Winter 2-25-2019

How Valuable and Secure is Your Personal Data

Joe M. Matrisciano
Olivet Nazarene University, jmmatrisciano@olivet.edu

How Valuable and Secure is Your Personal Data

Joe Matrisciano

Olivet Nazarene University

TABLE OF CONTENTS

Abstract

This paper explores security and the value of everyday personal data. This paper will explore how major breaches can affect both companies and their clients. Corporate attitudes regarding the security of personal data will be discussed, what companies do with our data and lastly what strategies are employed by corporate organizations to maintain our data safe and secure. This is an important topic that needs more review and research because in the world today, security paradigms are failing on both the user and business side. The average citizen simply does not understand how important it is to keep information secure given the big advances in cyber crime as we move forward into a digital world of tomorrow. As well, businesses need to employ excellent cyber security expertise , to ensure the information they are required to maintain does not fall into the wrong hands.

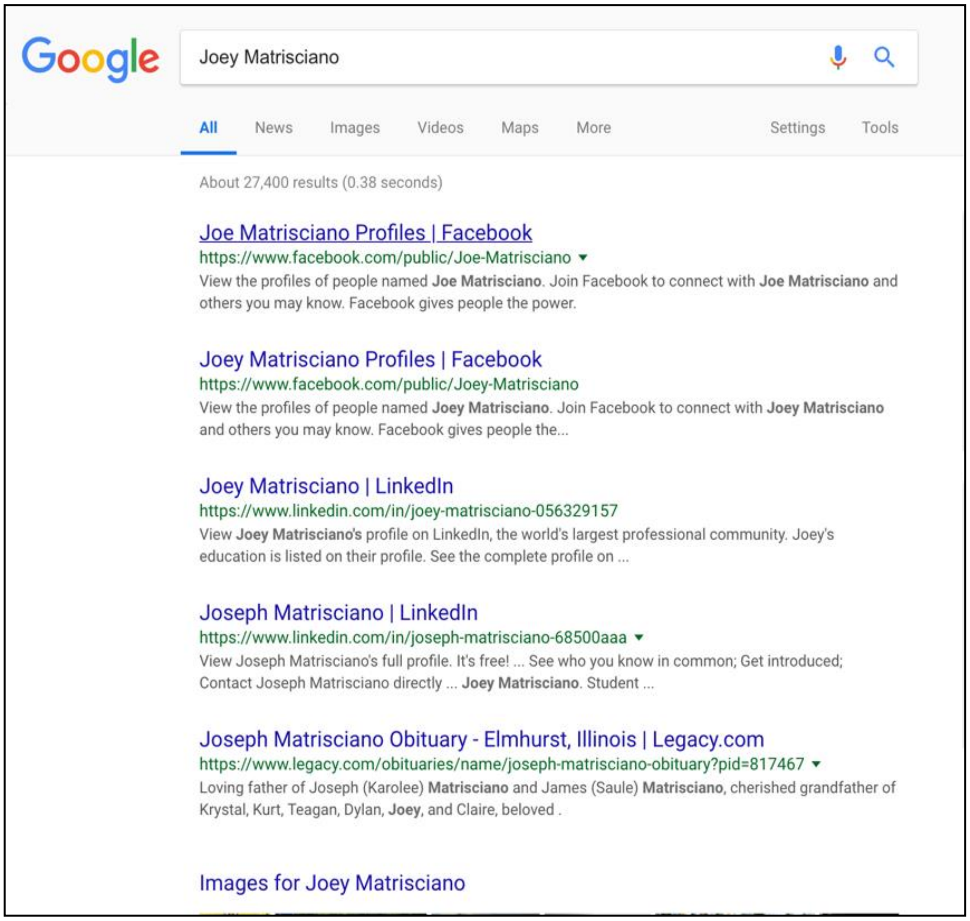
How Valuable and Secure is Your Personal Data

