Keyless Encryption:
Tomorrow's Solution Today.

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.

Part One

By Dr. Judge Joseph Eagle

January 5, 2023 First Draft

Contents

To all companies looking to buy an existing company

If everything today were working as designed, then cybercrime and budgets related to such would be going down, and ransomware attacks would be just a depreciated catchphrase. But that is not the case. To those individuals/corporations that are only interested in buying established IT Companies, and already have IT developers, etc., do not write this opportunity off simply because it does not come with a preexisting revenue stream. The product it represents is completely new and could completely rewrite cybersecurity as it is known today. It is time for a new solution to a problem that is only getting worse, just as the invention of penicillin was a new solution to bacterial infections. Doing the same thing as everybody else, over and over again, only manages to get you the same result as everyone else over and over again. Sometimes that works, sometimes it does not.

Just to immediately demonstrate the relevance of this solution:

While I was writing this:

The risk of cyberattacks will continue to increase in 2023, with five potential threats to businesses, individuals and the country sticking out above the rest.

https://www.foxnews.com/us/top-five-cybercrimes-watch-out-for-2023

Abstract

This paper will explore the current state of cybercrime in the world today, who it is affecting and how, and the amount of money that is being spent not only in regards to cybersecurity budgets but the cost of breaches, not only in loss of revenue and fines, but in the loss of reputation and how much this can affect small businesses versus large businesses. After that, the paper will explore the current state of data encryption, and then it will explore how my software is different form anything currently on the market.

The Problem

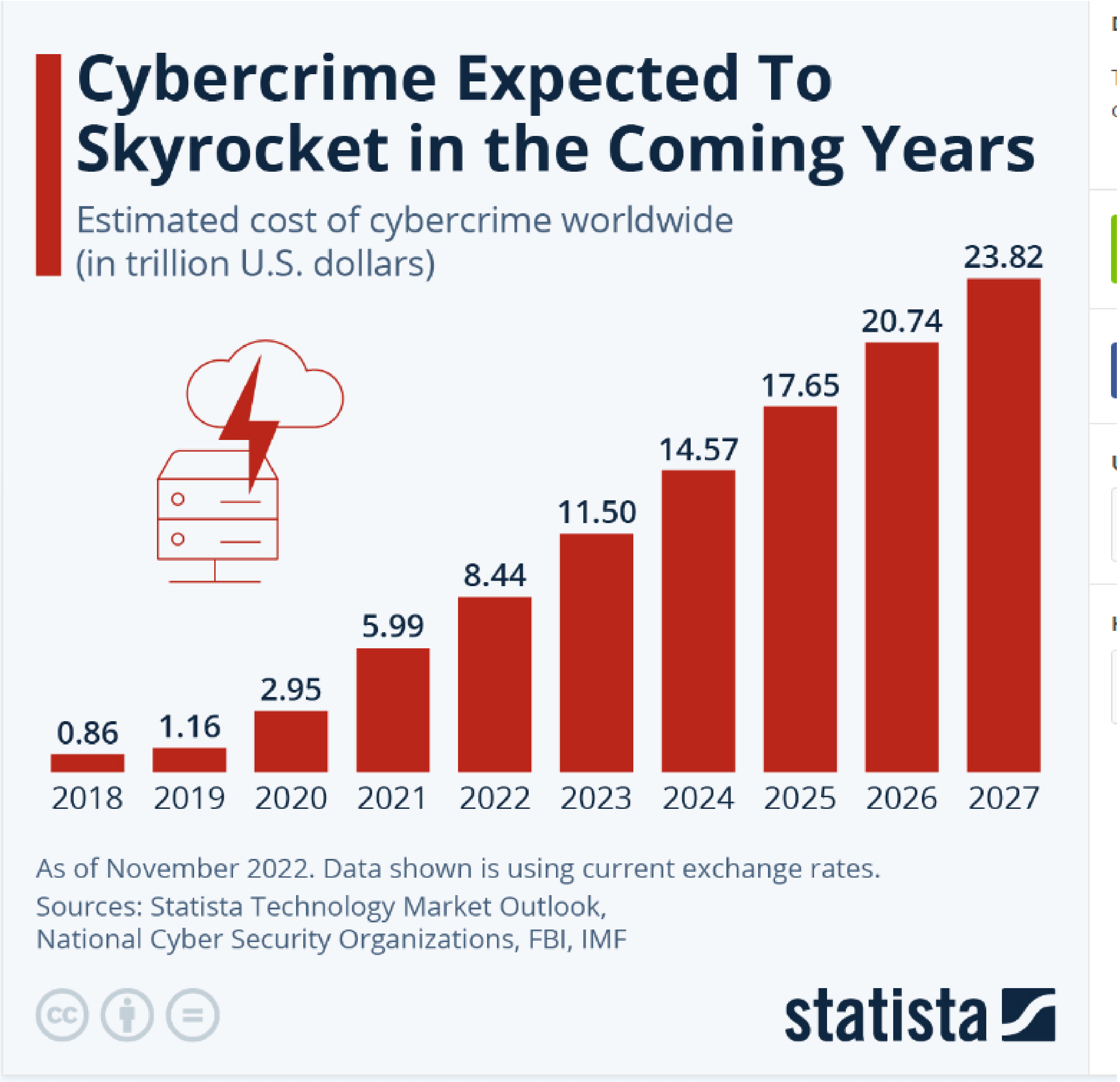
Introduction

In this section I will touch on what a cyberattack is, the types, and the damages that are incurred, and present an argument as to why doing the same thing repeatedly in terms of protecting your company and your client's sensitive and personally identifiable information is not working and it is time for a significant change in what needs to be done and the potential revenue that could result from having a new and distinct methodology available to protect sensitive data that is different from anything out there today, and why the market is ripe for it now. If everything was working, then we would not see the numbers going up. They would be going down and like many news stories, would disappear into the void.

Just keep in mind that:

If there was one set of tools, or one commercial database that prevented data breaches from occurring, then every business, big or small, that could, would switch over to it, and the number of data breaches, records and individuals affected would be going down, and the news would not be full of stories about cybersecurity. But that is not the case as shown below.

Anna Fleck of STATISTA (https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/#:~:text=According%20to%20estimates%20from%20Statista%27s,to%20%2423.84%20trillion%20by%202027.) noted that "According to estimates from Statista's Cybersecurity Outlook, the global cost of cybercrime is expected to surge in the next five years from $8.44 trillion in 2022 to $23.84 trillion by 2027."



Cybercriminals and other malicious parties are always upping the ante in terms of new techniques and tactics to breach networks. Remember, once an intrusion is detected, they are already in the front door. A cybercriminal only has to be “lucky” once. Any business with an online presence has to be “lucky” all the time. Cybercrime is evolving. Defenses against it have to evolve faster.

A successful phishing attack obtaining the proper user name and password will ultimately lead to all the expensive and intricate protection around the data falling away as if it never existed, and exposing the sensitive and personally identifiable information. With my software, as I will demonstrate later in this paper, a cybercriminal can have every user name and password in the company, and it won’t make a bit of difference.

Just remember, your home alarm system does not stop someone from breaking in, it just notifies the authorities when someone has. The criminal may not stay long, but the damage is done.

What is a cyberattack?

If you visit http://ibm.com/topics/cyber-attack they define it as "…unwelcome attempts to steal, expose, alter, disable or destroy information through unauthorized access to computer systems." CYBER TALENTS (https://cybertalents.com/blog/what-is-cyber-crime-types-examples-and-prevention) goes on to state: "Cybercrimes are considered a major risk because they can have devastating effects like financial losses, breaches of sensitive data, failure of systems, and also, it can affect an organization's reputation."

Why does it happen?

The primary effect of cybercrime according to TechTarget (https://www.techtarget.com/searchsecurity/definition/cybercrime#:~:text=Cybercrime%20is%20any%20criminal%20activity,to%20damage%20or%20disable%20them.) is financial. NIBUSINESS INFO.CO.UK (https://www.nibusinessinfo.co.uk/content/reasons-behind-cyber-attacks) states: "Every business, regardless of its size, is a potential target of cyber attacks." They go on to state: "That is because every business has key assets (financial or otherwise) that criminals may seek to exploit."

