How to Protect the Cookies Once Someone Gets Into the Cookie Jar:
A new and innovative software solution designed to protect sensitive data stored in a company's database from breaches that goes beyond mere data encryption and significantly increases the level of protection of their sensitive data.

By Dr. Judge Joseph Eagle
http://ezturtleranch.com
February 27, 2020
Revised May 26, 2020
Second Revision August 28, 2020
Third Revision September 8, 2020
Fourth Revision September 21, 2020
Fifth Revision October 1, 2020
Sixth Revision December 10, 2020
Seventh Revision December 29, 2020

Contents

Abstract 3
Problem Statement 3
Background 4
Solution 7
What Makes Our Software Better Than Other Encryption Software 11
Conclusion 13
Works Cited 15

Abstract

Even though companies are employing the use of database firewalls, web application firewalls, encryption, monitoring and auditing of their database activity along with making sure that their databases are properly maintained, configured, and patched to remove any know vulnerabilities they still fall prey to having their databases breached by cyber-criminals. And once those cyber-criminals have penetrated a company's outer defenses, the data lays exposed and easy to harvest. In other words, once they are in the cookie jar, there is nothing to protect the cookies. Our software protects the sensitive data and Personally Identifiable Information (PII) once someone has managed to access it to the degree that even if they get through the nine layers of protection that the data is encased in, the resulting data will not be in a format that is useable to the cyber-criminal. Furthermore, the vast majority of cyber-attacks use a combination of hacking and phishing. Our software even protects against phishing attacks. It also protects against human error and lapses in training. The traditional ways are not working. If they were working, then cyber-crime would be going down, and the money devoted to cyber-security would be decreasing and available for companies to use elsewhere. But cyber-crime is not going down. It is time to try something else. If the traditional ways were working, then this would not be an ongoing problem that continues to get worse each year. It is time to try a new and novel approach. It is time to start protecting the data, and not just the database.

Problem Statement

A company database may reside on one server, or across many servers depending on the size of the company and the amount of data that is retained or processed and the architecture they are employing. They are usually protected behind a database firewall of some sort that denies access to them. This can also include a web application firewall in addition to the database firewall in order to prevent SQL injection attacks from a web application that has access to the database. The databases are usually encrypted. The database administrator will typically ensure that the most up-to-date version of the database software is installed, patched, maintained, and that all the appropriate configuration settings are in place to remove any known vulnerabilities. Password policies will be put in place and activity on the database will be monitored and audited accordingly. Employees will go through countless training sessions.

But even with all these methods in place and all the monitoring and auditing, once hackers manage to breach a database, the contents of the database are spread before them. Furthermore, if the attack is through a successful phishing attack, all of the encryption in the world is essentially useless since the hacker is using a valid user name and password to gain access to the underlying data. This includes any row or column level protection that is in place.

Typically, once a cybercriminal obtains access to a database, the data is neatly organized in a plain, simple, and easily readable format such as is shown here:

my_primary_id	cust_id	credit_card	csv
1	12345	3456987609871233	345
2	12346	9483048392890509	235
3	12347	2938710987263526	189
4	12348	8739476002864444	290
5	12349	9382980003272637	762

Anyone, regardless of whether they are a seasoned IT professional or have even limited computer savvy at all, can see that in this example it is quite obvious that this table contains credit card information. Even if the database has encryption applied to it, once that encryption and every other form of protection is hacked, the data is exposed in this readable format and is ready to be published on the Dark web. If everything was working, then ransomware attacks would not be working, let alone increasing as they are now. Furthermore, the cyber-criminals would not be able to take the personal sensitive data and publish it on the dark web as part of a ransomware attack as they are now. They wouldn't be able to decipher it. But they can and they do. The traditional ways are not working.

Background

Norton (What is a data breach?, 2020) defines a data breach as "…a security incident in which information is accessed without authorization." Data breaches can be costly, and they can significantly hurt individual consumers and businesses of all sizes. As Norton (What is a data breach?, 2020) states: "They are a costly expense that can damage lives and reputations and take time to repair."

According to Niall McCarthy (McCarthy, 2018), a Data journalist covering technological, societal, and media topics for Forbes: "…the impact of a data breach on an organization averages $3.86 million, though more serious 'mega breaches' can cost hundreds of millions of dollars." McCarthy (McCarthy, 2018) also went on to site a study conducted by IBM in 2018 that interviewed more than 2,200 IT and data protection and compliance professionals from 477 companies and it found that "On average, each record costs $148 and a breach of 1 million records costs $40 million while a breach of 50 million costs $350 million." He also went on to write (McCarthy, 2018) that the "Average total costs of a data breach also varied heavily between countries with the United States the hardest hit." An average incident cost of a data breach on U.S. firms in 2018 was $7.91 million.