"Passwords are like underwear: don't let people see it, change it very often, and you shouldn't share it with strangers." This is a famous quote from Chris Pirillo, CEO and founder of a large tech blog and newsletter called *LockerGnome*. Passwords are a huge part of cyber security and is how we keep our personal data to ourselves and no one else; just like our underwear. Security is the act of staying free from danger or threat from anything outside of our own comfort. Within security there is a lot of value and responsibilities taken on to ensure that everything is safe and not accessible by the "outside world". The worst case scenario is od course the dreaded hacker; usually depicted in the movies a technnerd who sits at a complex computer setup late at night wearing dark clothes to stay mysterious and unknown from the world in which they live in. Although this tends to be a fantasy description that Hollywood sells us on hackers; is it real, do they actually exist and can they truly have an effect on my own personal data? This brings us to the topic of how valuable and secure is your personal data? With that question in mind there are three different ways in which we can address this concern. We can ask the question of what a data breach is and how does it impact us as the everyday average consumer? An understanding of a data breach then leads us to question how companies we do business with, either in person or online have our personal data stored, do they value our information and in what ways do they use it? Each company use personal data and information differently from the next. Some of those uses help benefit themselves, some the consumer. So the final question that we need to concern ourselves with is can they keep our data safe.

Cyber security within information technology is a booming industry and is hugely related to the way that the world is adapting to the technilogical threats emerging today . As stated earlier, security is the process of staying free from any type of danger or threat. This seemingly simplistic definition belies the complex facets of modern day cyber security..

This paper will present three case studies that will highlight the issues outlined above. Three companies situations will be examined; two whose security was breached and one which has not. The details of what factors contributed to the failures and success of each organization. In order for companies to keep us safe it is not only just their job but the job of the client. We need to understand what security is and how it can affect us on a daily basis.

The average consumer of today, frequently subscribes to a variety of social media apps online newsletters, or corporate sponsored infopages related to our particular interests. We do that with little thought of much these companies capture of us and store for their own benefit. In today’s world, it is very easy to find information on anyone by a simple Google search of the person’s name. Instantly, social media accounts will pop up as well as housing information and family history. To the right in Figure 1, is a photo I have conducted on myself. This is a basic Google search of my name and what shows up and can be found is incredible and so easy to use for social engineering attacks. This is where it is time for the everyday human to know more about our personal data by starting off understanding what security is and what a breach is.



About 27,400 results (0.38 seconds)

Joe Matrisciano Profiles | Facebook
https://www.facebook.com/public/Joe-Matrisciano ▾
View the profiles of people named **Joe Matrisciano**. Join Facebook to connect with **Joe Matrisciano** and others you may know. Facebook gives people the power.

Joey Matrisciano Profiles | Facebook
https://www.facebook.com/public/Joey-Matrisciano
View the profiles of people named **Joey Matrisciano**. Join Facebook to connect with **Joey Matrisciano** and others you may know. Facebook gives people the...

Joey Matrisciano | LinkedIn
https://www.linkedin.com/in/joey-matrisciano-056329157
View **Joey Matrisciano's** profile on LinkedIn, the world's largest professional community. Joey's education is listed on their profile. See the complete profile on ...

Joseph Matrisciano | LinkedIn
https://www.linkedin.com/in/joseph-matrisciano-68500aaa ▾
View Joseph Matrisciano's full profile. It's free! ... See who you know in common; Get introduced; Contact Joseph Matrisciano directly ... **Joey Matrisciano**. Student ...

Joseph Matrisciano Obituary - Elmhurst, Illinois | Legacy.com
https://www.legacy.com/obituaries/name/joseph-matrisciano-obituary?pid=817467 ▾
Loving father of Joseph (Karolee) **Matrisciano** and James (Saule) **Matrisciano**, cherished grandfather of Krystal, Kurt, Teagan, Dylan, **Joey**, and Claire, beloved .

Images for Joey Matrisciano

FIGURE 1. A BASIC SEARCH ON MYSELF THE AUTHOR

What is a breach

According to Dictionary.com a breach is an act of breaking or failing to observe a law, agreement, or code of conduct. While this definition is very accurate and true to nature and applies to the topic of technology to some point, we still want to know what is the true definition of a data breach? A multitude of definitions for a "data breach" exist, but all essentially state, a data breach is a security incident in which information is accessed without authorization. Norton by Symantic expands to say that; " data breaches can hurt businesses and consumers in a variety of ways. They are a costly expense that can damage lives and reputations and take time to repair.”