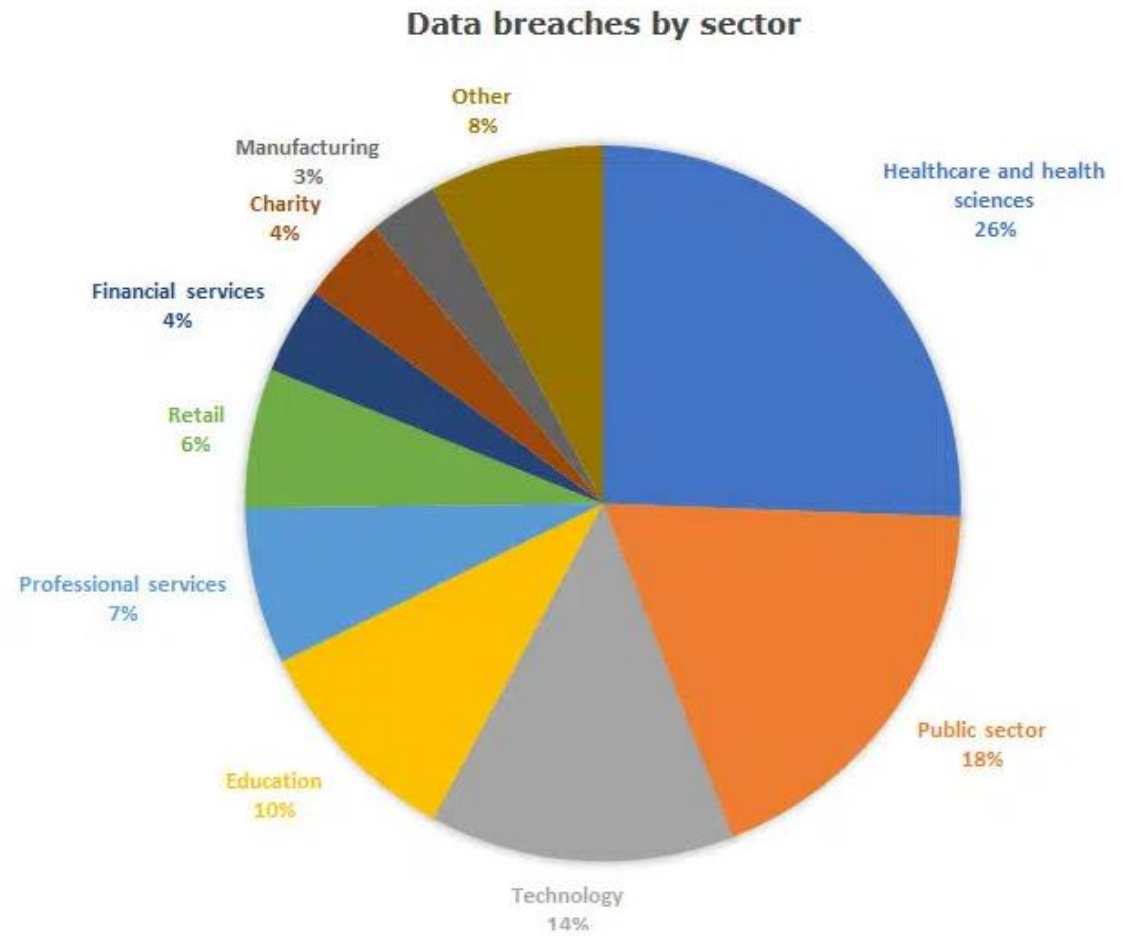
There are company financial details, as well as customers' financial details such as credit card numbers and social security numbers and other sensitive personally identifiable information that can be used for nefarious purposes. Email addresses and login credentials can be obtained, that can then be used to compromise the protection around corporate databases. Intellectual property can be stolen. IT services can be corrupted to affect the ability to accept online payments.

Who is affected?

According to michalsons (https://www.michalsons.com/blog/cyber-crime-and-cyber-security-affects-everyone/18167), cybercrime affects everyone. They state: "Crime affects everyone and in future cybercrime (and cyber security) is going to affect people more and more. No one is safe—it impacts the rich and the poor." Large and mid-sized corporations are affected. Edward Segal (https://www.forbes.com/sites/edwardsegal/2022/03/30/cyber-criminals/?sh=393f29f852ae) stated that "…small businesses are three times more likely to be targeted by cybercriminals than larger companies." Corey White, CEO of Security from Cyvatar (https://www.forbes.com/sites/edwardsegal/2022/03/30/cyber-criminals/?sh=393f29f852ae) stated: "Most small businesses are the perfect target for ransomware hackers."

According to Constella (https://constellaintelligence.com/top-common-targets-for-hackers/), cybercriminals typically target four main industries:

- Over 90% of hospitals have been victimized by cybercriminals. Most notably ransomware within the past three years, with Outpatient/specialty clinics having been a particular target. These attacks not only affect the hospitals and clinics themselves, but their patients as well. In 2020 34 million patients were affected. In 2021, 45 million patients were affected.
- Government organizations have been targeted with their abundance of confidential information. Over half of attacks (53.2% of attacks) target cities and local schools. The average ransom in government entities is $570,857 (USD) with over 41.75 million (USD) paid to cybercriminals in 2020.
- Half of nonprofit organizations have experienced ransomware attacks. They are particularly vulnerable and are ideal targets because of their financial data.
- The financial and insurance industries are 300 times more likely to be victimized by a cyberattack than other organizations. 70% of these digital attacks target banks. Insurance organizations are targeted 16% of the time. Other financial institutions are targeted 14% of the time.



Source: IT Governence

SECURITY MAGAZINE (https://www.securitymagazine.com/articles/98325-the-impact-of-a-data-breach) stated the following: “Cyber incidents have increased rapidly over the last few years, with ransomware and data breaches making their way into public consciousness following a slew of high-profile attacks. Combined with the rush to support remote work, many organizations have found themselves in a situation where interim solutions have become the de facto security stack — leaving them exposed to threat actors that exploit weak technologies independent of industry or organization size.

According to ThreatConnect, those on the frontline of cyberattacks and data breaches may find the speed and scale of these digital threats “insurmountable and infinitely expensive.” In today’s digital economy, security teams alone cannot adequately address cyber risk; instead, companies need to create a layered defense-in-depth approach to tackle cyber risk.

In a survey of 500 IT decision-makers, ThreatConnect found the frequency and severity of attacks are impacting the mental health of cybersecurity professionals; 32% or respondents reported feeling highly stressed about work and more than half said their stress levels had increased over the last six months alone. Gartner has argued that the role of cybersecurity leaders needs to be reframed: "Cybersecurity leaders are burnt out, overworked and in 'always-on' mode," said Sam Olyaei, research director at Gartner.

It's important to note that cybersecurity burnout threatens more than just security and IT teams. Human error is a significant factor in data breaches and, as the Stanford/Tessian study found, nearly half (47%) of employees cited distraction as the reason they fell for a phishing attempt, while the other 44% blamed being tired or stressed.

Threat actors are opportunistic and data breaches happen, but they don't have to be career- or company-ending. Organizations with a good security culture learn from data breaches by implementing policies and controls to reduce the risk of a future risk. Cybersecurity awareness training programs help give employees the tools to recognize, report and respond appropriately to phishing attempts. Technologies such as multi-factor authentication (MFA), endpoint detection and response (EDR), next-generation firewalls, and offline backups can make a huge difference in network defense.

In addition, data breaches can be the gift that keeps on giving for threat actors. Some technical vulnerabilities require a user to be authenticated before they can run the exploit. Data breaches significantly increase the chance of these attacks being successful. A great example of this is a recent Microsoft Exchange vulnerability announced in March 2022. The more credentials are published in data breaches online, as we saw with the LinkedIn data breach in 2021, the more likely these types of exploits will be successful in the future.

