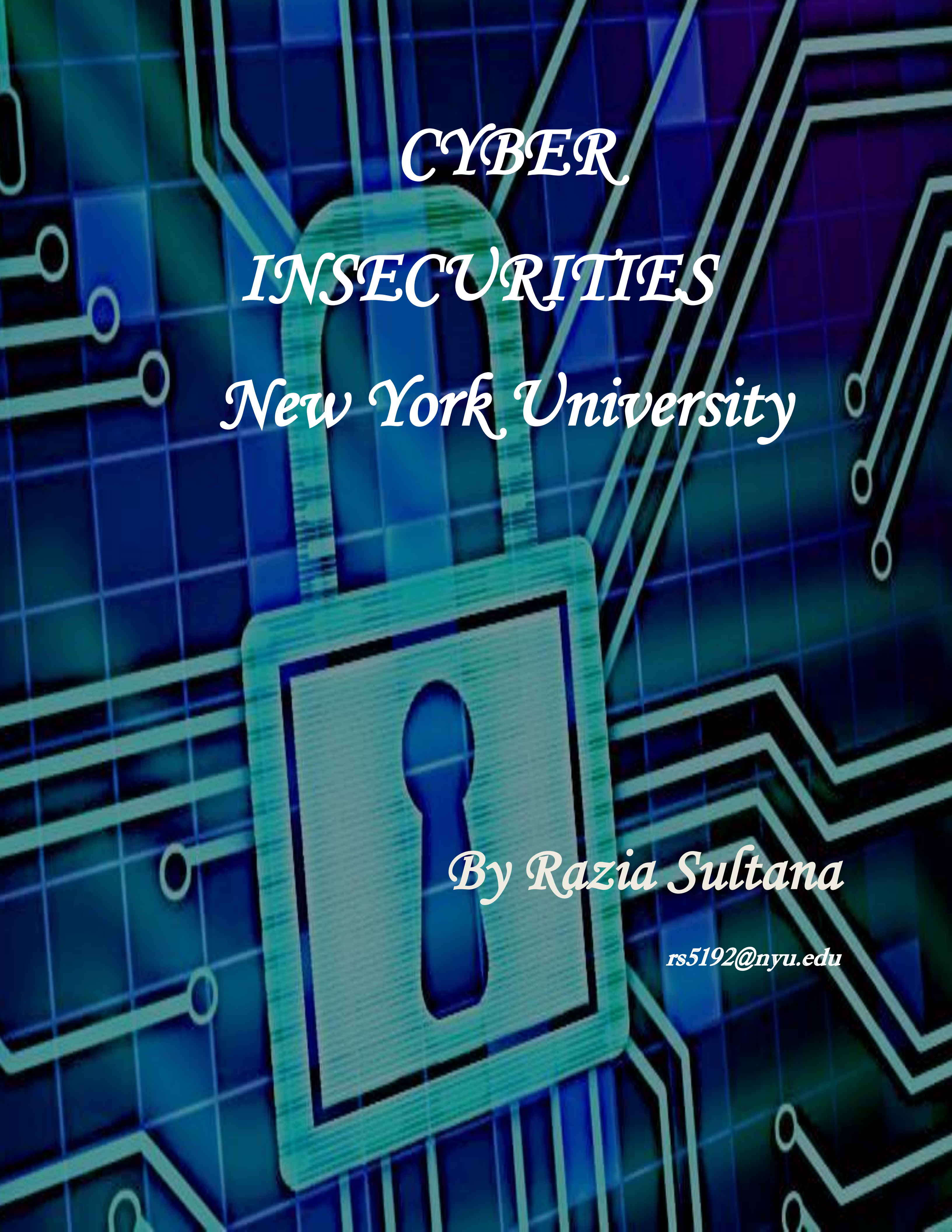


CYBER INSECURITIES

New York University

By Razia Sultana

rs5192@nyu.edu

CONTENTS

"All of a sudden, we've lost a lot of control,' he said. 'We can't turn off our internet; we can't turn off our smartphones; we can't turn off our computers. You used to ask a smart person a question. Now, who do you ask? It starts with g-o, and it's not God…"

~~ Steve Wozniak

The Land Of Integers

In 2006 I initiated my A. A.s degree in culinary arts from a campus in Florida as I was/am a passionate chef and all about anything to do with hospitality. My mental minor was always a curiosity about computers. I still remember opening the tower of my desktop in 2004, and staring at it with no clue about the bundle of wires in front of my eyes, and all I hunted to know was why the speed of the internet is so slow, when all the trouble shooting attempts came out with "no issues found"? I noticed dust trapped all over the wires and inside the tower, analogous to the one a human being finds in that vacant castle or a fort uninhibited or locked down for decades. So, I unplugged each and every wire, and in order for me to remember which plug belonged where, I took pictures from my phone so I could go back to them for conformation, as I was sure I will fail to recall.