Now that we know what the definition of a data breach let us explore some typical scenarios of a breach are and how these breaches might impact us as the user, subscriber, or even owner. During the process of this paper on security and personal data there was research constructed on two companies which are known as Equifax and LifeLock. These two companies have had major breaches within the past years that have made huge news and paper article headlines. Before we dig into why these two companies where breached we will first look at a conversation in which I had the privilege to take part in with the retired Assistant Vice President of Information Technology at State Farm who is known as Ken Endrizzi. As many of you have probably heard of State Farm or seen commercials on TV, but for those who do not know State Farm is one of the largest Insurance and financial service organizations within the United States. I have had the honor to network out to Ken and get his personal knowledge of how security works within a large and prestigious company. Let's start off with a little background knowledge of who Ken is and what he does at State Farm. Like I stated earlier Ken was the Assistant Vice President of Information Technology at State Farm. Ken retired this past January from State Farm but is still well connected in the company and filled with an abundance of great knowledge. Ken's position dealt with all aspects of IT including security. At State Farm they have a very Robust security division that is its own independent department within the company. There is a very important reason why they are their own independent department; this allows them to create their own measures with no restrictions or problems interfering with their extensive penetration testing and their written scripts to run security hacks on their own infrastructure. These tests range from Denial of Services attack (DDOs) to virus and firewall attacks as well as internal attacks such as walking around the office to see what information is accessible. Now, you have a basic understanding of what their robust security team does we can see how they are able to stay safe and secure from a breach. Firstly, there team knows that hackers will get into their infrastructure due to human error because no one is perfect, and mistakes are made. This makes them very versatile. Ken talked to me about the three types of breaches there are. 1/3 is an accident, 1/3 is an internal hack, and 1/3 is a true hacker from the outside. The part that makes State Farm's security team stand out above others is that they are constantly looking for weaknesses before hackers can, they are the hackers at State Farm. As well as performing their own tests they go out to other companies that have been breached and study what happened and why they have been breached as a form of audit security. You would think that every company should have this type of department so there would be no concern for security, but there always is a concern not matter how safe we are. Most smaller companies don't have the budget or staff to keep up with security like State Farm does so that's why they are always targeted by outside hackers; because it is simple to find an antivirus patch that hasn't been ran or a firewall that hasn't been updated in some time. Attacks are getting easier and developed upon over time to make them faster, cheaper, and more reliable. Over time Expertise has rolled down hill, what was once a hard advancement made by NASA is now in the hands of an 11-year-old child exploring hacking.

Now that you have seen what a large corporation does to make sure they are secured let's take a look two companies that did not take these complete measures and have been breached within their company's lifeline. Equifax and LifeLock are both large companies just like State Farm and hold a certain standard when it comes to taking care of there clients. We will go into a little background about both companies as well as how they were breached.

Equifax

Equifax is a consumer reporting agency company that serves over 800 million consumers and more than 88 companies. This company aggregates and collects information about individuals and other companies to give their clients more insight to make better business and personal decisions. Now, while focusing on other business and clients to succeed for the future Equifax forgot to make sure they were staying secure and on top of their own company. Their data breach affected over 140 million US consumers, the data that was seized was credit card accounts and some social security numbers. This breach should have never happened if the companies Information Technologies Security team was on top of software patches for the program called Apache Struts. This program is a free open source framework for creating web applications and is widely used by many Fortune 100 companies. Equifax was using this framework as an online dispute portal were consumers can go online to report any log issues with credit reports. There was a patch released for this framework in March and Equifax new about the release but pushed it off for months, this is what caused their biggest slip up to happen. In those two months, hackers were able to exploit their infrastructure through the online portal and sit in their systems for months until they set off suspicious activity and were caught. A simple human error from within the company is what made this company lose very valuable data as well as hurt their own reputation. There is never knowing what a company is doing to keep their customers privacy and security safe even though they all say they are serious about their customers personal data. All companies say they have the highest of security procedures, but this can never be trusted. The majority of companies do not post security executives on their executive leadership page because to many company’s security is not their main focus. It is delivering their product fast, efficiently, and to as many people as possible. As much as Equifax diluted the truth to the papers as to what actually happened to protect themselves, it was their internal negligence that put them in the position of failure.

Just life Equifax other companies have been breached due to internal human error. It is more common than we know as an everyday person. We trust the companies that we are consumers at that they take care of our needs and keep us protected but in all reality, we never really know if they do. Major companies tend to paint the picture that some malicious hacker breached their infrastructure because they were some super computer wizard, but greater number it comes down to internal fault and poor software scripts. In a rapidly changing world, business leaders want production to be pushed out faster and not with more concern for how they are written and protected. That is why software patches is how we get security. Through after math testing and user stories we find our faults that should have been taken care of in the production phase. Not all faults are easy to find, and it takes deployment to find them but too many times have sprouted where software is being pushed out poorly written. We will look at another company LifeLock that has a similar internal fault that had taken place just like Equifax in which caused an external breach.

