bonafeyed
privacy in plain sight

Demonetizing Breached Data

Over the past year, we have been asking leaders in different organizations how valuable is the data in their company? Not surprisingly, their answers have been about the same: “it’s like oxygen”, “as valuable as gold”, “it’s how we make decisions” and “it’s our most important asset”. Data is the fuel that powers a company, and without it, most of them will not be able grow or stay afloat. When faced with ransomware events, they have few choices to safeguard these assets. According to cloudwards.net, 2019 tallied $11.5 billion in ransom payments and Cybersecurity Ventures in their 2019 Cybercrime report estimates 2020 will come in at nearly $20 billion. Based on the number of breaches in the past 12 months, it is safe to say that data is also important and valuable for cybercriminals with the average payout at $178,000, 14 times greater than 2019 according to Coveware’s August 2020 report. They may have different motives, but one thing is for sure… they all make money from the data they steal.

In the case of a ransomware attack, the cybercriminal usually holds hostage the victim’s data for cryptocurrency, promising that once payment is made, they will re-enable access to the data with no guarantees of leaking it. Unfortunately, most of the time, adding insult to injury, cybercriminals not only collect the payment from the victim, but they also place the data on the dark web for the highest bidder. Imagine this being Personal Health Information (PHI). Whoever buys this data can now use it to extort anyone, even a high-profile target like an executive, celebrity or political figure, or worse yet, collect massive amounts of money via fraudulent insurance schemes using patients’ medical reports. Since Bonafeyed focuses solely on protecting the data, even when a cybercriminal hits the jackpot and stumbles into a wide-open database with millions of PHI records, the individual data fields and records remain encrypted requiring multiple keys to access a single record and millions of encryption keys to reveal the entire database.

Now consider another scenario that lately has been breaking many headline news – a cyberattack coming from an organized crime gang with affiliation to an unfriendly country. Up until now, we are witnessing more cases mentioning the FBI and other agencies helping companies resolve the problem with mixed results. Talk about a serious hostage situation! A quick pay-out to the criminals to get your business back is no longer a valid option and companies are stopped dead on their tracks, causing major headaches due to impact on operations and revenue. Relying on the reaction time of an overworked government agency to assist in the process for paying out the ransom, if allowed, should not be the only option.

Bonafeyed protects your data – your most valuable asset – and keeps it protected in the unfortunate situation it is stolen or held hostage. You may need to replace the infected equipment and leverage the next generation of perimeter security appliances to recover. The question is what about the data? Sophos, Ltd in their “The State of Ransomware 2020” report, found that paying the ransom doubles the cost to fix the issues caused by ransomware and for those that paid the ransom experienced an average cost to recover was $1,450,000, while those that didn’t pay spent only $730,000 to recover from the attack. Bonafeyed data is fully encrypted within the database. Meaning, companies no longer need to pay any ransoms because the cybercriminals will not be able to derive any value from your encrypted data.

When ***Cy4Secure*** protected data is lost, stolen, abandoned, or forgotten, it remains secure and becomes permanently inaccessible once access to the encryption keys are removed or retired ensuring cybercriminals or non-authorized users only obtain unintelligible digital data.

Contact us at info@bonafeyed.com for a demonstration or visit us at www.bonafeyed.com.