The brand-new duster that was not bought to sweep interiors of a computer tower came in handy and I ran it all over the wires thus sweeping away a good amount of dirt. Plugging back all the plugs, as the pictures displayed (yes, I did forget which plug belonged where), still not knowing the outcome, but it felt good to have a clean tower (on the inside). Upon turning on my PC, I noticed a debauched noise rather than a gloomy sound from my tower, Internet opened in less than a minute, like when it was brand new.

Oh my God! The dust was slowing down the speed! It's not just the internal; it could be external too with computers. The thought that "my PC geek would never tell me what's wrong with my PC, but definitely charge me a bundle", always intrigued me to solving problems that seemed enormous, at home first. Whenever my family's regularly playing online games had the PC hacked I would immediately format it. What F7, F8 and F2 were capable off, was a lifesaving discovery, that I cultured just by trolling around and reading Microsoft articles that I found online.

The minute we see our computer screen opening internet pages back to back without any command, unplug the PC, from the roots to stop the transfer, and upon disconnection the files will not completely download, thus saving the user from a potential hack attempt. Whereas on the other hand an unfamiliar person may perhaps try to close those pages constantly and be stunned with the screen that would appear to read “you have been hacked”, and with that goes all your files, pictures, documents in the hands of the unknown. Privacy is endangered and could shortly go viral or a ransom can be demanded to have them back.

“There are no incurable diseases __ only the lack of will. There are no worthless herbs__ only the lack of knowledge”

~~ Avicenna

My father told me “don’t do Culinary, do something in computers” and I retorted “but I love culinary”, he never repeated. I always came handy to my sisters whenever there was an issue with their computers. I even discovered logging into their administrative accounts that had passwords and logging out respectively. All they were troubled with was for some reason the computer would ask them to change their password when they logged on. (lol)

I successfully graduated from my culinary degree in 2008 and thus catered to my community’s hospitality needs for the next 4 years. I started with a dinner for 8 guests, consequently upgrading to 500 people, who were served at the mosque during Ramadan, and I had 15 cooking nights out of those 30 days of Ramadan every year among other private occasions and parties. Heavy lifting landed me with 3 herniated discs, well used back I say, thus moving me to an office job as an insurance agent in January of 2013, where I found myself very comfortable in front of the computer screen, for a Muslim woman I must add.

I knew how to maneuver around glitches that generally popped up while filing and completing an E-application. I would find myself resolving them, while keeping my clients engaged in conversations on their dining table and it remained mysterious to them that I am having a computer cliché, thus submitting their E-applications efficaciously. Even though I had a bad start in life and I am still a struggler and can possibly be categorized among the survivors of happenings in life, a sense of curiosity to know what’s unknown to me keeps me going.

Life hit me again with its worst in November of 2013 and in order for my soul to remain thankful for what I have regardless of my brawls; I took up a week in Argentina for humanitarian efforts with Red Cross. I had signed up for it months ago through a couple who served at Red

Cross as they had no children and plenty of time on them. I met them on the road while walking with a gallon of gas in my hand, since my van ran out of gas and they stopped to give me a ride to a gas station. It wasn't a rocket science to predict I needed help. Nobody really wants to aid a Muslim as they fear unsafety, and thus they were a blessing in disguise for me. While in the process of getting me to a gas station and dropping me off back to my van, we connected as human beings. Ended up exchanging numbers, as they said "if I ever needed anything I could give them a holler", and in exchange I asked "how could I give my share to humanitarian efforts?"

This one week in Argentina changed my life, my purpose in life and thus gifted me with a brand new definition of who I want to become from here after. On my return back to the States I never took my connecting flight to go back to Florida, and while sitting at the airport I decided to make New York my new home. Sticking to my topic of subject, in fall of 2014 I applied at NYU as a resident of New York, not knowing what I want to pursue that instant except that it's Bachelors in Science. I was denied and suggested to re-apply again in the spring of 2015 as NYU had a high volume of applications. I continued with my life and applied again as advised. Getting accepted seemed like the unsurpassed thing to happen to me after over a decade for sure.

My advisor during our appointment asked me what I wanted to pursue in, and this time I knew I am going for Information Systems Management, and majoring in a degree my father suggested to me 10 years ago.

My topic of research will be *"Cyber Insecurities"* in Information Systems Management. During my research, I will be interviewing:

a) At least five Professionals who hold expertise in this medium.

b) My hands-on understandings and learnings as a member of staff in the IT Department of NYU. (Campus anonymous)

c) Evaluate while comparing and contrasting life before and after Technology.