LifeLock

LifeLock is an American identity theft protection company that has over 3 million subscribers. Yes, it is true, they harp on security and that is the main focus of their company to keep their subscribers’ credit and non-credit related services secure. Just like Equifax, from up above, LifeLock forgot to check all vulnerabilities of their own sites and infrastructure. Now, it wasn’t completely LifeLock’s fault for the breach since it was a third-party contractor that managed the page that had been cracked. This third party managed a marketing page that allowed the companies subscribers to unsubscribe from all emails from the company. This tends to be a popular and useful tool that many companies utilize worldwide but this third-party contractor forgot to tie down all loose ends. Since this web browsing page wasn’t tied down completely there was multiple traces of emails and subscriptions keys that were leaked when a user clicks the unsubscribe button. Now, in the mind of a hacker knowing the email addresses and subscription key of thousands of users it is time to play a little game with basic phishing attacks on all of the users for ransom of some sort. At the end of the day LifeLock and other companies that have been breached did not tests their systems, web sites, and updates with thorough planning and patching. This lead them all to experience fault and reputation lost that they were never expecting from the beginning.

As you can see from the two examples above our data is not always as secure and private as we wished it was. We put our trust into companies that they can do their part and we need to trust and question them before signing up to make sure that they stay on top of their security needs and complete all of their jobs fully. To do our part as a consumer there are a few things we can do to help ensure the safety of our own personal data. First and foremost is having a secure password that we keep private to ourselves. Passwords should always be 8 or more characters long and include more than just numbers and letters. Our password should contain special characters to throw off password cracking software, so our data doesn't get brute forced and breached. As consumers we all need to learn what a phishing attack is and how to spot and avoid phishing attacks, so we don't get ourselves into a sticky position. Any out of the ordinary email addresses that you don't know of or have never see is a good sign at first. As well, anything that has a file in it from a person or company you don't have contact with should NEVER be opened for these can contain malware. Last but not least in a world of growing social media we need to learn to not over share personal information to the world wide web.

Even though all of our information is in the hands of the companies that we are consumers at we hope and trust that they can keep our data safe, it is also important to understand what these companies do with our information. Why do they need to know so much about us like our names, emails, social security number, age, and so on the list continues and differs for each organization. Companies value our information just as much and we value our own information. Companies use our personal data folders for marketing uses so they can deliver the best products in the time of need of the consumers. Let's take a look into how corporations' value our personal data.

The value of personal data

Before we can understand to what magnitude our personal data is valued by corporations, we need to first start off by understanding what Big Data is. Big data is a collection of extremely large data sets that may be analyzed computationally to reveal patterns, trends, and associations, especially relating to human behavior and interactions. Everything we do that is connected to technology leaves a digital trace of big data to be collected. These digital traces are then used for future advances in companies and governments. The collection of Big Data comes from everywhere for example, it comes