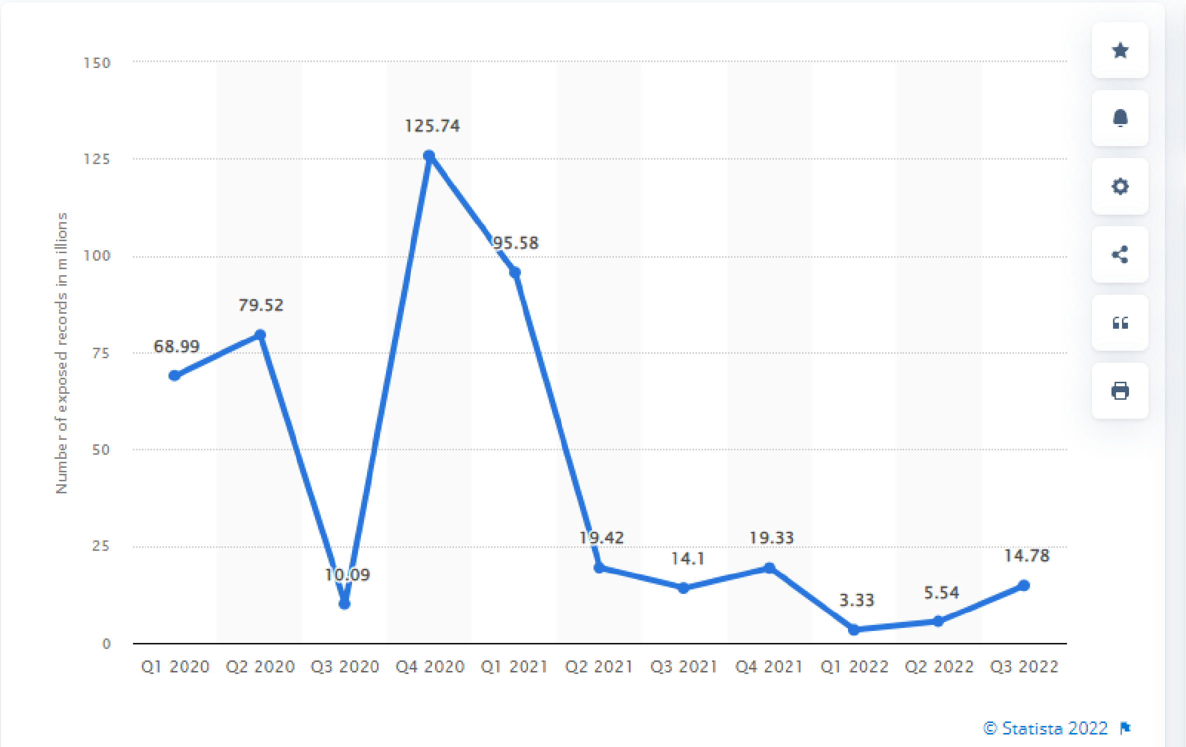
However, tools are only one part of the solution, and alert fatigue can result in valid cyber risks getting lost in the noise. Alert fatigue occurs when security professionals become overwhelmed by the volume and repetitive nature of the alert queue, losing the ability to distinguish alerts that represent actual issues (true positives) and everything else."

Some alarming facts

Aimee O'Driscoll (https://www.comparitech.com/blog/vpn-privacy/data-breach-statistics-facts/#:~:text=4.,breach%20in%20the%20past%20year) has stated that 88% of companies consider cybersecurity a business risk which can affect a company's bottom line as well as resulting in fines, legislative repercussions and a business' share value. 56% of customers now express interest in the cybersecurity of the companies' they do business with. 45% of companies have experienced a data breach. Also, companies that have experienced a breach underperform the market by more than 15% three years later.

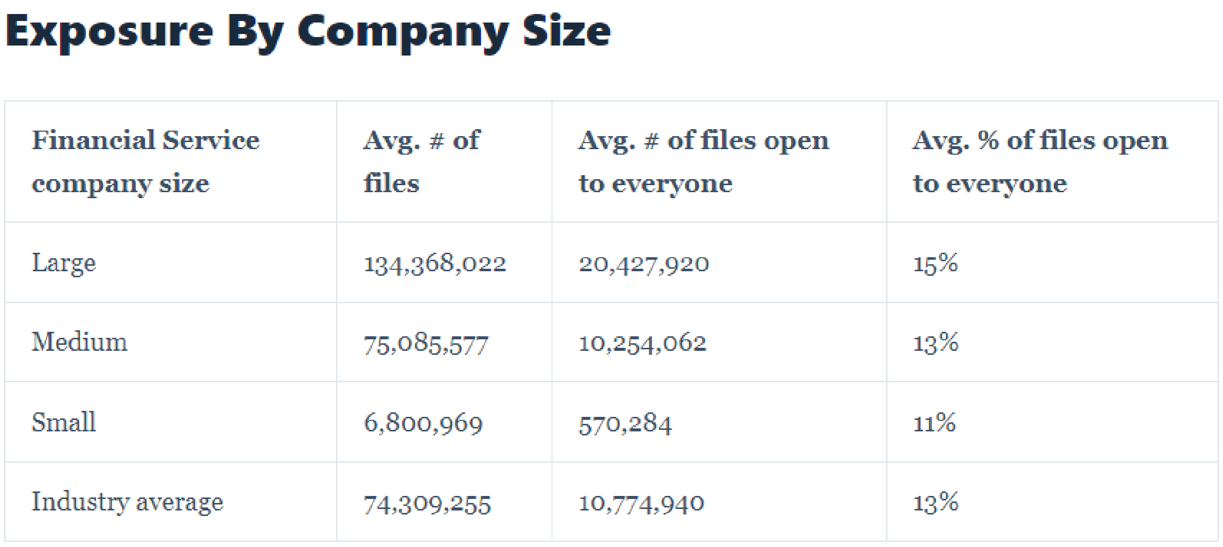
Komron Rahmonbek (https://www.strongdm.com/blog/small-business-cyber-security-statistics) noted that "Cybercriminals assume that weaker security measures will make small businesses easier to crack than larger enterprises. Small businesses are generally not financially prepared for an attack, and most lack cyber insurance. For many smaller companies, a successful cyberattack may even put them out of business." 46% of all cyber breaches have impacted companies with fewer than 1,000 employees.

The Statista Research Department (https://www.statista.com/statistics/1307426/number-of-data-breaches-worldwide/) noted that during the third quarter of 2022, that approximately 15 million data records were exposed worldwide through data breaches. Compared to the previous quarter, this is a 37% increase. The following shows the number of data records exposed in millions, worldwide, from the 1st quarter of 2020 to the 3rd quarter of 2022.



Pramod Pawar (https://www.enterpriseappstoday.com/stats/data-breach-statistics.html) had the following startling statistics:

- Nearly 68 records are compromised per second.
- Around 71% of data breaches are monetarily motivated.
- Nearly 76% of firms around the world faced a phishing attack in the past year.
- The median cost per lost record is $150 (USD).
- Nearly 75% of firms have said that they have faced material disruption in a business process due to a data breach.
- The worldwide spending on information security was estimated to be $150.4 billion (USD) in 2021.
- "A comprehensive survey of firms around the world has revealed that nearly 3 out of 5 firms have faced a data breach at some point."
- Employees working at large firms can access around 20 million files, which a successful phishing attempt with a valid user name and password will expose to a cybercriminal:



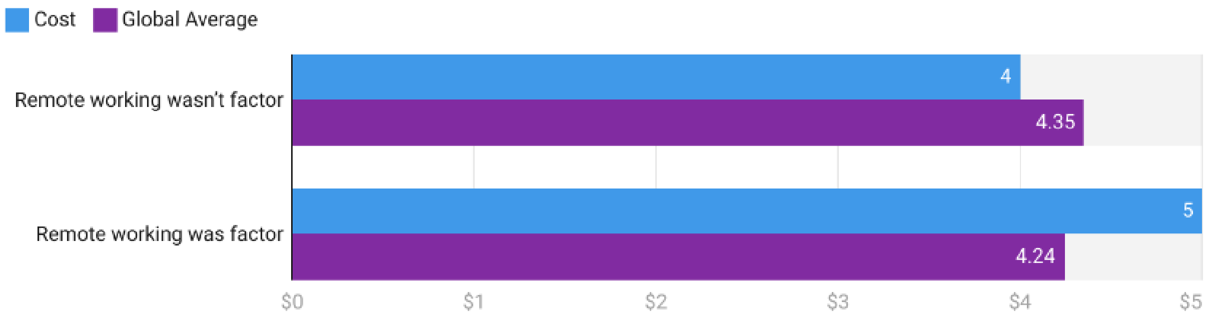
Exposure By Company Size

Financial Service company size	Avg. # of files	Avg. # of files open to everyone	Avg. % of files open to everyone
Large	134,368,022	20,427,920	15%
Medium	75,085,577	10,254,062	13%
Small	6,800,969	570,284	11%
Industry average	74,309,255	10,774,940	13%

(Source: Varonis)