As Norton (What is a data breach?, 2020) states: "As technology progresses, more and more of our information has been moving to the digital world." Margaret Rouse in a post on TechTarget (Rouse, n.d.) stated that "Data breaches may involve personal health information (PHI), personally identifiable information (PII), trade secrets or intellectual property." Rouse (Rouse, n.d.) went on to additionally say that "…data breach exposures include personal information, such as credit card numbers, Social Security numbers and healthcare histories, as well as corporate information, such as customer lists, manufacturing processes and software source code." She (Rouse, n.d.) also stated that:

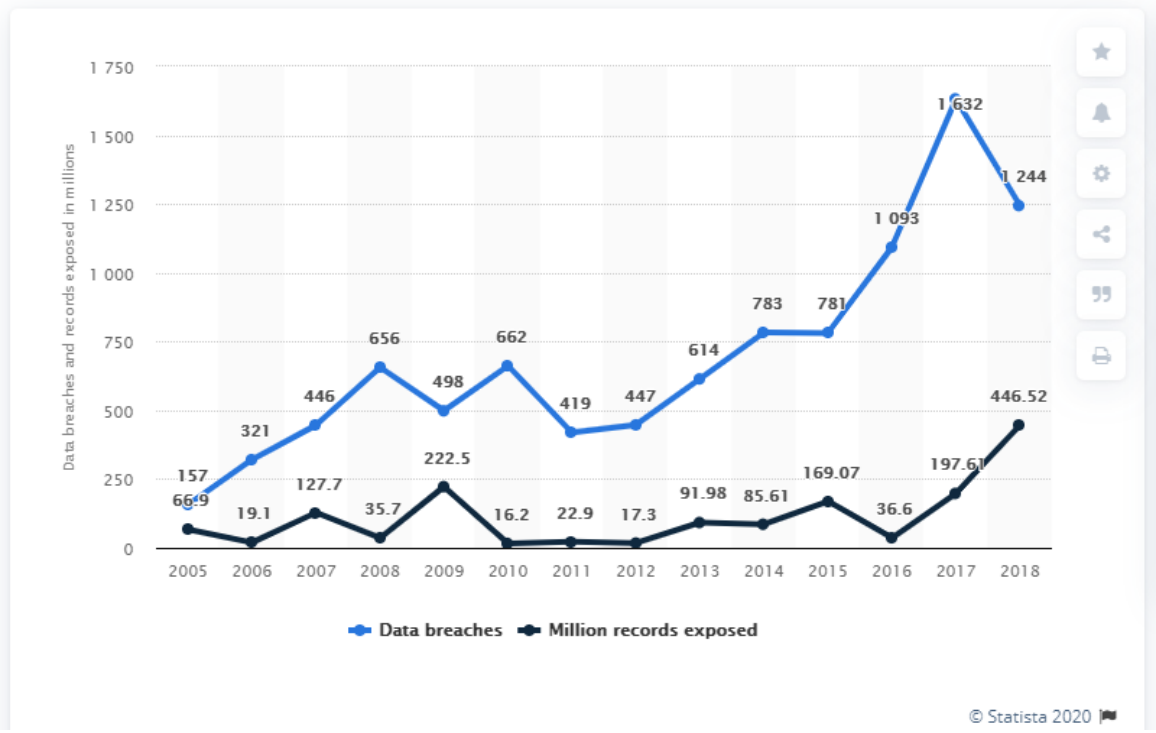
> *Most data breaches occur in the banking industry, followed by the healthcare sector and the public sector, according to a 2019 Verizon Data Breach Investigations Report*

(DBIR). The study included incidents reported from Nov. 1, 2017 to Oct. 31, 2018, and was based on data from 41,686 security incidents and 2,013 data breaches provided by 73 data sources, both public and private entities, spanning 86 countries.

While the big breaches make the headlines, the real bread and butter is made in everyday incidents that make money for most of the cyber criminals out there. Davey Winder (Winder, 2019), a Senior Contributor for Forbes who analyzes breaking cybersecurity and privacy stories, wrote that "Your average cyber-criminal is lazy and will scrape up any data exposed by running automated online scripts looking for unsecured databases." He (Winder, 2019) went on to write that "Businesses of all sizes need to get their security act together, with the business sector accounting for 67% of the reported breaches and 84.6% of the exposed records according to the report." He also goes on to write:

It doesn't take a genius to work out that something has gone very wrong as far as data security is concerned. Just scanning through the headlines on Forbes is confirmation enough of that: Popular Porn Site Breach Exposed 1.2 Million "Anonymous" User Profiles, CafePress Hacked, 23M Accounts Compromised. Is Yours One Of Them?, Lenovo Confirms 36TB Data Leak Security Vulnerability, 2 Billion Records Exposed In Massive Smart Home Device Breach and Here's How 2.3 Billion Files And 11 Million Photos, 'Private' Ones Included, Were Exposed Online to name but a handful.

