypted as well.

Even if you routinely disconnect your external hard drive when you aren't backing up, you're still not fully protected as this malware runs silently in the background so you could unknowingly overwrite your good files with encrypted files.

The best backup solution physically stores your files separate from your computer and incorporate 'file versioning', which means it keeps multiple copies of the same files as they are changed.

Incorporating a cloud-based backup such as Carbonite (https://goo.gl/XKum9f) provides the best protection against not only ransomware but fire, flood, theft and even employee sabotage.