This research will answer my curiosity, "Why cyber security that was not an important key or even considered I should say, when the first "personal computer" by Ed Roberts was introduced in 1975, has now become crucially important?"

I am thankful that Allah granted me with a will of not giving up no matter what, and knowing that "knowledge is power" keeps me motivated towards learning.

From Invention To Convention 176 Years Later

"The world is divided into men who have wit and no religion and men who have religion and no wit"

~~ Avicenna

In an attempt to constructing grounds for my topic of research I first wanted to get to the roots of my invention, a computer that is!

In 1822, Charles Babbage first idealized a machine capable of making computations. In 1936, Alan Turing created the first modern-style computer, and Konrad Zuse created the first electronic-programmable computer. In 1942, John Vincent Atanasoff created the first digital computer. In 1944, two University of Pennsylvania Professors built ENIAC, the first digital computer. This machine filled a large room and contained over 18,000 vacuum tubes. In 1946, the same two professors, John Mauchly and J. Presper Eckert, built UNIVAC, the first commercial computer. In 1953, IBM designed and marketed the first mass-produced computer and during the same year Grace Hopper created COBOL, the first computer language. In 1958, Jack Kilby and Robert Noyce created the first computer chip. In 1964, Douglas Engelbart created the first modern computer with a video screen, keyboard and a mouse.

Although each of the machines had a limited amount of memory available and ran on 8-bit microprocessors, the computers were affordable for the average person. Before this period, computers were built for businesses and government organizations only. They were built much larger and were much more expensive, so they were not practical for home use. In 1976, Steve Jobs and Steve Wozniak started Apple Computers and created the Apple I personal computer. I opened my research paper with Steve Wozniak's words of truth and a fact!

In 1981, IBM introduced the first personal computer to use Microsoft's MS-DOS operating system. In 1983, Apple released the first personal computer with a graphical user interface. In 1985, Microsoft created Windows, and in the same year the first dot-com domain name, Symbolics.com, was registered. In 1990, Tim Berners-Lee created HTML, which led to the formation of the World Wide Web.

Throughout the 1970s, a wide range of personal computers hit the market. While many of these models achieved some success, it was the Apple II, released in 1977, and the Intel- and

DOS-based IBM PC, released in 1981, that laid the groundwork for modern personal computers and most modern servers.

Apple quickly created a new personal computer called Lisa, which had a graphical user interface and allowed the user to perform simple options by using a mouse. IBM countered with its own new products. The rivalries grew throughout the 1980s, and this is when the rivalry between the Macintosh and Windows operating systems began. This contention is one of the reasons why personal computers were able to change so quickly with new technological advances. The companies pushed one another to find new technologically savvy ways of using personal computers, as companies also pushed to make the technology user-friendly. There was always an upgrade in hard drives, building an even speedier processor and a bigger RAM. More features such as USB ports, high-quality sound cards or latest wireless adapters models, enhanced appearances, lighter in weight, thinner in width, pocket sizes to carry conveniently just about anywhere.

The reason I wrote all the conceptions and their dates of birth, was so that hopefully you also get annoyed and recognize that Technology immediately after its first assembled has continually been on an upgrade, but “cyber security” was not even in question. And it remained immobile till after one hundred and seventy-six years of this invention (***176 years***), when one of the first recognized worms to affect the world's nascent cyber infrastructure in 1998 that spread around computers largely in the U.S hit. The worm used weaknesses in the UNIX system Noun 1 and replicated itself regularly. It slowed down computers to the point of being unusable. The worm was the work of Robert Tappan Morris, who said he was just trying to gauge how big the Internet was. He subsequently became the first person to be convicted under the U.S computer fraud and abuse act. He is still alive and now works as a professor at MIT (Massachusetts Institute of Technology).

What Did The Inventors Forget?

So, in my miniature diminutive brain I am thinking about this catastrophic state “cyber insecurities” as such: when I become rich and invest in a beautiful home or a mansion in a very safe location, I should still not overlook to install the latest home security system. But this is today’s convenience available to me. Let’s go back in the 90’s and reevaluate my options of security. When I become rich and invest in a beautiful home or a mansion in a very safe location, I must also have unleashed German shepherds, guarding all around my home, and have security guards at the main entrance. Security guards for all those who are invited and welcome, and German Shepherds for all those who are not invited, from the main entrance or from any loose loops on my property.

And that's exactly what the genius inventors of the "computers" forgot to do. They assumed coding, learning the language and applying the programs will always be practiced under the restrictions and compliance to the policy put in place respectively. They forgot it is a human, who is known to use the same weapon that is built for self-defense, to kill and hurt also. So, the human traits such as honesty, loyalty, sincerity, hatred, recognition, jealousy and betrayal from our non-technical lives transferred into the "land of technology" as well, overlooking it is human behind the screen too. Thus, giving us the great IT techs, Network administrators, Web developers, Database Administrators, Network architects, Information security analysts' programmers, software developers, Cyber security guards and Hackers also.