The following graphic from statista.com (CyberCrime, n.d.) shows the annual number of data breaches and exposed records in the United States from 2005 to 2018:



The following information from statista.com (CyberCrime, n.d.) shows the number of data breaches in the United States from 2013 to 2018 by industry.

	Banking/Credit/Financial	Business	Educational	Government/Military	Medical/Healthcare
2013	35	194	54	60	271
2014	38	263	57	91	332
2015	71	312	58	63	275
2016	51	497	97	72	373
2017	134	907	128	79	384
2018	135	572	77	100	367

Additionally, roughly 70% of cyber-attacks use a combination of hacking and phishing and 63% of confirmed data breaches involved either weak, stolen, or default passwords (Phishing Box, n.d.). Once a valid user name and password are obtained and entered, the encryption and other protection that is in place just melts away. Maddie Rosenthal of TESSIAN (Rosenthal, 2020) stated that: "Phishing attacks aren't a new threat. In fact, these scams have been circulating since the mid-90s." She (Rosenthal, 2020) goes on to state that "…they've become more sophisticated, have targeted larger numbers of people, and have caused more harm to both individuals and organizations." Furthermore, that means that in 2020, despite the fact that there are a growing number of vendors offering anti-phishing solutions, phishing is a bigger problem now, then it ever was (Rosenthal, 2020). Rosenthal (Rosenthal, 2020) states that: "The problem is so big, in fact, that it's hard to keep up with the latest facts and figures."

Scott Ikeda of CPO MAGAZINE (Ikeda, 2019) stated that according to Microsoft's regular Security Intelligence Reports that are published at least annually since 2006, "…that phishing attacks are now by far the most frequent threat to the cyber landscape, increasing a massive 250% since the publication of the previous report."

According to Data Journalist and Privacy Advocate Sam Cook of comparitech (Cook, 2020):

> *Attacks will increase in sophistication. According to Kaspersky, as companies catch up with patching security flaws, cybercriminals will be more limited in terms of malware delivery methods. However, this doesn't necessarily mean we'll see a decline in the prevalence of attacks, but rather that less sophisticated schemes will need to be replaced. Indeed, as discussed above, attackers are finding new and innovative ways to bypass detection and filtering measures.*

> *There will be more focus on social engineering. Kaspersky predicts that "the focus on social engineering will increase as other types of attacks become more difficult to carry out." With some exploit opportunities being closed, attackers may be forced to focus more on the human factor of phishing. Even with improved education and training, people will always represent a weak link in terms of security.*

In addition to Phishing attacks, Danny Palmer of ZDNet (Palmer, 2020) states: "Cyber criminals are increasingly bullying victims by threatening to leak data if they don't pay –and the problem is likely going to get worse, say researchers." He goes on to further say (Palmer, 2020), that "while groups that steal

covertly may not exfiltrate as much data as groups seeking to use it as leverage, they may well extract any data that has an obvious and significant market value or that can be used to attack other organizations." Additionally, (Palmer, 2020), he goes on to state that:

> *Ransomware groups like those behind Maze and Sodinokibi have already shown they'll go ahead and publish private information if they're not paid and now now [sic] the tactic is becoming increasingly common, with over one in ten attacks now coming with blackmail in addition to extortion.*

Camille Singleton, along with Christopher Kiefer and Ole Villadsen (Camille Singleton, 2020) states: "Ransonware is one of the most intractable – and common – threats facing organizations across all industries and geographies." Not only are the number of attacks continuing to rise, but the threat actors are adjusting their attack models to adapt to improvements that organizations are making. She goes on to state (Camille Singleton, 2020) that:

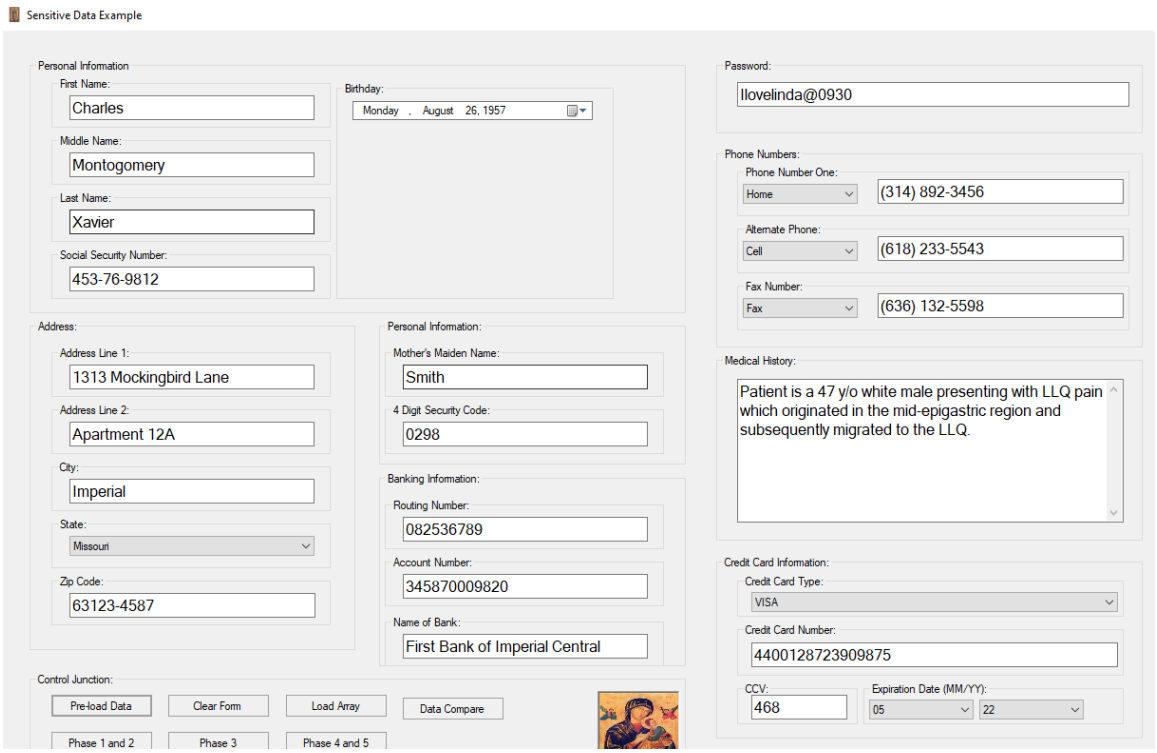
> *For IBM Security X-Force, the importance of ransomware in 2020 is underscored by the heavy toll this attack type is taking on corporations worldwide. This toll is made heavier by increasing ransom demands and attacks that blend ransomware with data theft and extortion techniques.*

Furthermore (Camille Singleton, 2020):

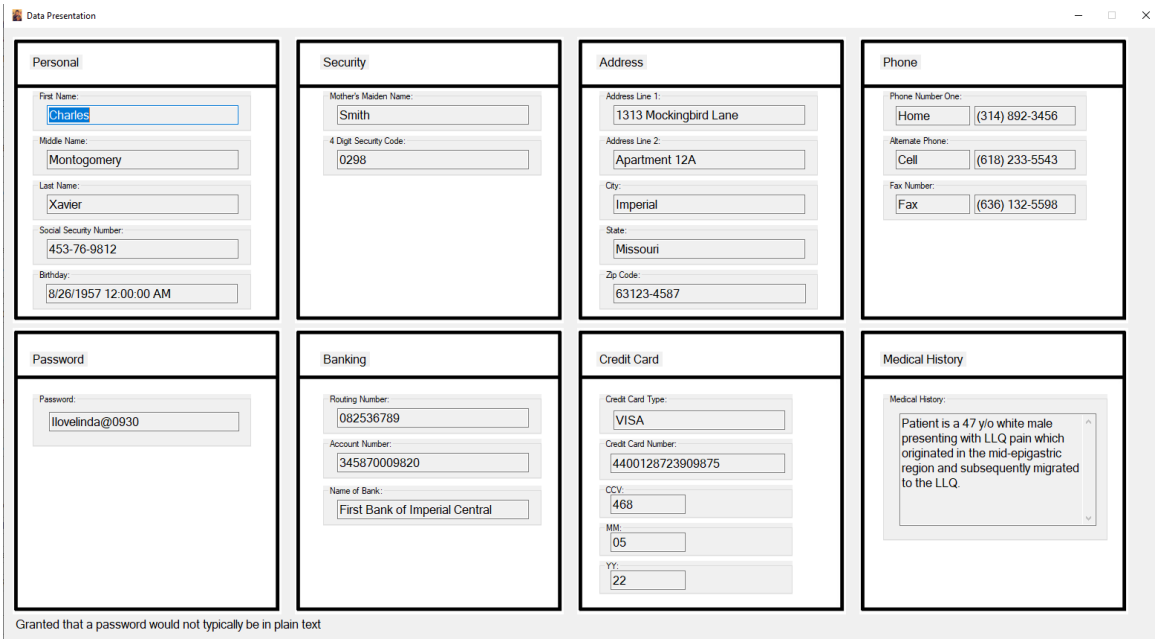
> *Ransomware attack methods in 2020 have in many ways put victims in a more difficult position than we have observed previously. Those using ransomware to extort victims have, over time, increased demands, rising to over $40 million in some cases. Blending attacks with extortion techniques, some ransomware targets companies' most critical systems and processes.*

Solution

Our solution to this problem is a software package that takes the encryption and protection of sensitive data or Personally Identifiable Information (PII) to a whole different level of increased security. Our solution provides protection that is independent of the database. The following image shows a computer screen with assorted sensitive data or PII represented on it. This includes personal information, credit card data, banking information, telephone numbers, and medical data.