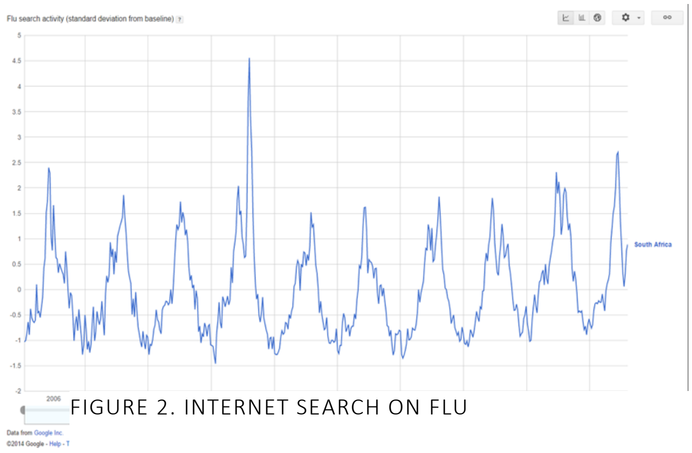


FIGURE 2. INTERNET SEARCH ON FLU

from browser searches, credit card uses, social media activity, email inbox activity, employer databases or subscriptions, gameplay, loyalty cards, as well as internet cookies. Every single transaction and action we make leaves a trail behind for a corporation or company to use for their own personal advantage. Each person who has ever made a transaction has a valuable storage vault of big data that is used for a greater marketing use as well as future predications. For example, when it is flu seasons and people start catching symptoms, majority of people tend to go online to play doctor and look at their symptoms. Most realize they symptoms are related to the flue and then go ahead a search for cures, medicine, or vaccinations. The spike in internet searches for flu related symptoms, or what is the flu, send a wave of suggestions and predictions to make for the next upcoming flu season. This gives corporations the ability to prepare and sell vaccinations and medicine relate to the flu. Up above is a visual representation of the internet searches, the spikes are when flu season comes around. As you can see the flu season has a tendency to land in the same time frame as the year before and the year to come. Hence with big data, future advancements and assessments can be made by corporations for a multitude of different reasons. Big data is data that is exceeding Terabytes in size and is composed of a variety of data types. This data gravitates to being unstructured and with no purpose until one is put to the data. In order to understand the importance of Big Data the data itself needs to be organized and queried or analyzed.

State Farm as well as many other large corporations have a moto they follow when it comes to Big Data, they follow the 4 V's of Big Data or to some they have 5 V's. The 4 V's are a way for companies to collect all of their data and know what to do with it. These V's stand for Volume, Velocity, Variety, and Value. We will leap into each one of these to show you how a large company handles and uses their data for their own benefit. Volume is the catcher's mite of Big data, it is the scale of data that is collected from the 6 billion people having cell phones, to the 40 Zettabytes of data created, to the 2.5 quintillion bytes created each day in our fast-past environment. Anything you do to cause data is captured and organized. There is almost too much data and no order for it to be in. Velocity is the speed at which data is changing from each type of platform. So much data is coming at you in different ways and speed and it all needs to be analyzed for a purpose. The amount of data over corporations such as trade information, network connections, sensors and triggers all contribute to the analysis of streaming data. Next, is the variety of data which is the different types and forms of inputs in our society from billions of pieces of content on social media sites, or store transactions, to cctv cameras that are posted all over public buildings, to voice data, videos, and so many more. All of this data is in a different form and comes at different speeds and different times and at mass quantities.

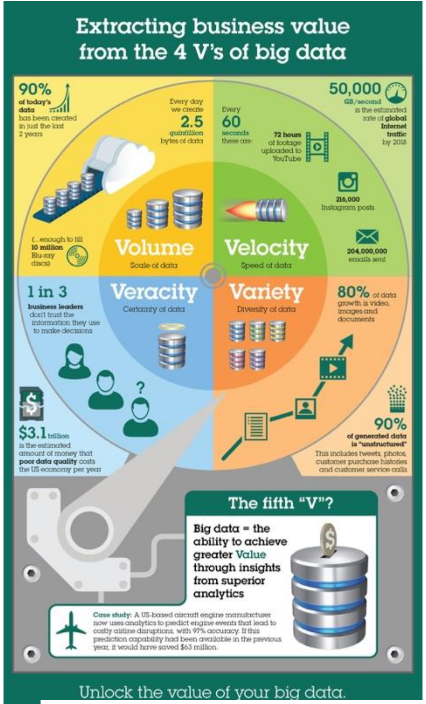

Extracting business value from the 4 V's of big data
90% of today's data has been created in just the last 2 years
Every day we create 2.5 quintillion bytes of data
(...enough to fill 10 million Blu-ray discs)
Volume
Scale of data
Every 60 seconds there are:
72 hours of footage uploaded to YouTube
216,000 Instagram posts
204,000,000 emails sent
50,000 GB/second is the estimated rate of global Internet traffic by 2018
Velocity
Speed of data
1 in 3 business leaders don't trust the information they use to make decisions
Veracity
Certainty of data
$3.1 trillion is the estimated amount of money that poor data quality costs the US economy per year
Variety
Diversity of data
80% of data growth is video, images and documents
90% of generated data is "unstructured"
This includes tweets, photos, customer purchase histories and customer service calls
The fifth "V"?
Big data = the ability to achieve greater Value through insights from superior analytics
Case study: A US-based aircraft engine manufacturer now uses analytics to predict engine events that lead to costly airline disruptions, with 97% accuracy. If this prediction capability had been available in the previous year, it would have saved $63 million.
Unlock the value of your big data.

