NO N.I.C.E. WAY TO DEAL WITH RANSOMWARE ATTACKS

More Cyber Attacks are coming. Are you prepared?

Russia has vowed to engage in a Cyber war on all NATO countries that are assisting the Ukraine in their war with Russia. All NATO countries are taking these threats seriously, so should you. Let's look at the N.I.C.E. ways currently being employed by most companies.

N…..Not going to happen to me. If you'll pardon the pun, that's playing Russian Roulette with your business. Small to Medium business is a prime target of hackers. In fact, 60% of all businesses suffer a Cyber attack for many reasons, mostly because they are easy targets without the budget to install the anti-cyber attack software necessary to detect and prevent the majority of cyberattacks.

I.....Insurance. I have Ransomware insurance that will pay any Ransomware demand should I get hacked. Well, there are several problems with that strategy. Ransomware is becoming much more difficult to obtain. Even if you can find a market, the limits are reduced, and the price is 200-300% higher than last year.
Plus of course the limit is usually an aggregate amount, meaning that once the policy limit is used up, you're on your own when the next attack occurs.
Will you I get hacked again? Probably "yes", the chances of being hacked again after paying a Ransomware is a staggering 80%.

C…..Cyber Security software. A lot of companies spend a large part of their budget on Cyber Security. Is it effective? Yes. Is it foolproof? No. While a lot of the detect and prevent cyber software is very effective, the sad truth is that none can be 100% effective in preventing a cyber hacker from penetrating the defense in place. The US Department of Defense was hacked, CNA Insurance was hacked, the Government of Ukraine was hacked. Is your cyber software better than theirs, probably not?

E…..Expectations of data recovery. Most companies have back-up servers and/or keep their data in The Cloud, which they feel is sufficient in recovering their data in the event of an attack. While the data will eventually be recovered, it takes a lot of time, expense, and manpower. Speed is of the essence in maintaining "business as usual" and even if the ransom demand is paid, it could be some time before you are given the "key" to unlock the encryption and get your data back.

Fortunately, there is a solution. Your association has partnered with NeuShield Data Sentinel www.neushield.com to offer broker members and their customers the ability to instantly recover any encrypted data without ever having to pay Ransomware.

Ken Rayner CIP, CCIS
President, Cyber Insurance Solutions
www.cyberinsurancesolutions.ca
CIS is the Worldwide Master Distributor
NeuShield, Insurance Services