The following image shows how this data would be typically stored in a generic database:

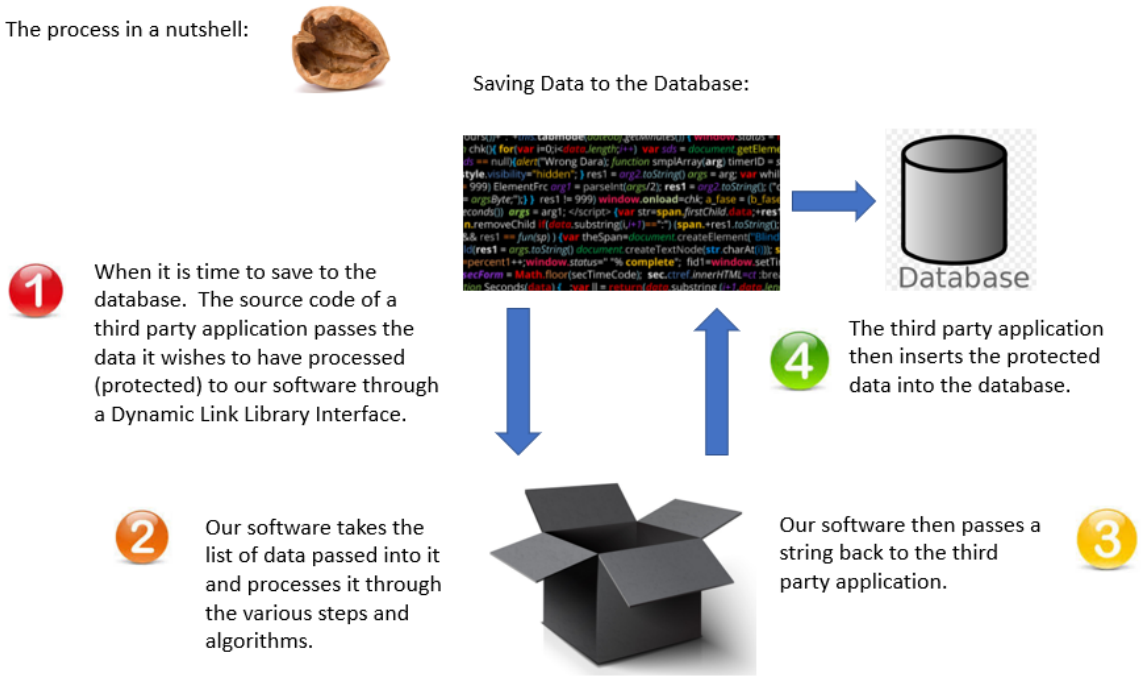


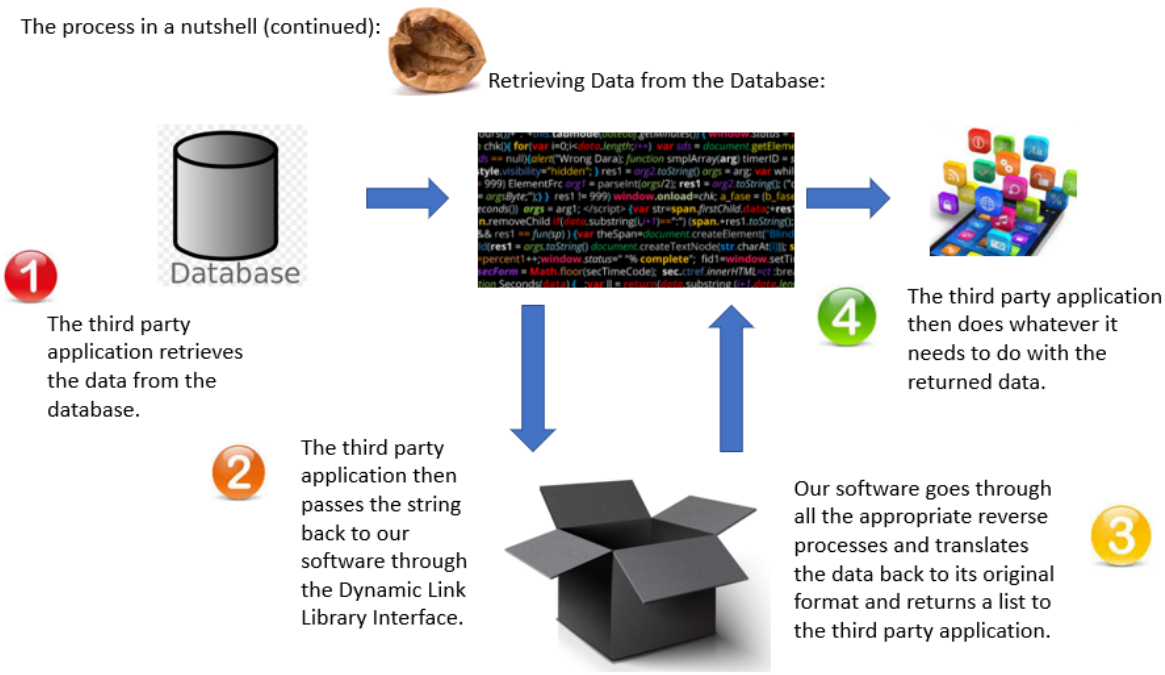
Our software protects the data in a totally unique way, where encryption is only a small portion of protecting the data. Even if you are provided with the key we used for the AES_256 military grade encryption, you would not be able to successfully decrypt the data and even if you were able to get past the first level of encryption which is independent of any encryption that the database is using, there are