Average Cost of a Data Breach where Remote working was a Factor in 2022

Measured in USD Millions



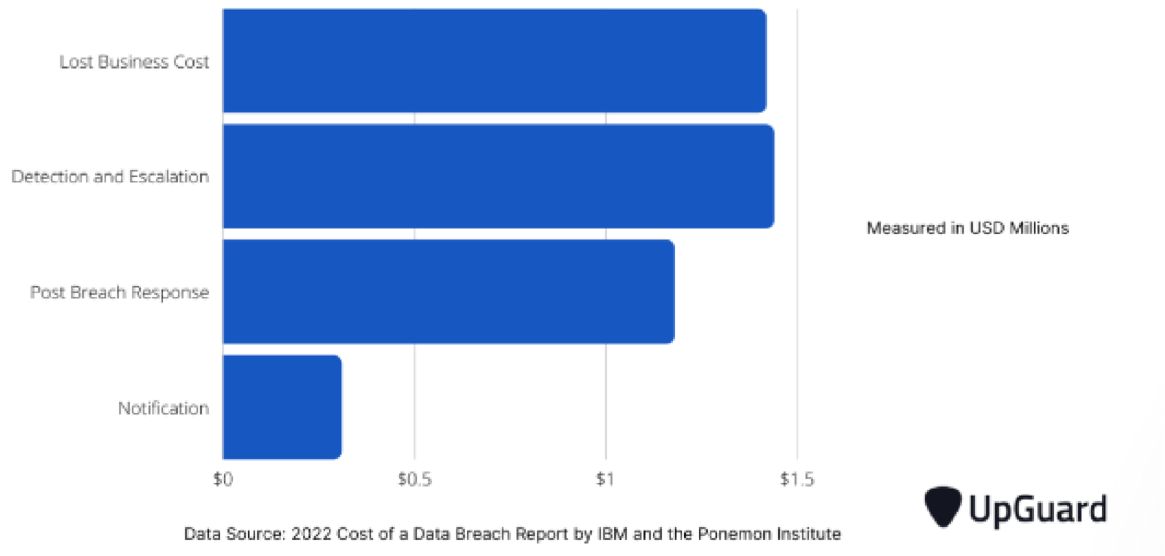
Data Source: 2022 cost of a Data Breach Report by IBM and the Ponemon Institute

Source: Enterprise Apps Today

How are they affected in general?

Abi Tyas Tunggal (https://www.upguard.com/blog/cost-of-data-breach#toc-1) stated that according to a report by IBM and the Ponemon Institute (https://www.ibm.com/reports/data-breach) the average cost of a data breach has reached a record high of 4.35 million dollars (USD). This is a 2.6% rise from the 2021 amount of 4.24 million (USD).

Average Cost of a Data Breach Across Four Segments in 2022

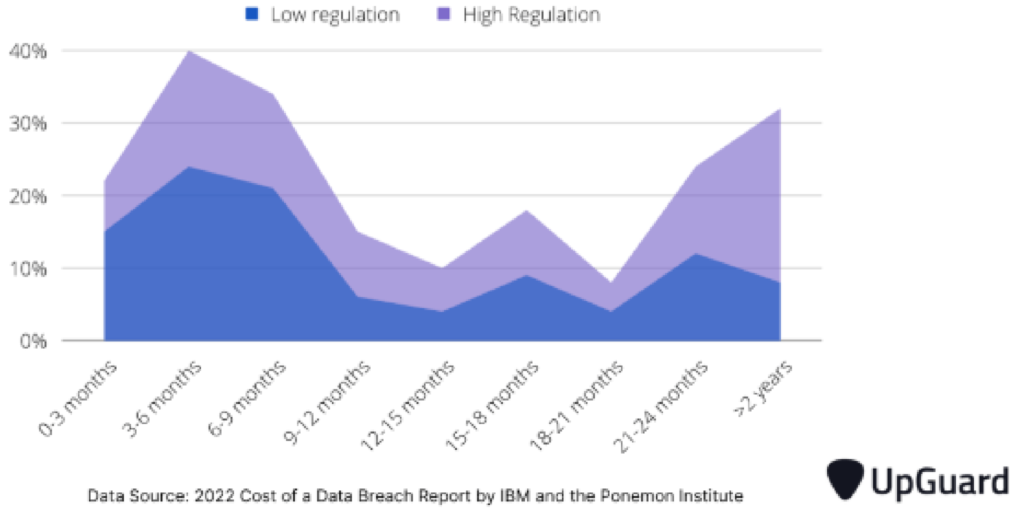


Data Source: 2022 Cost of a Data Breach Report by IBM and the Ponemon Institute

The report took into account hundreds of cost factors, including regulatory, legal, technical activities, loss of brand equity, customer turnover, and drain on employee productivity. Its findings are based on 550 breaches across 17 countries and 17 industries.

It was also noted: "Data breach costs accrue over several years. The 2022 cost of a data breach study found that, on average, 52% of data breach costs were incurred in the first year, 29% in the second year, and 19% more than 2 years after the event."

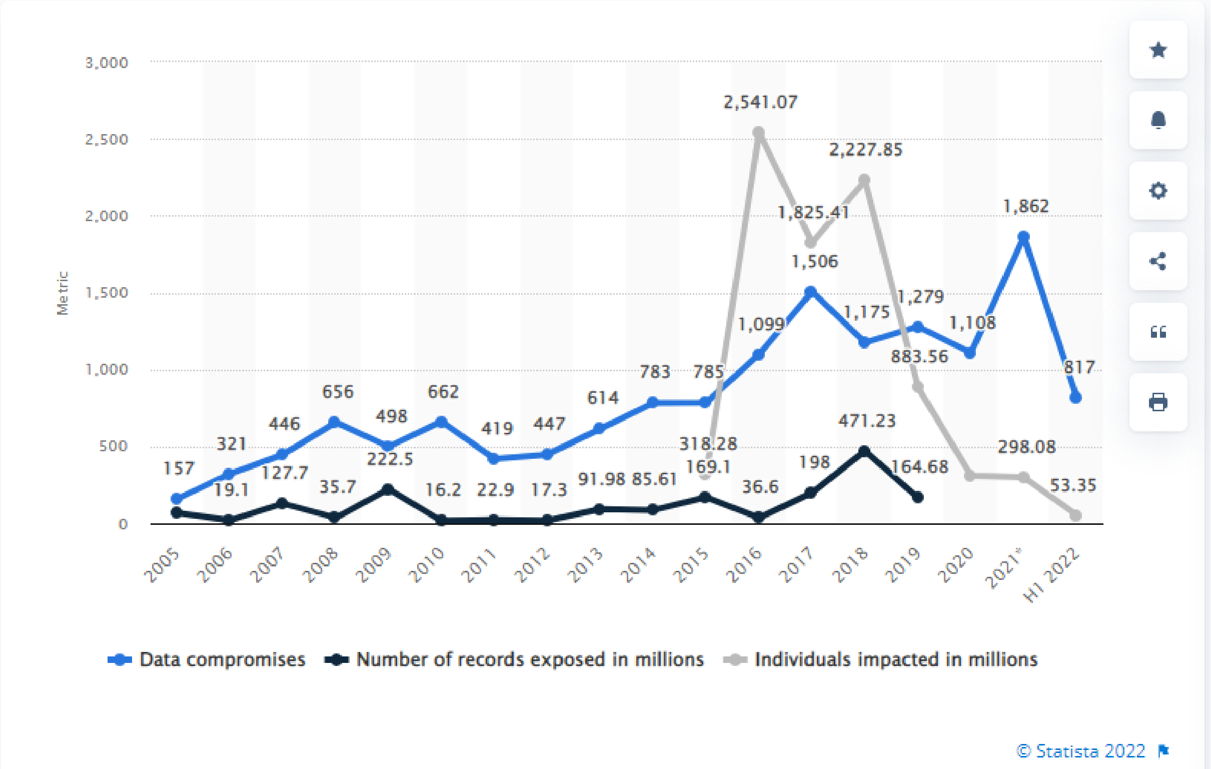
Average Distribution of Data Breach Costs in Low vs. High Regulation Environments



Data Source: 2022 Cost of a Data Breach Report by IBM and the Ponemon Institute

Additionally, it was found that "Organizations in highly regulated industries, such as healthcare organizations and financial services, suffered the worst long-tail costs with the cost of a breach rising in the second and third years compared to low-regulated industries. High data protection regulatory environments incurred 45% of breach costs in the first year, 31% in the second year, and 24% more than 2 years after a breach."

The Statista Research Department (https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/) noted that "in the first half of 2022, the number of data compromises in the United States came in at a total of 817 cases." During this same period, over 53 million individuals were affected by data compromises which included data breaches, data leakage, and data exposure. While these are three different events, the one thing that they all have in common is that they result in sensitive data being accessed by an unauthorized third party.



© Statista 2022

The Healthcare industry has the highest data breach costs. According to Abi Tyas Tunggal, "…the healthcare industry is paying an average of US$ 10.10 million for a data breach, 9.4% more than the figure in 2021."

In general, the longer an attack goes undetected, the higher the financial impact will be. Ransomware breaches are the hardest to detect. Typically taking 49 days longer to detect, while supply chain breaches took about 26 days longer to detect. In 2021, the average number of days to identify a breach was 212 days, and 75 days to contain it. In 2022, the average number of days to identify a breach was 207 days, with an average of 70 days to contain it.