FIGURE 3. 5 V'S OF BIG DATA

The different types and volume in which data is received needs to be handled to make some sort of sense and have a use for the future production. Next, is how companies value this data. This is the most important part to them because without a value there is no purpose to be collecting all of this data. All of the three V's above create value. Value is how an organization can take all of the data and use it for a competitive advantage. They sort through the information and figure out what they want to keep and get rid of. The value of this data is what created ads and commercials and all the selling points to products. The value is the marketing piece of gold to help the company succeed and get the consumers to come back. For instance, what you previously looked at on a clothing website always seems to have an ad on another website that has nothing to do with clothing. This is a hook and reel tactic where the company makes you contemplate if you really loved their product and if it is worth going back and buying. They convince and reel you into a transaction. That is how Corporations value all of the data and information we give them and how they turn around and use it for their own benefit in sales, marketing, and future predications. At this point we know what a breach is and what a breach looks like and how messy it can really get. As well as we know what Big Data is and the value behind all of that data and the use it really has in our society today. Now we will leap into talking about how companies keep all of our data and themselves safe, secure, and away from hackers and internal faults.

How do companies keep data safe?

Now that you are a professional in the area of what security breaches look like and how companies use personal data for their benefit, lets now look into how companies take it all in and keep it secure which is the most important part. To start off there are many different areas of security that need to be taken into consideration but that is a research paper just in itself. For now, we will take a glimpse on the surface of how companies keep data safe. We will explore the three points of security, physical security, as well as we will look at State Farm and their advice for keeping their company secure and locked down.

The three pillars of security are the main pivotal point upon what security stands for. All security professionals know the three security pillars practices because they bring a basic understanding on protecting systems from loss of confidentiality, loss of integrity, and loss of availability. These three pillars are referenced heavily in all robust security departments like State Farm for example. All three-work hand and hand to keep our information safe as well as to boost the productivity of the organizations. Let's take a dip into each category.

Integrity

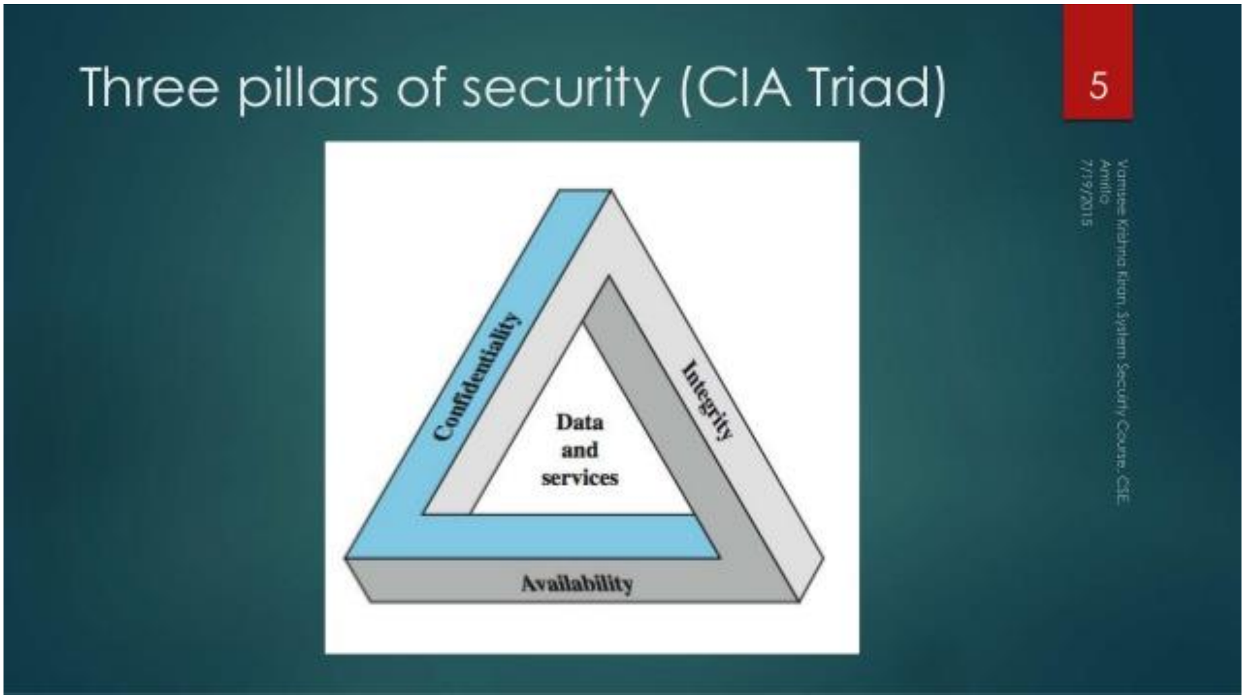
Integrity is the first pillar in these security practices that focuses on guaranteeing that information doesn't present errors or faults in communication. Threats and hazards that damage or destroy information infrastructures not only impact integrity but they also impact the productivity of a company. Integrity entails that all types of communication aspects are established correctly and with no interference. This means that the bridge that connects users, organizational units, external audiences happens properly with no interruptions. Without this pillar a company can't produce what they are trying to and can't get their users the tools to participate in their desired products.

