AUTOMATED
BUSINESS SOLUTIONS

The Ransomware Threat

The truth is that hackers think very carefully about the return on investment for their efforts. Most of us have heard about giant retailers, banks, credit card providers, and email service providers being hacked with devastating results. From the risk-reward perspective, these companies have become high-risk-but-high-return targets. Large companies will remain big targets, but they will generally be pursued by very sophisticated actors.

Today, many hackers are seeking out easier targets. Usually, these are somewhat smaller organizations who do not realize they are potential targets, or simply do not have the resources to protect themselves. You might say, “Our business information is confidential and pretty valuable to us, but it’s not worth a hacker’s time to steal.” The emergence and ubiquity of ransomware, however, has made every piece of business data worth targeting.

What is ransomware?

Ransomware is essentially a software program (a.k.a virus) that prevents individuals or organizations from accessing their data, usually until they pay a sum of money. Many times there is a set, short timeframe in which they can deliver this money. After that deadline, data will be permanently deleted or encrypted. The most common form of ransomware is called CryptoLocker.

Example of a ransomware message

The effects of ransomware are being widely felt, as it makes any sort of personal or business data valuable. For example, your company's financial records might have little value to a hacker or for resale on the Internet. But they are very valuable to your organization.

Due to this value, the person or entity behind the ransomware attack hopes you will make a substantial payment. This same strategy could be used for human resources records, customer information, or other proprietary information your company generates as part of your business. This means basically all digitally stored information is a potential target.

How should organizations address ransomware and other IT security threats?

If your organization is one of the many small and medium sized businesses (SMBs) that generate data, then you should seriously consider how this data is protected. Most small and medium businesses (even those with an IT department) are going to have a hard time addressing such a difficult topic as security.

Fortunately, there are IT services organizations with security expertise and knowhow specific to SMBs. They provide services in a variety of forms, whether it's advisory/strategic, for a specific project, or ongoing monitoring, that can be crafted to your needs and budget. Organizations with managed security services included in their managed service contract are 50% less likely to suffer from a ransomware attack.

Whatever your industry or business size, it is worth approaching a company that offers IT infrastructure assessments to at least understand where you stand, and what your options are. From there you are better positioned to decide if managed IT security services is right for you.