SOBEL & CO. LLC
CERTIFIED PUBLIC ACCOUNTANTS & ADVISORS

An Interview With Jim Mottola on the Recent Global Ransomeware Attack

Over the course of the weekend, I think most of us heard the news of the worldwide Ransomware attack on over 200,000 individuals across 150 countries. According to Jim Mottola, Sobel & Co.'s Director Forensic Investigations & Risk Mitigation Services, this something that should concern small to mid-size businesses in the US.

Every business owner should be concerned with any attempt by criminals to steal their information. The latest attempt to compromise users with Ransomware was unique in that it was focused on unpatched, updated versions of older Microsoft systems, which increased the likelihood and impact of its effectiveness.

While Ransomware is nothing new lately these attacks have become more common. Actually, the prices of Ransomware demands and subsequent payouts have been going down because the barriers to entry into "this type of attack" have become easier to get around. As a result, the attacks are more frequent.

Businesses can protect themselves from these types of organized or sophisticated events by launching "Defense in Depth." This approach means that you must adopt multiple measures in a layered approach. The first step is to make sure your data is backed up and protected via an encryption method. If this is not your area of expertise, seek assistance from a trusted advisor, to point you in the right direction. Next, install patches or updates to all your devices upon request. Although sometimes we avoid these because they seem too time-consuming, they are important. Thirdly, updating your Anti-Virus software is another recommended method by information security experts.

Owners should not ignore the importance of employee training as a key part of defense in depth. Regularly instructing employees to think before clicking can be very useful and reduce overall risk especially because in the vast amounts of previous cyber events, employee behavior was a key factor. (Nonetheless, in this latest version of Ransomware, it would not have been helpful.)

Jim has suggested a range of resources to help business owners learn more about how to be prepared and then what to do to respond to a Ransomware event.

Knowbe4, an information security awareness training company, published a Ransomware Hostage Rescue Manual last year that is a good way to become familiar with this issue. But doing it yourself is not necessarily the best approach. In fact, finding an IT professional who can assist your specific business would be a step in the right direction. Knowing what questions to ask and conducting audits of their work by a third party can also provide you a level of confidence in your preparedness. Here are two strong articles that provide good information and resources:

https://www.nytimes.com/2017/05/14/world/europe/cyberattacks-hack-computers-monday.html?hp&action=click&pgtype=Homepage&clickSource=story-heading&module=first-column-region&region=top-news&WT.nav=top-news

http://money.cnn.com/2017/05/13/technology/ransomware-attack-protect-yourself/