Don MacLennan (https://www.forbes.com/sites/edwardsegal/2022/03/30/cyber-criminals/?sh=393f29f852ae), Barracuda's Senior Vice President of Engineering and Product Management Email Protection stated: "Small businesses often have fewer resources and lack security expertise, which leaves them more vulnerable to spear-phishing attacks, and cybercriminals are taking advantage." He goes on to say: "That's why it's important for businesses of all sizes not to overlook investing in security, both technology and user education."

The USA Today (https://www.usatoday.com/story/money/business/smallbusiness/2022/03/04/small-business-ukraine-russia-ransomware-attack/9379667002/) stated: "Small businesses are most vulnerable to the expected wave of ransomware attacks. Cybersecurity professionals are urging them to take immediate steps to defend themselves."

Robert Johnson, III (https://cybersecurityventures.com/60-percent-of-small-companies-close-within-6-months-of-being-hacked/), President and CEO at Cimcor, Inc., states "…60 percent of small companies go out of business within six months of falling victim to a data breach or cyber attack."

FIS Global (https://www.fisglobal.com/en/insights/merchant-solutions-worldpay/article/how-the-consequences-of-a-data-breach-threaten-small-businesses#:~:text=Perhaps%20the%20biggest%20long%2Dterm,place%20to%20protect%20their%20data.) noted that "Although a business can be the victim of cybersecurity crime, it may also be held responsible for its failure to safeguard the sensitive customer information with which it has been entrusted. A business can be hit with civil liability if it didn't take reasonable, precautionary measures for protection – or if it failed to respond in a timely and cooperative manner following a breach." They also note that: "A good reputation is often a company's most prized asset as a business must work constantly to build and maintain the integrity of its brand. However, one compromising episode like a data breach can tarnish the best of reputations."

Business.com (https://www.business.com/articles/smb-budget-for-cybersecurity/) stated: "Like many core business functions, cybersecurity often requires a monetary investment and therefore needs space in your budget. The need for cybersecurity isn't going away anytime soon." They go on to list some of the potential direct costs to a business because of a breach:

- The obvious one is monetary theft.
- Costs for remediation and system repair.
- Regulatory and compliance issues and fines.
- Legal and public relations fees.
- Having to provide monitoring services for the client accounts that were hacked.
- Identity theft repair for affected parties.
- Increase in insurance premiums.
- Having a forensic investigation conducted.

Some of the potential indirect costs associated with a breach include:

- Business disruption and downtime.
- Loss of business or customers. For a business in a highly competitive market, that could be catastrophic.
- Loss of intellectual property.

- Damage to company credibility, brand, and reputation.
- Inability to meet contractual obligations.
- Damage to investor perception after a security breach can cause a drop in the value of a company.
- Businesses may also face increased costs for borrowing and greater difficulty in raising more capital as a result of a cyberattack.

According to SECURITY MAGAZINE (https://www.securitymagazine.com/articles/98325-the-impact-of-a-data-breach), "…the long-term consequences of a data breach never really go away. The internet never forgets, and even with professional cleanup and remediation, data is never truly recovered or deleted."

Why something else needs to be done and how my software does it

If you only thoroughly read part of this document, then start here.

As we have seen earlier in this document from a variety of sources, cybercrime has caused, and continues to cause a significant amount of damage to companies large and small. The damage being done is not going down in scope and value. The number of attacks is not going down. The cost is not going down.

Companies can employ a wide range of policies and procedures to protect themselves:

- Malware protection.
- Anti-virus software.
- Regular reviews of network alerts, error reports, performance, and traffic.
- Installing firewalls.
- Instructing end users to report suspicious activity.
- File integrity monitoring.
- Regular risk assessments.
- Incident and failure response strategies.

All of these are good. But something to keep in mind for the sake of comparison is, that a home security system tells you once someone is in your house. It does not stop them from entering your home if they really want to, and motion security cameras will tell you if someone is outside your house, but it will not stop them from entering your house if they really want to. Furthermore, the outdoor security cameras will show you someone outside, whether it be somebody walking by, an Amazon delivery, or a porch pirate, but it will not show you their actual intentions until they occur. Nothing can respond by predicting a person's actions. If someone really wants in, they are coming in. You know about it, the Police know about it, the alarm company knows about it, but they are in.

Then, when you factor in the following (https://securityboulevard.com/2022/07/8-most-common-causes-of-a-data-breach/):

“Data breaches are a rising global threat. According to IBM and the Ponemon Institute, data breaches reached a record high in the last two years. Over 2,200 cyberattacks happen daily, costing large companies $4.24 million with each attack.”

Furthermore:

“Social engineering is the number one cause of data breaches for companies and organizations worldwide. Most cybercriminals are good at social engineering since it’s much easier then creating access points to exploit a system. Social engineering attacks rely on psychological manipulation to trick users into giving up their credentials. These attacks are carried out using emails, SMS messages, social networks, and even calls.”

So what I am saying is, a company can invest millions into security, and it can all come crumbling down because one employee accidentally clicks on a bad link, or someone working in your call center at a relatively low wage because they need a job and the only other options are in the fast food industry, doesn’t care or doesn’t pay attention to what they are clicking on, and now the cybercriminal has a valid user name and password. And even if that individual only has access to ten percent of the data stored in your database, that is ten percent of sensitive and personally identifiable information that can be used in a ransomware attack. It is not insignificant to the people that are affected, and it is really sad when something could have been done that is not doing the same thing over and over again and expecting a different result, but something that could actually make a difference.

Now add to this, back-door attacks through third party software and utilities that are included in the coding of applications (such as with SolarWinds). These cracks go unnoticed by software providers and regular users, while cybercriminals find them to initiate a zero-day attack. Again, doing the same thing over and over again, and expecting a different result, is not working.

The above is further complicated with the fact that encryption is essentially a standardized solution that everyone is using with limited exception. Whether the process is using RSA, DES, DSA, AES, or 3DES

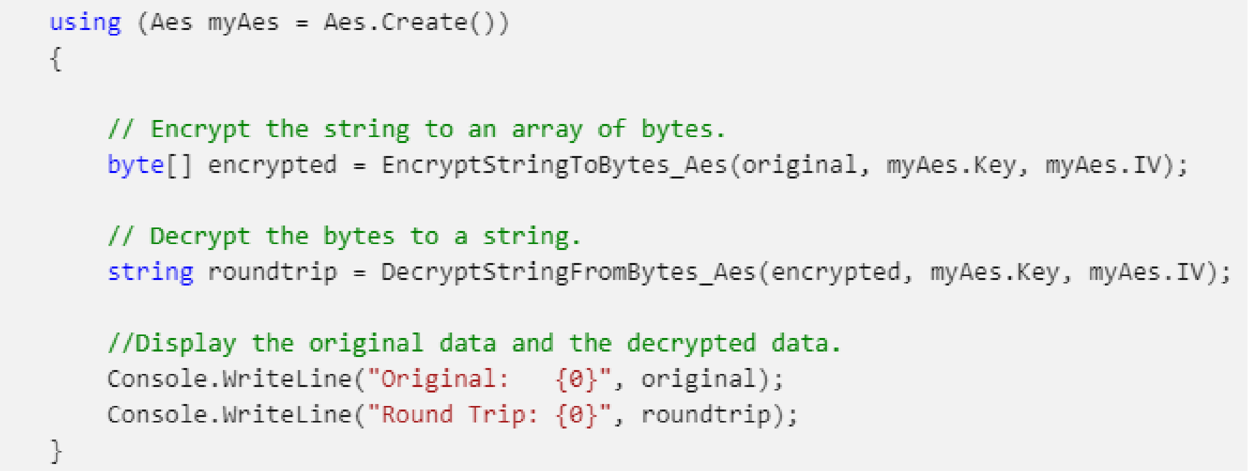
But regardless of the type used, they all take in a string and convert it into an array of bytes. Their code is readily available, with all the bells and whistles, on the Internet as quickly shown here:

- RSA: https://learn.microsoft.com/en-us/dotnet/api/system.security.cryptography.rsacryptoserviceprovider?view=net-7.0
- DES: https://learn.microsoft.com/en-us/dotnet/api/system.security.cryptography.des.create?view=net-7.0
- 3DES: https://learn.microsoft.com/en-us/dotnet/api/system.security.cryptography.tripledes?view=net-7.0
- AES: https://learn.microsoft.com/en-us/dotnet/api/system.security.cryptography.aes?view=net-7.0
- DSA: https://learn.microsoft.com/en-us/dotnet/api/system.security.cryptography.dsa?view=net-7.0

The only difference from one company to the next, is that Company A uses the same key that it stores somewhere on the system for its encryption and decryption, and Company B using the same code creates a unique key for each row of data but has to store that key in a table somewhere so that the decryption process can occur. Same code, different keys, but other than that…

DES is no longer considered secure (https://www.encryptionconsulting.com/why-3des-or-triple-des-is-officially-being-retired/). 3DES is officially being decommissioned. RSA is crackable (https://jonathan-hui.medium.com/qc-cracking-rsa-with-shors-algorithm-bc22cb7b7767 and https://www.forbes.com/sites/forbestechcouncil/2021/05/06/rsa-is-dead---we-just-haventaccepted-ityet/?sh=4c1528565d22). DSA keys have been depreciated due to weakness by OpenSSH (https://gitlab.com/gitlab-org/gitlab-foss/-/issues/44364).

