RANSOMWARE INSURANCE: IS IT TIME FOR YOU?

Posted on January 1, 2020 by Kristian Cruz

Category: Ransomware Detection

Written by Oli Thordarson, CEO of Patchworx. Oli shares his thoughts on a recent article, The Biggest Beneficiaries of the Bitcoin Ransomware Boom are Not Hackers, regarding ransomware and cyber insurance, and why the buyers of cyber insurance are getting it all wrong.

Cyber insurance should not be insurance for the negligence of basic cyber security hygiene, like software security update patching and vulnerability assessments/penetration tests. As a side note, we recently picked up two new clients needing ransomware recovery, one with 6,000 users and the other with 500. Both clients were hit on Christmas Eve. Read **Ransomware v2.0 Recovery** for more info on this new phenomenon.

A recent study by Chubb Insurance states that **ransomware attacks have increased** by 84% from 2017 to 2018. In another report, the **global cyber insurance market has been experiencing yearly growth** between 20% to 25%, putting it at $2.5 billion in premiums in 2015, according to KPMG. KPMG says it will grow to $7.5 billion by 2020 and then to $20 billion by 2025.

This is a lot of money to pay out for what is, in many cases, an absolute careless disregard of network security. I do not mean to suggest that all breaches can be prevented; even with good care and substantial investments, breaches can occur from a simple oversight in an otherwise well managed security environment. Or if the hackers are smart and have the persistence, talent, and some luck on their side, breaches may also occur. However, in some cases, buyers of cyber insurance are buying what they think is a “get-out-of-jail-free” card for lack of discipline and understanding of their cyber security landscape. Don’t let that be you!

I do advocate cyber breach insurance. We bundle limited cyber breach insurance as part of a Dark Web Monitoring add-on we recently included with our **Patchworx Patch Management as a Service**.

This is not only a first of its kind, but an only of its kind.

It is important to note what is actually included in a cyber breach policy. A few key points to note:

1. In almost all cases, there are stipulations you must comply with to get the insurance. I presume that if the insurance company can point to failure to comply with those stipulations, coverage can be denied. These stipulations generally detail good cyber security practices that, if followed, almost completely negate the likelihood of a breach or significantly mitigate damage.
2. Cyber breach policies limit the amount to be paid out, or do not pay out in certain circumstances. The amount paid for ransom is typically very limited. Many polices don't pay from recovery efforts, just forensics, etc. Know what you are getting and seek good counsel on what you are buying.

In the article, "*The Biggest Beneficiaries of the Bitcoin Ransomware Boom Are Not Hackers,"* the authors states…

> *"Given a choice between reviving a breached computer network at a massive cost and paying a ransom, which is usually a couple of bitcoin, it is easy to see what choice insurance companies will make in the case of a cyber-attack."*

As of today, the price of a bitcoin is $7,192.45. Click **HERE** to see the real-time pricing for Bitcoin. Three Bitcoin ransom is about $21,000. As in the case of the City in Florida, 65 Bitcoins is almost $500,000. We have worked cases where the paid ransom was well over a million dollars. Even then, encryption recoveries don't always work. One recent ransomware variant had a bug in the code; even when the ransom was paid, the recovery provided the victim absolutely nothing.

While paying out might be better for the insurance company, it still leaves the breached entity in a very vulnerable position. Sure, all the data can get unencrypted, but there is also a high likelihood that malware still resides on the system to exploit the entity again later. A Kansas hospital is a good example of this case, in which they got hit twice in less than six months. In order to be safe, all systems need to be wiped clean and rebuilt, data reloaded, and all configurations put back into place. This can be a huge expense and time commitment not likely covered by the insurance carrier. You can read more about this in the Forbes article, "***Ransomware Is A Repeat Offender: How To Protect Your Business.*"** At Alvaka, we have seen too many companies get hit twice when they did not do all the recommended protection remedies after the first attack. So far, everyone has been

shielded from a third attack after finally taking security matters seriously.

Alvaka Networks turned to an expert on the topic of cyber insurance, David McNeil, a Principal at **EPIC Insurance Brokers and Consultants**. David says…

> *"Certainly, it is true, that a part of a cyber policy includes 'reasonable' maintenance of your network and patching. Of course, a definition of 'reasonable' would be nice. But, no one has ever confirmed or made that clear to me….and, I've asked. So, I would recommend a conservative approach as more defensible.*
>
> *The Cyber insurance marketplace continues to evolve at a rapid pace. New cyber insurance players and cyber insurance products are entering the marketplace all the time; some good, some not-so-good. Because there is no standard ISO for cyber policies, it is critical to have a trusted advisor who knows what to look and ask for, given your particular needs.*
>
> *Part of my own new minimum standard includes a few coverages to address exposures that I've seen companies get hit with recently. If a policy does not address these particular exposures, I would consider them inferior.*
>
> *So, either the underwriter would need to modify/extend coverage for these items , or I'd look elsewhere for my client cyber coverage.*
>
> *1. Supply chain interruption from cyber-attacks against the insured or its suppliers*
>
> *2. Invoice manipulation resulting in payments that have been misdirected or fraudulently directed*
>
> *3. Technology disruption affecting operational industrial controls hardware and/or software*
>
> *4. E-crime losses from payment or delivery of money or securities as a result of fraud*
>
> *There are many more factors as part of the overall consideration of what cyber coverage may be needed. None are a panacea. They are simply a survival tool. The best loss to have, is the one that never manifests. Good cyber-hygiene practices do not make you bulletproof. They simply make the next company an easier target than you."*