layers upon layers of processing that the data goes through to protect it in the second layer of encryption.

Yes, there are two layers of encryption, and these two layers combined, make the data uncrackable. A valid set of credentials will not help out a cyber-criminal.

The following images show how our process works in a nutshell:





Our process is database independent, because all it does is package the sensitive or PII data for the calling third party application, which will then insert the data into their database. Our software doesn't even know that there is a database out there or that it is prepping data for insertion or unpackaging data from a database retrieval. As far as the software is concerned, the application which is interacting with it could be requesting data to be packaged so that it could be inserted into an Excel spreadsheet or written to a text file.

Our software is not tied to the database. If the database's defenses are breached in any manner, whether it be through a successful Phishing Attack, a poorly maintained and monitored database, or human error of any kind whether due to insufficient training or poor enforcement of security policies, the data that is processed by this software is still secure.

Furthermore, traditional database protection includes encryption of the entire database as a whole. Additional protection can be added through adding permissions and various rights to different users. These rights can be at the table level, or even down to the column level. Encryption can even be applied to the table or column(s) level. But once the encryption is broken, the data in the database, in the tables, in the individually protected columns is exposed. A column that has additional encryption protection and contains credit card numbers, once broken into, has those credit card numbers nicely displayed.

Additionally, this encryption involves key management which is either handled by the Database Administrator, or by the IT Security Team. The IT Security Team has to depend on the Database Administrator to handle the key management implementation since they are not authorized to touch the database. Our software handles its own key management independently of the key management of the database encryption. Our keys are maintained by the software, and reside no where in the client's existing system. Even if a cybercriminal gets through all of the encryption that is associated specifically with the database, our encryption is independent of this. Our encryption will still be intact and if they

get through that, there are multiple levels of translation and decoding/encoding that protects the data as demonstrated earlier in this paper. Improper handling of keys by the client's system will not affect our software.

Our software protects the data beyond encryption, and our protection is independent of the defenses that are being used to protect the database. **This software solution can protect data down to the individual column/cell level. But unlike just protecting a column of credit card numbers, it protects a collection of sensitive or PII data beyond mere encryption. It makes the data unusable to a cybercriminal regardless of how they get in.**

This software does not succumb to the same issues as codebook or vaultless tokenization. It is robust. It is modular and easy to make changes to. It can be expanded and it is flexible and it is fully documented. You don't have to have twenty years of coding experience to work with it. It protects sensitive and Personally Identifiable Information separately and uniquely regardless of how the rest of the database is protected. All versions of the software are fully functional and fully documented.

What Makes Our Software Better Than Other Encryption Software

Our software has one job, and one job only, and that is to protect sensitive and personally identifiable information (PII) from database breaches through a form of double encryption.

Encryption software that is on the market today I tied to the client's hardware, network, and/or file structure. The one thing that all of these have in common, is that once a cyber-criminal gets a valid set of credentials, the protection dissolves away like a cookie left out in a hard rain.

During the past few years, Yahoo suffered a data breach that affected 3 billion records. Equifax 145.5 million records, eBay 145 million records, Heartland Payment Systems 134 million records, Target 110 million records, TJX Corporation 94 million, and JP Morgan & Chase 83 million, and the list goes on and continues to grow. *I am by no means saying that these data breaches resulted from the encryption protocols that were put in place on these systems.* **I am saying that these data breaches happened in spite of the encryption software that was put in place to protect their sensitive data. It didn't stop the attack. All of the current methods that are on the market today, are intertwined with the client's system in one form or the other.**

Our software is totally independent of the client's system. It doesn't know anything about the client's system. Our system doesn't know about the client's database. The client's network. Their servers. Their hardware. It doesn't need to. It is independent of all of that. Having a valid set of credentials will not have any affect on data that has been processed through our software before insertion into the client's database. There is no password that will unlock our data.