Availability

Availability is the next major pillar that works hand and hand with Integrity. Availability focuses on guaranteeing that information is available to the users and to the system. This pillar is linked directly to productivity because availability allows users the right to access information when they request it, regardless of where they are located or when they want it to be present. While companies need to make sure this access is there, they have the challenge to ensure this access, but they use the tools of technology and devices to utilize this access. Frequently these technologies are at risk from attacks such as hijacking information through phishing attacks, spearing, social engineering and so many more. Companies focus on high availability, redundancy and speed in their connections.

Confidentiality

Confidentiality is the last pillar of security that focuses on guaranteeing that information is only accessed by users with due right. This pillar is a growing concern in the eyes of companies and security teams. Several cybercrimes techniques are linked to the theory of security and how information is accessed. This harps heavily on confidentiality. This pillar is directly correlated to the protection of users' privacy and their information. For the vast majority of organizations this is the most strategic pillar because it reflects on how good the protection of a business infrastructure is.



Three pillars of security (CIA Triad)

5

Vamsee Krishna Kiran, System Security Course, CSE
Amrita
7/19/2015

FIGURE 4. THREE PILLARS OF SECURITY

Security remains one of the most important values at organization seven though organization heads never show it, they also show of their product. Following these three pillars gives companies a good enhanced idea of what needs to be protected as well as why they need to be protected. At well robust security organizations like State Farm these three pillars are examined and are kept up to date with new tool and practices to ensure future safety and security. These principles are very important to follow as well as many other aspects of security including physical security which we will cover next.

To help us get a good idea of what physical security is I will give a personal experience from my summer internship. I had the opportunity to take part in as an IT technician at a financial accounting company. Physical security is just what it sounds like, it is the act of protecting personal information, hardware, software, networks, and data from any physical actions that could cause serious loss for an organization. The art of physical security is often overlooked since companies are always so worried on how to protect themselves from malware, hackers, and cyberespionage. While in essence physical security is a lot easier to implement as well as a lot easier for a hacker to use for their benefit in a social engineering attack. There are three major parts when it comes to physical security and these are access control, surveillance, and testing. At my internship I had the opportunity to experience all three of these first hand.