AES is powerful, but the one thing it has in common with all of the others listed here, is a key is needed, and that key has to be stored somewhere. You can use the following code to generate a unique key:



```
using (Aes myAes = Aes.Create())
{

    // Encrypt the string to an array of bytes.
    byte[] encrypted = EncryptStringToBytes_Aes(original, myAes.Key, myAes.IV);

    // Decrypt the bytes to a string.
    string roundtrip = DecryptStringFromBytes_Aes(encrypted, myAes.Key, myAes.IV);

    //Display the original data and the decrypted data.
    Console.WriteLine("Original:   {0}", original);
    Console.WriteLine("Round Trip: {0}", roundtrip);
}
```

But the significance of this, is that if you create a key every time you encrypt something, you need that exact same key stored somewhere so you can decrypt that data. There must be a key(s) stored somewhere. Either in another table, in the source code, a file somewhere, etc. and all of this is really pointless once you have a valid user name and password that gets the cybercriminal to where they want to be.

My software does not care about user names or passwords.

When you depend on key management, which all of the above do in one form or another, key management must be handled properly. 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.

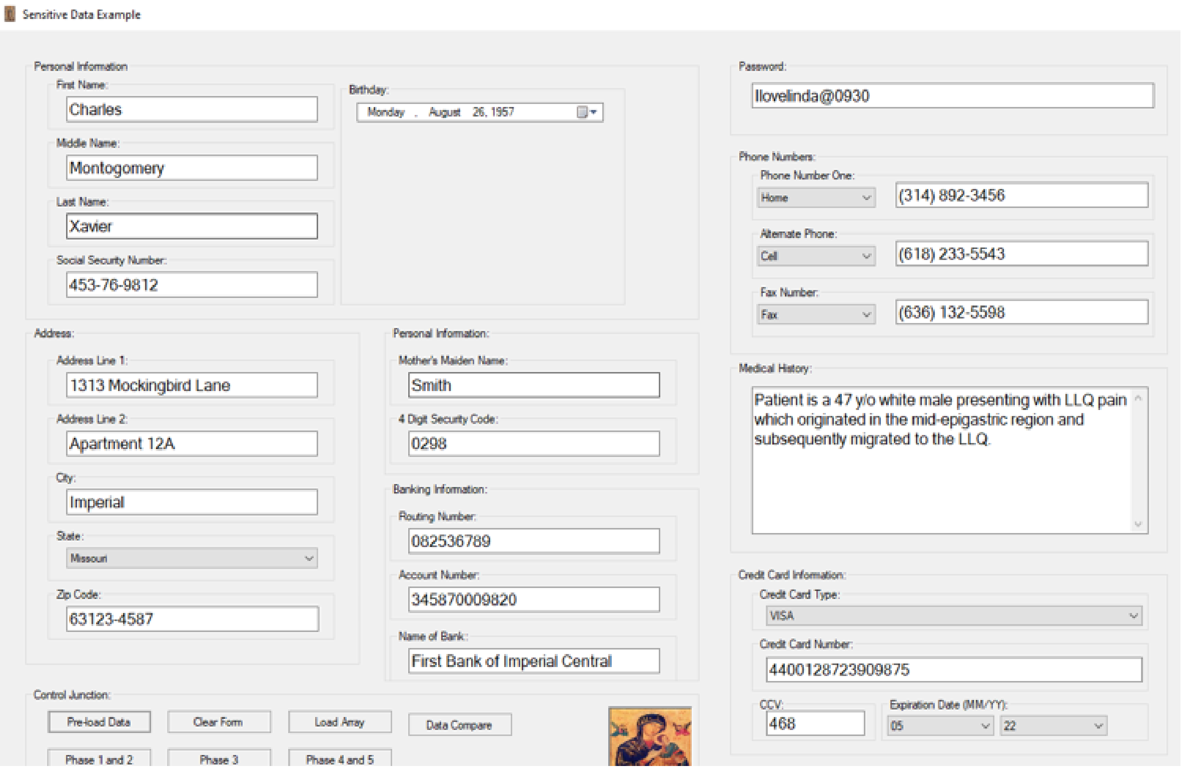
Key management has to be managed by somebody, whether it is the development team, a Database Administrator, or an IT Security Team. Somebody has to take care of it, and it has to exist somewhere. And let us be brutally honest about it, but I have personally seen where the key is in a class in the company's GIT repository. I have also seen where user names and passwords are not changed or deleted, depending on the system, when an employee leaves for one reason or another. The company may turn off their user name to their desktop, but the user name and password exist for an external facing portal. Not making this up.

So, the bottom-line in terms of encryption and decryption, whether they are using symmetric or asymmetric encryption, a key or keys must be properly maintained and stored somewhere. But as we have clearly seen, with a successful phishing attack or clicking on the wrong link, a third-party application or component incorporated into home grown software opening the door for a zero-day attack, completely throws all of the network monitoring, firewalls, and encryption right out the window.

Why my software is different and is like nothing else out there

My software is completely independent of the database that the client is using. It is not even reliant on whether the data is structured or unstructured and there is no key to mess with. The software is intelligent enough to know how it was encrypted, so it knows how to decrypt it. There are approximately 1,000 different combinations that can be used to encrypt the data. Furthermore, it is not just a simple encryption process where "a" based on the key used, gets changed to "S" or "-". It goes far beyond that. There are many unique processes that come together to create the encrypted data using my software.

The following image shows a collection of sensitive and personally identifiable data from a number of sources. This includes names, social security numbers, credit card information, a little bit of medical information and so on:



Sensitive Data Example

Personal Information

First Name: Charles

Middle Name: Montogomery

Last Name: Xavier

Social Security Number: 453-76-9812

Birthday: Monday , August 26, 1957

Address:

Address Line 1: 1313 Mockingbird Lane

Address Line 2: Apartment 12A

City: Imperial

State: Missouri

Zip Code: 63123-4587

Personal Information:

Mother's Maiden Name: Smith

4 Digit Security Code: 0298

Banking Information:

Routing Number: 082536789

Account Number: 345870009820

Name of Bank: First Bank of Imperial Central

Password: Ilovelinda@0930

Phone Numbers:

Phone Number One: Home (314) 892-3456

Alternate Phone: Cell (618) 233-5543

Fax Number: Fax (636) 132-5598

Medical History:

Patient is a 47 y/o white male presenting with LLQ pain which originated in the mid-epigastric region and subsequently migrated to the LLQ.

Credit Card Information:

Credit Card Type: VISA

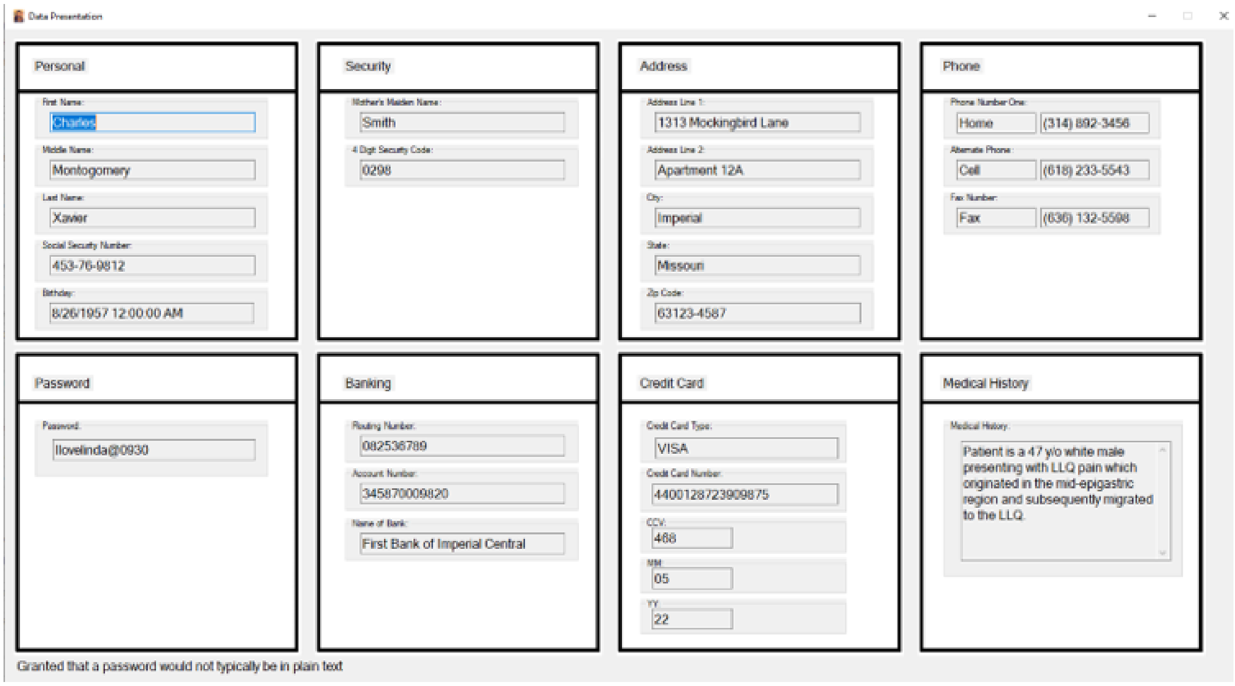
Credit Card Number: 4400128723909875

CCV: 468

Expiration Date (MM/YY): 05 22

Control Junction:

The next image shows how this data might look in a typical database to someone that has a valid user name and password and permission to look at the data:



Personal

First Name: Charles

Middle Name: Montogomery

Last Name: Xavier

Social Security Number: 453-76-9812

Birthday: 8/26/1957 12:00:00 AM

Security

Mother's Maiden Name: Smith

4 Digit Security Code: 0298

Address

Address Line 1: 1313 Mockingbird Lane

Address Line 2: Apartment 12A

City: Imperial

State: Missouri

Zip Code: 63123-4587

Phone

Phone Number One: Home (314) 892-3456

Alternate Phone: Cell (618) 233-5543

Fax Number: Fax (636) 132-5598

Password

Password: Ilovelinda@0930

Banking

Routing Number: 082536789

Account Number: 345870009820

Name of Bank: First Bank of Imperial Central

Credit Card

Credit Card Type: VISA

Credit Card Number: 4400128723909875

CCV: 468

MM: 05

YY: 22

Medical History

Medical History: Patient is a 47 y/o white male presenting with LLQ pain which originated in the mid-epigastric region and subsequently migrated to the LLQ.

Granted that a password would not typically be in plain text

Pretty straightforward, nothing left to the imagination.

This same collection of data using my software could be processed together as a collection of data, or individually, resulting in a string that would look something like this (this string contains all of the data above in it for this example):

ptLXG5zDCUjOki0H2E/NwKZB6CMPfxj8MS1LJgTodoolx48i3nB3Ie27GGiQt3G3C/nQEG
+PdAhoHUD1iTgJxDNDxmv9ZECSYexR9TLqbpLyMYW7E9QkJzV/YDiOZk4JooNM8NVZk
apRUDQx4UtM4GQuz09WiOTGMFbsHT0Ceb6d1zu2X7fSi3TZjQ9RW6aVw8ITcDmn8u
QfeyTjrvRv1rtbxkZNeWxlNlxKXDJwlbZpooVOqURXdRRLxZT5KAYi2q6cUmBrFPpkNRhF
BTKTjdSyg/fVB4VPfvF9U9p4QWDAoij5wqRjcrvQRtp6Vkc1NHnSApTolZy7FDaP1UUdF
RgCfEE5d7jISXueQMajbmGim8LK6xk0SO4ZQMgslEX1WWR/KRFjQqTVEpEg0vmzyug
Mx0olOzr4Oho1oEZ/Nbwo9oOYEpWTdgfxIsRuAy4fF+wf7ylFeKMwARdFYwOJ7h4Y+i5
xuj8e2LkpH81F1OkI75tl8P+zxH77PMEh6lWOTyMuAIZkaD5BSCEEWrLkUPcfso75gx+X
04AXsgBEuDOKpMuLaNrIuhl/r1N4s3WUidrozq/SQlt8somUjY5boxCZ6f4D7hw7cK5YP
w4pRK9dd4YWLB3V6NEYg6rO9DTM3sOxD5i4eOnCwyQ7wMvFdlG3c4IJKBan2Xg/Pkl
SZLzU/rQMTt4jjyaTXIccaG/5TfkCvZXjah7UX7Eo+A4/8ccIP/JNI/lys584kLJ0FIOsbx0aK7
8a2ZM0iSdNS5UbHF2BaUvZHyPMBxlUCRGx5f4Dau6T4uQKIg0cWA82LRzABQwLLOse
vRFfuv4R5om5a/EhXCrFIdlAXtGZWj6yvwfYC5H8/HXfUE13/XtvI4g+LAWNCfCjoq3UYA
REBo7fTs76grjHrmElaiD/3pwIXBiQG+2rQ40baWxKd/juUidrZNl3UcpXg6ucv18SgFlq7I
w/anpsIPR3aGtjsA1Itw==

The outer layer is a homebrew variation of AES encryption along with some other manipulation of the data. The inner layer of protection does much more than just change “d” to “x” based on a key. To demonstrate how sensitive data is protected, let us use the Routing Number in this example which has a value of 082536789. The following image shows what it would look like in the above string if you stripped off the external layer of protection shown above, with the other items from the collection along with the other various manipulations redacted:

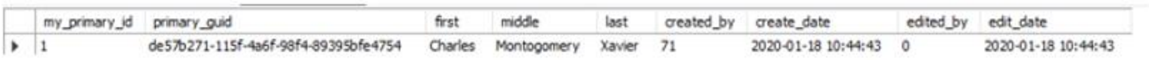
[redacted]

Can you tell which part is which? Can you tell that this is a routing number, and furthermore, there are around 1,000 different ways this same data could be processed resulting in the routing number being represented by different values and found in different locations in this string and in different orders. This goes beyond just reversing a string and encrypting it intact. Not only that, but there are other objects in there that have nothing to do with the data that further clouds the picture of what the data is.

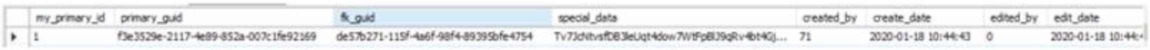
In this example, I have shared with you the data that was presented to my software, and the resulting string that was returned by it, along with one possible way that a piece of sensitive data could be represented in it. And remember, there is no key stored anywhere. My software is intelligent enough to look at the string and figure out each possible step to return it to a routing number or whatever is stored in it.

Not only that, but if someone were to manipulate this string, such as encrypting the data in the table due to a ransomware attack, my software can look at the data, and know that it has been manipulated and shut off any further decrypting of data if so desired. The data will be useless to the cybercriminal.

Finally, just to boil it down to a smaller scale, here is an example of sample data in a MySQL table in the top row, as it would look to a user with a valid user name and password, and the second row is an example of a modified table showing the same information packaged by my software using the same valid user name and password:



	my_primary_id	primary_guid	first	middle	last	created_by	create_date	edited_by	edit_date
▸	1	de57b271-115f-4a6f-98f4-89395bfe4754	Charles	Montogomery	Xavier	71	2020-01-18 10:44:43	0	2020-01-18 10:44:43



	my_primary_id	primary_guid	fk_guid	special_data	created_by	create_date	edited_by	edit_date
▸	1	f3e3529e-2117-4e89-852a-007c1fe92169	de57b271-115f-4a6f-98f4-89395bfe4754	Tv7JdNtvsfDB3eUqt4dow7WtFpBJ9qRv4bt4Gj...	71	2020-01-18 10:44:43	0	2020-01-18 10:44:4

My process is database independent, because all it does is package structured and unstructured data for what ever process is sending the data to it for encryption. The calling process will then insert the data to where it wants it to go. My software does not even know that there is a database. As far as the software is concerned, the software that is making the call to process the data could be putting it in an email or a cell in a spreadsheet. It does not care what the data is, or where it is going. The software has one job and one job only, and that is to protect sensitive data in a way that has never been done before and to provide a level of security that does not exist today.

Think about this. If you have two basically identical customer relation management applications, and the only difference is that one protects data in a way that cannot be decrypted by someone for the various reasons shared here, which one do you think people would buy? Also, if you could create a suite of tools for small businesses that incorporates this software and can provide a level of protection to them that might otherwise be out of their budget for cybersecurity, don't you think that suite of tools would sell? And sell well and serve an underserved population of businesses that do not have the revenue that larger corporations do. This software could be used in a wide variety of applications. Plus, this code is robust, well documented, and easily expandable. It also is not the same exact code that everyone else is using and that can be found out on the Internet.

