NCIPHER IS NOW ENTRUST

www.ncipher.com

Can Hardware Security Modules (HSM) lower your insurance costs?

Have you ever heard of Cyber Liability Insurance? If you have not, you will soon. In 2019, according to industry reports, about 47% of companies with revenues in excess of $1B in annual revenue are currently investing in Cyber Liability Insurance with the adoption rate increasing at about 15% annually*. In addition, with the average data breach and ransom payment costing between $450K and $11.6 million** (depending on the size of the company), you can see why the topic of Cyber Liability Insurance is coming to a boardroom near you.

Cyber Liability Insurance is marketed to financially cover a company who has been a victim of a data breach. This insurance can cover things like lawsuits from people whose data was compromised, fines paid to municipalities, payments to credit watching agencies and ransom payments when necessary. As the concept of insurance has been around forever, it is not surprising that insurance companies would eventually offer this new product. We do not think twice about getting auto insurance but in reality, some early motorists had about two decades of uninsured driving pleasure before someone got the bright idea to offer drivers an insurance policy that covered them against the liability in case of an accident.

> ***“Cyber liability insurance companies will be asking about the type of encryption method the company is using, the encryption key strength or what type of key management is being used”***

Most of us have applied and are paying for auto insurance. We probably remember the initial questions we had to answer in order to get a quote for the policy: “Where do you live? How old are you? How long have you been driving? Have you had an accident in the last three years?” etc. Since I have been known to have a lead foot, my favorite is always, “have you had any tickets?” I’m the poster child for traffic school after all. The questions with Cyber Liability Insurance are not too different. In both cases, the insurance company is testing to see how much of a risk you are to their investment.

Today, a typical Cyber Liability Insurance application has security questions like: “Do you have firewalls in force across your network? Do you have data backups? Are you encrypting your data?” No one reading this article would ever answer no to any of these questions. As Hamlet once said, “There’s the rub.” Imagine the first automobile insurance application, do you think it asked about tickets or accidents or years driving? Probably not, because insurance companies were not yet educated on the upcoming risks associated with driving. We are in the exact same predicament now.

As companies are still experiencing data breaches, insurance companies are bound to get smarter in the questions they will be asking about the cyber security of their prospective customers. How long do you think it will be before Cyber Liability Insurance companies will be asking about the type of encryption method the company is using, the encryption key strength or what type of key management is being used? Let's not forget the incredibly fundamental question of how are your keys generated or where are they stored. Trust me; these questions are coming.

The reason these questions are coming is that insurance companies hate to lose money. However, you already knew that. All it is going to take is a data breach from one of their insured companies. Following that breach, the insurance will review why their application questionnaire didn't uncover the latest vulnerability. Once the factors are uncovered, a few additional questions will be added to the application coupled with increased insurance premiums for those who cannot answer all of the questions correctly. Over time, the current two to four page applications are destined to become 10 to 15 pages with appropriate answers causing increased or decreased premiums.

Unlike automobile insurance where the applicant can decide to drive a brand new expensive sports car or a ten-year-old inexpensive compact car in order to save money, corporate data cannot be made less or more expensive. The liability of a breach is typically dependent on the data risk of the company and the depth of the "pockets" of the applicant. As such, the premium costs start with that knowledge and the costs will go up or down based on a company's ability to demonstrate their readiness to prevent a data breach and their history of being party to a breach of any kind.

In the very near future, if you're looking to apply for Cyber Liability Insurance, you will be dealing with very educated, financially motivated companies who will be asking you very detailed questions about your security posture. Because of this and because security professionals all agree that the generation and protection of cryptographic keys must be done using hardware for true crypto security to be achieved, get ready to answer the question do you use HSMs or expect your insurance rates to be higher. Also there isn't traffic school for data breach offenders and don't forget, after a car accident or ticket, your rates go up for years; do you think Cyber Liability Insurance will be any different?

With some certainty, I think it's inevitable that the question about the presence of an HSM within a corporations' crypto environments will eventually be on an insurance company's application and while the initial reduction in premium might not pay for them outright, the increased in premium payment following a breach without an HSM will most definitely pay for your HSMs.

Will you be ready?

Brad Beutlich
Vice President of Western and LATAM Sales, Entrust

To find out more how we can deliver trust, integrity and control to your business critical information and applications, visit www.ncipher.com & www.entrust.com

References:
**Marsh/Microsoft 2019 Global Cyber Risk Perception Survey*
***NetDilligence 2019 Cyber Claims Report*

Search: nCipherSecurity