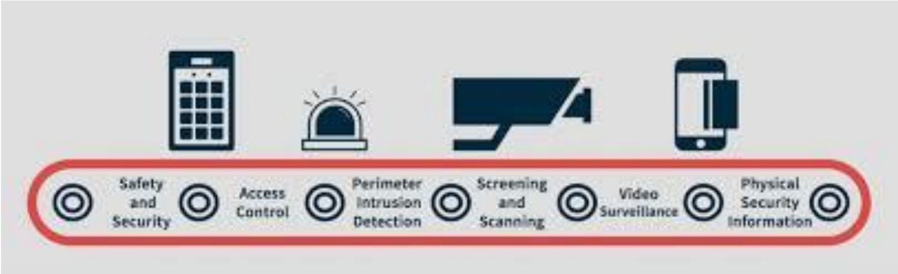


FIGURE 5. PHYSICAL SECURITY COMPONENTS

To start off is access control, how do we know who to give access to where and who is able to get behind what door. At this company we were located on the second floor of a large multi-use office building. In the space in which we use there are only four doors of access. The main door is the door to the front lobby where visitors and clients come in and are greeted by the front desk receptionist. The other three doors are located through the offices for employees to use to go to the restroom and the lunch facility located on the first floor. All of the three doors located throughout the office are locked at all times and take a key card access to get into that the Information technology team programs and assigns to employees. Everyone is allowed access to these doors during office hours to enter the office to do work. Now there is one other door with a 2 security locks on it and this is the door to the server room which only IT staff have the permissions to enter so no networking, firewalls, or servers are touched in any physical action. There are surveillance cameras at all entrances as well as spread out around the office building for monitoring. Additionally, there are cameras in the server closet just in case the door is broken into or breach by some sort of force. Now, having all of this physical security is great, and the monitoring is awesome, but it doesn't work if it is not tested. Monthly the doors are tested as well as the cameras to make sure they are still working to the guidelines in which are in place. As well as there are enforced rules that no accountant should leave their laptops unlocked when they walk away, nor should they leave documents laying all over their desk. To ensure that employees follow these directions we do weekly walk through at the end of the day to ensure everyone is following in suit. If not, action is taken by the heads of each department when we report what we find.

Physical security is an important part of security that like I said earlier tends to be overlooked. With good practices and much planning physical security can be made much easier and can be the first line of defense for an organization to stay safe from physical damage as well as social engineering attacks. For much more security the security team at an organization should look into the three pillars of security to ensure that their infrastructure, data, and services are all secure and within the right hands. Security can be very confusing for the normal human being who is not at all interested in the field, but it is very important to understand that most companies do keep a high standard to the amount of security that they enforce. What we talked about above is just a basic outside shield of what they practice ensuring that our privacy and information is secure and, in their hands, and not a malicious hackers' hands.

Conclusion

In conclusion, it is very important for an everyday individual to understand how valuable and safe their personal data is in the hands of companies and the organizations in which they belong to. Through the entirety of this paper we talked about what a breached looked like and we analyzed two larger companies and why they have been breached. The reason we did this is to let people know that companies do get breached if they are not careful and up to date with everything they do. To ensure that we aren't scared of companies and sharing our data we have viewed a company, State Farm, that has a very robust security department and why they stand out compared to the other two companies. With knowing this information, we hope to show consumers that questions about the security of an organization should be taken into consideration when thinking about giving out our personal information like credit information, social security information, and housing information. We showed what these companies do with this information and how they use it for their very own benefit which makes their information very valuable to many companies. Lastly, we scratched the surface on how companies do keep their companies safe with the three pillars of security as well as the first line of defense through physical security. The purpose of this paper was to have the average human to understand how important it is to keep our information secure with the big advances for moving into a digital world of tomorrow. Our information is the key to our humanity and with that data being stolen we have a hard time to get it all under control and reassessed. With knowing what can happen to our data we can start to secure ourselves through our passwords that we use on a daily basis. Doing this will make us more protected from malicious hackers as well as allowing us to help out organizations form being attacked through our access to their products. Knowing security is something every human should have a basic course on to ensure future success and safety.

For the future, I can see a lot more where this research can branch into and what other peers can take what I have started and build off upon. One of the things I wanted to do but never had the opportunity to during my time of research was to setup breach scenarios with a company or with a test server. I think that preforming pen tests, vulnerability tests, and audit security would provide a lot of background knowledge of what it is like to tests an organizations infrastructure and how to really make sure it is secure. These tests would be an outstanding way to prove to the public the type of scenarios the organizations that we are a part of set up to ensure that they are secure and keeping everything unavailable for those that shouldn't have the authorization. These tests would allow us to give readers a way of assurance as to how these companies are really keeping everything safe on a daily basis by giving an insight as to what these tests are and what the results show us security professionals. This would be great knowledge for the average human to know to give them the satisfaction that they are truly secure and safe as long as security teams keep at the jobs they do and don’t let human error get into the way.

Overall, security is a really complex field that involves so much more than what the average person knows. Everyone should get a taste of what security is and they should explore security and the value that is taken into action when it comes to everyday personal data. With this knowledge we can protect ourselves from loss of data. Knowing that our data is safe and valuable is always very relieving to a consumer. We can never get to achieve this until we realize that we can’t share our passwords just like we don’t share our underwear with others. This is when we can come to conclusion that we are safe and secure with our personal data.