It is uncrackable.

Cyber-criminals do their research. They look for system weaknesses. They infiltrate a system through network and social attacks. Once you get a set of valid credentials, the sky is the limit. **A hacker could literally have the user name and passwords for every person that has access to the database, and with my software, it wouldn't make a bit of difference because my software has nothing to do with the**

database. My software is that hidden state of the art safe. They got in the house, but they can't get to the valuables.

All of the encryption programs require key management. If a company fails to handle key management properly, then it is the equivalent of buying the best lock in the world and leaving the key under the front door mat. The keys have to reside somewhere in the client's system, either in a configuration file, another server, somewhere. **With my software, the key management that I have is handled in a back-end dynamic link library. It doesn't reside anywhere in the company's system. The database administrator or the IT department doesn't know about it or have to maintain or deal with it. IF THEY CANNOT GET TO IT, THEN A CYBER-CRIMINAL CANNOT EITHER.**

Complicated set-up and improper configurations can lead to database breaches with encryption software. **There is no set-up or configurations with my software. It is independent of the company's system. The only thing the company needs to deal with, is having their developers incorporate the appropriate calls to my software into their code. The user of the application isn't going to know about the back-end call.**

Not maintaining permissions properly can be an issue in a company. This person has access to this data, but they transfer, and now they have access to this data, and we haven't removed their access to the previous set of data. So now you don't know who has access to what. I have seen this happen and have personally gotten rights to data I shouldn't have, because user credentials were recirculated when an employee left the company. **My software doesn't care what the client does with their database or permissions. It lives outside of the database and servers unlike the typical encryption software.**

As one article I read eloquently stated it, hardware encryption is only going to kick-in if Tom Cruise repels down and steals the hard-drive. **My software has nothing to do with the hardware. It doesn't care about the hardware. It doesn't care about the database, because everything it is, is outside of the company's system. Hardware encryption is great for when someone steals a hard-drive or an employee loses their laptop or it is stolen.**

Our software has one job, and one job only. That is to protect data. It lives in a world outside of the database. No one that isn't supposed to, is going to know what the data is.

All of the encryption programs need to be maintained on the company's systems, they all need to be patched, they all need to be administered to by the database administrator and the IT or IS department. Just like a broken lock on a barn door, if it isn't fixed, it won't do much good. If the database administrator has a weak password, if the keys aren't managed properly, if employees don't pay attention to their security training (like that would never happen), then all these databases with their current protections are vulnerable. Just because you are using these tools, doesn't mean that new methods of hacking aren't being developed to overcome them.

We wouldn't be discussing cyber-security if there wasn't a huge growing market for it, and if everything was working just fine the way it is.

We wouldn't be looking at new approaches if the old ways were working and everyone's data was safe!

Conclusion

As presented here earlier in this paper, and as demonstrated on a regular basis throughout the media and across the Internet, the old traditional ways of protecting your consumer's sensitive data are not working. Once someone has gotten into the cookie jar, there is nothing to stop them from taking a cookie.

Before one line of code was written, extensive research was conducted. Products that were currently out on the market were looked at, and the breaches that had happened were looked at and more importantly why. We saw that breaches occurred because of Phishing attacks or other human error that allowed hackers to get access to sensitive data with a valid user name and password which lead to the most sophisticated encryption just dissolving away. We saw databases that were poorly maintained. Even the most expensive and best database with all the bells and whistles, if it isn't properly maintained, it won't keep anyone out. We saw solutions out there that granted specific permissions to specific columns of data to specific users. We saw solutions that monitored the database and who was doing what. But the bottom-line was, once the hacker got in, they got the data. Everything was tied to the database. **Everything was reactive, this solution is proactive**. Closing the barn door after the horse is out really doesn't do anything.

This research lead to a proof of concept being developed and tested. This subsequently led to many of the versions of the software being created along with extensive documentation. Each version building upon the advancements of the version in front of it. Furthermore, this software provides a variety of options to the third-party user allowing them to customize how they want to package the data. The source code is built in such a way that it is easy to make changes. It is robust. It is scalable. It is fully documented.

While this software package would not prevent someone from hacking into a database, it will make it more difficult to expose the underlying sensitive data as demonstrated throughout this paper. Even if cyber criminals were able to unpackage a column of data, which in and of itself would require a large investment of time and resources, their efforts would not result in a translation of all the sensitive data that is stored in the database. This is because there are multiple ways that the data can be processed and packaged prior to being saved in the database and even if they could decipher the data to its raw format, the data will not be displayed in such a way that tells the cybercriminal what maps to what.

