The Real Truth of Cyber Insurance.

A Realistic Editorial View

By Stephen Turner
President of Managed Security Services
Longevity Technology
www.longevitytech.us

Insurance, a wonderful concept in practice designed to save us from financial disaster or to help us rebuild when things go “really” wrong. From health insurance, dental insurance, auto insurance, life insurance, homeowner’s insurance, consumer insurance, etc. over the past couple years we have seen the emergence of a new form of insurance called cyber insurance.

Now corporations big and small can purchase cyber liability insurance that protects them if their network or computer systems are compromised by a nefarious individual or group. Since the development of the concept of cyber insurance, large companies have been gobbling it up as quickly as possible to protect their financial investments and the penalties that can come when a company is compromised.

Lately, this form of insurance has also been seeing its way into the small and medium-size business sector. Whereas the large enterprise will combine cybersecurity efforts including hardware, software, staff and even outside consultation, I am starting to see a troubling trend in the small medium-size business sector where they are leaning on cyber insurance as a fallback rather than protecting their environment with cybersecurity solutions.

The idea is that if we take the basic form and first line of defense in true cybersecurity, the vulnerability assessment, and perform said assessment on a quarterly basis this can cost a small to medium-size business anywhere from $15,000-$25,000 annually. On the same note a cyber insurance company will come in and write them a multimillion-dollar protection policy and charge them a couple hundred dollars a month.

The executive teams in the small to medium-size businesses look at this cost different from an operational perspective and for them it is easy to conclude that the cheaper route is to just buy insurance and hope for the best. It is the equivalent of the Hail Mary in football in the cybersecurity world.

If this is your method of handling cybersecurity, then I will say a few Hail Mary's for you, that you are never the victim of a major virus, ransomware, crypto virus, data leak, denial of service attack, website defacement, insider threat, one of the worst kind possible of an active attacker gaining direct access to your servers for no reason other than to maliciously destroy them and your backup data.

Now if you do fall victim, it's time to call that cyber insurance company in place a claim for damages incurred by being attacked. Depending on your policy, that can include anything from downtime, lost revenue,

staff costs, hardware, ransomware payments, and other factors that are typically involved in getting your organization back into a production state.

What they truly failed to cover though, at least our original argument against a cyber insurance only position, is your brand. What is the value of your brand? The downtime incurred where a customer cannot utilize your services, whatever those may be, could make them less loyal to your brand in the future. A data leak of consumer information can outright cause customers to flee your brand for a competitor. Not to mention all the media attention that attacks get these days thanks to mass distribution methods involving social media and the Internet.

In with the new regulations in both the United States and European Union, the idea that you might be able to hide this event in the shadows has become much less likely. For a major company, to do this, can lead to a very expensive fine and potential sanctions by the affirmation governments. But legislation is already rocketing its way through many governments to hold executives criminally liable for events that happen in which they did not properly prepare and can show due diligence that they took every feasible step to prevent an attack.

Cyber insurance is not going to prevent a criminal charge after that legislation is pushed through. It is my opinion that cyber insurance carriers will offer additional “riders” to potentially cover some or all the legal fees associated with a criminal charge, but again, you are still left with plea bargaining or going to trial for negligence.

Now we put all of that aside and look just at the financial damages that are covered by cyber insurance, there is some peace of mind that an organization can get back into production with minimal financial impact. Or so we thought.

So, we all sit here in peace believing that we are covered with insurance, and particularly the small medium-size businesses that forgo proper cybersecurity checks and balances, and then in the past few weeks breaking news:

“Zurich American Insurance Company is refusing to pay out a $100 million claim from consumer-packaged goods company Mondelez, which was one of the biggest victims of the infamous NotPetya ransomware attack in June 2017. Zurich says the NotPetya ransomware attack was actually an act of “cyber war,” and therefore, is not covered by the policy.”

Surely this is an insurance tactic we have seen before, deny the claim for any reason and then make you fight for your right based on that

policy. But this is producing a whole new level of argument by one of the biggest players in cyber insurance and assuredly the outcome of this legal case will set precedent for all future cyber claims. Zürich is arguing that this ransomware attack was state sponsored and therefore an act of war, or better titled a cyber act of war.

Based on this being an active cyber war, Zürich is claiming that the policy does not cover such acts, but the argument that this is a state sponsored attack and therefore not covered under the policy. This is very similar to many insurance policies that do not cover acts of God. This has the ultimate potential to redefine the entire cyber insurance industry particularly at the enterprise level.

But, what effect will this have on the small to medium-size businesses that are relying on cyber insurance over actual cybersecurity practices? Inevitably, if Zürich wins the legal battle on this case, it will become the insured's responsibility to prove or disprove that any attack was not state-sponsored nor an act of cyber warfare. But the reality is there is no true definition to an act of cyber warfare. Which means every case or claim will potentially have to fight for the benefits of their cyber insurance policy.

What makes this difficult even further for the small to medium-size business, is that by not employing actual cyber security measures and

preventative technologies, they will be lacking in the ability to gather information on the attack and prove one way or the other as to the legitimacy of the claim that it was a act of cyber warfare.

What they should do, and what small to medium-size businesses should react to and consider is the true cost of cyber insurance versus cybersecurity. While the finest architected cyber defense will never be 100%, the statistical factors in which you can reduce the probability are high. Longevity Technology, specifically, has three separate but interoperable security solutions that include real-time monitoring with real-time remediation of an attacker, with the capability to log and track their entire attack for analysis should a legal battle with a cyber insurance company become inevitable.

The same technologies that Longevity Technology utilizes to protect our clients also prove due diligence by the organization in question, which removes the criminal argument of negligence and protects the executive group of an organization from criminal persecution. Whether your company is in healthcare, legal, financial, retail, I could continue to list just about every industry, there is some form of regulatory compliance that you fall under, whether you realize it or not and whether you give attention to it or not.

So, the real question is what is the truth of cyber insurance and in the event of a successful attack against your organization, in the end which plan actually protected and saved to your organization, cyber insurance or cybersecurity?