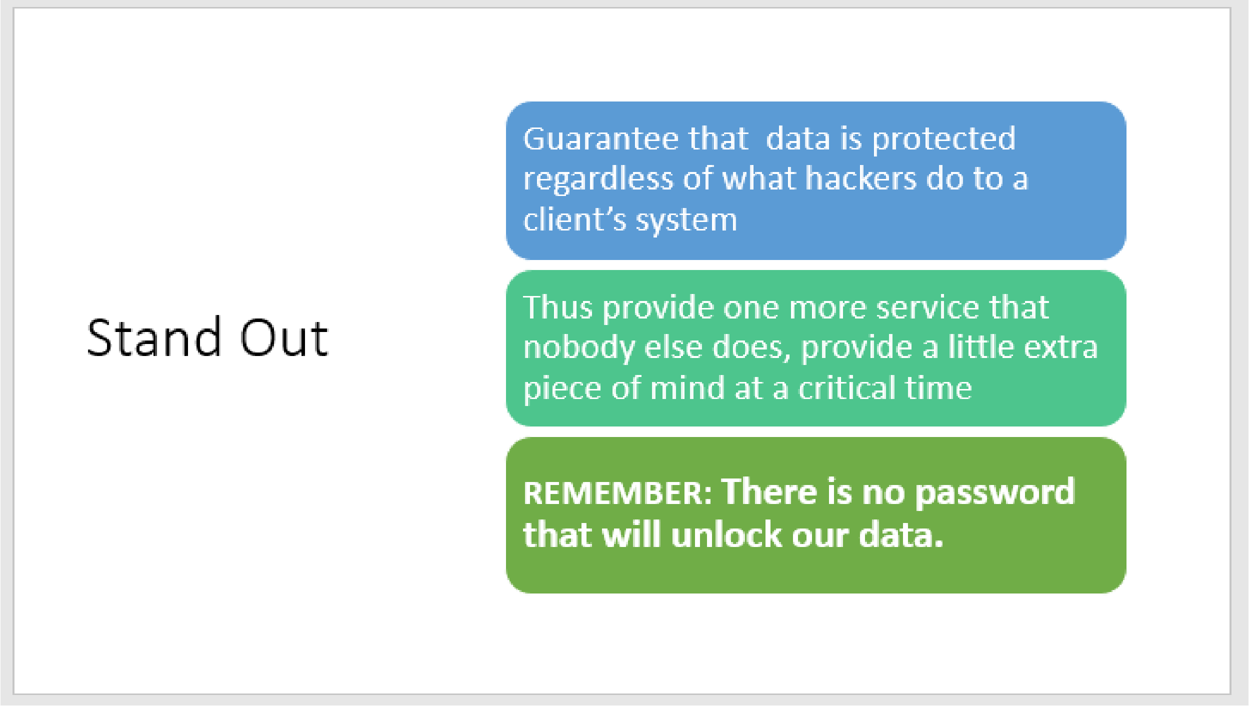
Since my software is not tied to a database, if the database's defenses are breached in any manner, whether it be through a successful phishing attack, a poorly maintained and monitored database, or human error of any kind whether due to insufficient training, or poor enforcement of security policies, or an employee that just does not pay attention to detail or really just does not care, the data that is processed by this software is still secure. Employee training is only useful when the employee is truly engaged in the training, and not just clicking through the nth PowerPoint presentation that they are required to view.

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. But once the encryption is broken, the data in the database, in the tables, in the individually protected columns is now exposed. A column that has additional encryption protection and contains credit card numbers, once broken into, has those credit card numbers nicely displayed. Unless that data has been processed by my software first.

The ransomware attack may still happen, but the cybercriminal will not be able to publish sensitive data out on the dark web, and this is one less thing that has to be dealt with in regards to recovering from the attack. Yes, they got into the system, but our client's data remains intact. They got in, but we successfully blocked them once they were in. People will notice that. And when you factor in how many days pass before the actual cyberattack is uncovered, and how much time the cybercriminal has to gather and post data on the dark web, this is something that will protect the data until the breach is discovered. Remember, as mentioned previously in this document, even with all the tools and monitoring that currently exist, it can still be a couple of hundred days before the breach is discovered. That is a lot of time to do damage.

Additionally, standard encryption as shown earlier in this document, depends on a key and proper 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. My software, as I have said over and over again, really has no key management like traditional encryption processes. My software knows what has been done and what has to be done to reverse it.

My software does not care if you are working with the latest version of Oracle or SQL Server or if you are working with a version from 12 years ago. There is no complicated installation process. There is no requirement that you have to be this operating system or this version of that. No downtime for upgrades. The software can be used as SaaS.



Stand Out

Guarantee that data is protected regardless of what hackers do to a client's system

Thus provide one more service that nobody else does, provide a little extra piece of mind at a critical time

REMEMBER: There is no password that will unlock our data.

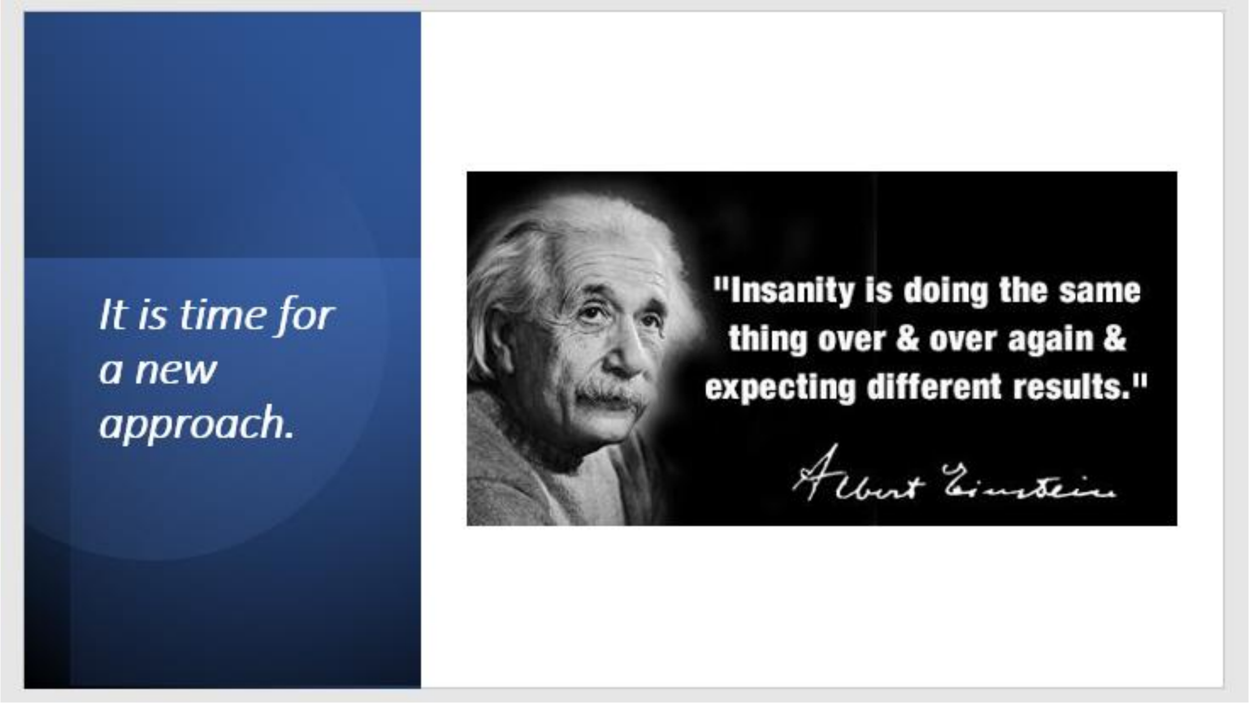
Conclusion

As presented 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. Things are not getting better. They are getting worse. Once someone has gotten the lid off the cookie jar, there is nothing to stop them from taking all the cookies they want.

Cybercrime is very costly, and the protection of sensitive data is an extremely lucrative business. Having a tool that does something that no one else has, and that works like nothing that is currently out there can generate a lot of revenue for its owner. It is tomorrow's solution today.

Instead of having one version or another of what everyone else is doing, and be running with the pack, you will be leading the pack. You will stand out and be noticed.

If you would like to know more about the specifics of this software, please contact Brian S. Mazar, MBA of American Fortune (800-248-0615) or mazar@fortunebta.com, and request an NDA to receive additional information (including part two of this whitepaper) and to set-up a demo, ask specific questions, etc.



It is time for a new approach.

"Insanity is doing the same thing over & over again & expecting different results."

Albert Einstein