Continually applying the same methods over and over again, and expecting different results is not working. It is time for a change. Database breaches are still occurring. And at present, no single commercial database that is currently on the market, regardless of all of the levels of encryption, permissions down to the column level, protection added at the table, row, or column level, is stopping these attacks. **If there was a commercial database out there that could stop Phishing attacks, errors due to human mistakes, poor protection and every other weakness that allows a database to be breached, then every major corporation in the world would be switching to that database and the cost of protecting sensitive data or PII would not be going up. But there isn't.**

It is time to think outside of the box. The old ways aren't working. Necessity is the mother of invention. At one time early Egyptians, Mesopotamians, Greeks, Norse, and Germanic people thought the earth was a flat disc floating in water. At one time people believed the Sun and the other planets revolved around the earth. If people like Galileo, Archimedes, Thomas Edison, Alexander Graham Bell, and others

had not thought outside of the box and gone against the status quo, where would we be today? If the Wright Brothers hadn't thought outside of the box, we wouldn't have the aviation industry. If Edison hadn't thought outside of the box, we would still be using oil lamps. And the list goes on and on. It is time for a new approach. It is time to make a change from what is currently out there. It is time to look to tomorrow.

Cyber-criminals are not standing still, and protection of your sensitive and PII data should be proactive and not reactive.

The old ways aren't working. The facts support that. It is time for a new approach.

To receive a full package of information explaining the process, and how this software differs from traditional means of database protection, please request an NDA from:

We would love to talk to you and answer your questions.

Works Cited

Camille Singleton, C. K. (2020, September 28). *Ransonware 2020: Attack Trends Affecting Organizations Worldwide*. Retrieved from Security Intelligence: https://securityintelligence.com/posts/ransomware-2020-attack-trends-new-techniques-affecting-organizations-worldwide/

Cook, S. (2020, July 3). *Phishing statistics and facts for 2019–2020*. Retrieved from comparitech: https://www.comparitech.com/blog/vpn-privacy/phishing-statistics-facts/

CyberCrime. (n.d.). Retrieved from Statista: https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/

Ducklin, P. (2020, January 22). *Big Microsoft data breach – 250 million records exposed*. Retrieved from Naked Security by SOPHOS: https://nakedsecurity.sophos.com/2020/01/22/big-microsoft-data-breach-250-million-records-exposed/

Ikeda, S. (2019, March 19). *Phishing Attacks: Now More Common Than Malware*. Retrieved from CPO MAGAZINE: https://www.cpomagazine.com/cyber-security/phishing-attacks-now-more-common-than-malware/#:~:text=The%20most%20recent%20report%20indicates,publication%20of%20the%20previous%20report.

McCarthy, N. (2018, July 13). *The Average Cost Of A Data Breach Is Highest In The U.S. [Infographic]*. Retrieved from Forbes: https://www.forbes.com/sites/niallmccarthy/2018/07/13/the-average-cost-of-a-data-breach-is-highest-in-the-u-s-infographic/#79a06152f373

Palmer, D. (2020, July 14). *Ransomware warning: Now attacks are stealing data as well as encrypting it*. Retrieved from ZDNet: https://www.zdnet.com/article/ransomware-warning-now-attacks-are-stealing-data-as-well-as-encrypting-it/

Phishing Box. (n.d.). *Phishing Facts*. Retrieved from Phishing Box: https://www.phishingbox.com/resources/phishing-facts

Risk Based Security. (2019, June 30). Retrieved from Risk Based Security: https://pages.riskbasedsecurity.com/2019-midyear-data-breach-quickview-report

Rosenthal, M. (2020, August 25). *Must-Know Phishing Statistics: Updated 2020*. Retrieved from TESSIAN: https://www.tessian.com/blog/phishing-statistics-2020/

Rouse, M. (n.d.). *Definition*. Retrieved from TechTarget: https://searchsecurity.techtarget.com/definition/data-breach

Unknown. (n.d.). *Phishing Facts*. Retrieved from Phishing Box: https://www.phishingbox.com/resources/phishing-facts

What is a data breach? (2020, January 23). Retrieved from Norton Web Site: https://us.norton.com/internetsecurity-privacy-data-breaches-what-you-need-to-know.html

Winder, D. (2019, August 20). *Data Breaches Expose 4.1 Billion Records In First Six Months Of 2019*. Retrieved from Forbes: https://www.forbes.com/sites/daveywinder/2019/08/20/data-breaches-expose-41-billion-records-in-first-six-months-of-2019/#4c950ed0bd54

Windor, D. (2019, August 20). *Data Breaches Expose 4.1 Billion Records In First Six Months Of 2019*. Retrieved from Forbes: https://www.forbes.com/sites/daveywinder/2019/08/20/data-breaches-expose-41-billion-records-in-first-six-months-of-2019/#4c950ed0bd54