In the 1990s, the typical hacker's approach used to be "hit-and-run", and in many cases, it was about reputation and acknowledgement. Back in those days most organizations only had a firewall implemented between their internal network and the Internet. As time passed, the focus started fluctuating, and cyber-attacks evolved into a money-making profession for cyber criminals. As we are now living in the world we once thought of as the impending life, we are witnessing classy and besieged attacks and occurrences against many organizations and even people. And the most effective cyber-attacks are those that hack people rather than systems. Business email compromise attacks are one such example. There is no email virus that just deletes all the data, but the attempt made is to invade the privacy and put the owner in a state, where they feel stranded and raped.

So, who are these hackers? And the answer to that is, they are simply the software developers, who have a bandit in their biological systems by default and they just want to cause a hindrance, and defeat another program or a programmer by hacking their accounts or programs, exploiting a script, a command or a piece of data where they manipulate with the language, or even gaining access through open ports, tracking IP addresses just to prove "I code better than you, I just decoded your best created program, ha-ha!"

Man, Against Machine Or Machine Against Man?

Study shows a program that has just come in the market can only be tested so much. Practicing in a lab on mice, other animals or dissecting a human cadaver is one thing, and then a real human being in the surgery room is a whole different skill. So, a "lone" hacker will even target new programs to find holes, and thus taking over the control of the system the program is installed upon. And a common man usually clicks on "remind me later" when their computer pops on the screen "updates are available", thus dragging and delaying the patches to these holes and even protection from possible viruses the new programs introduce.

In Washington, on September 6th of 2017 the blind survey of 200 federal IT executives, performed by research company Market Connections, asked about modernization priorities at defense and civilian federal agencies. Respondents included decision makers who develop requirements for federal modernization projects, project managers and contracting officials. While nearly two-thirds of respondents (62%) rated cybersecurity as the top priority for agency modernization projects over the next year, nearly the same percentage (59%) reported that they think their agency's IT modernization efforts have resulted in an increase in the IT security challenges they face. And when asked to grade their agencies' modernization efforts, 43% graded those efforts at "satisfactory" or lower when it came to improving cybersecurity.

"The results of this survey tell us that many federal agencies may not have adequate staff and resources to manage security challenges in today's more complex and modernized IT environments, which in our view explains the feedback about modernization efforts exacerbating security challenges," said Venkatapathi "PV" Puvvada, President of Unisys Federal. "To achieve successful digital transformation, agencies must make security a priority and embark on projects that enhance security at the core, as well as boost operational efficiency to meet mission-critical goals".

I attended a meetup over the summer (2017) that discussed "Cyber Security" among other technical fields, and Ariel Cohen, a CEO of HackerUSA & HackerU International Marketing Manager, proclaimed that cyber security is such a mandatory requirement now. And that as we speak we need 100 thousand "cyber security guards". Sounds like an urgency to me!

"It used to be expensive to make things public and cheap to make them private. Now it's expensive to make things private and cheap to make them public"

~~ Clay Shirky, Internet scholar and Professor at N.Y.U

Above are the words of wisdom by Clay Shirky who is born in 1964 and is an American writer, consultant and a teacher on the social and economic effects of Internet technologies and journalism. My obligation and a duty as a reader of all these online links and books that I have and will be construing throughout my essays and research, is not to copy/paste you what happened and all the lengthy details of the incidents but to rather trace, "where and what went wrong? Can it be avoided in the future?"

Are We Trading Privacy For Security?

Privacy has been one of the most debated topics in the recent remembrance of technology. Not just the NSA (National Security Agency) but social platforms such as Twitter, LinkedIn, Instagram, Facebook and even snapchat are all rummaging through people's information, it's the entire online podium. Have you ever read all the permissions you agree to when you download an app to your mobile device?

Is this just the price we pay for living in the digital age or an infringement on our rights as citizens and consumers? And what are organizations doing to protect our information? How do we truly keep our data safe? Is there such a thing as "been safe" anymore? In just past few months, a scary strain of ransomware attacks such as WannaCry, Petya and Leaker Locker, has made chaos worldwide by shutting down hospitals, vehicle manufacturing, telecommunications, banks and many businesses. Let's not forget the infamous Mamba full-disk-encrypting ransomware and the Locky ransomware that caused commotion across the world last year and the bad news is, they are back with their new and more damaging variants than ever before. Unfortunately, at this time, there is no decryptor available to decrypt data locked by Mamba and Locky. Ransomware has become one of the largest threats to both individuals and enterprises in the last few months, initiating several widespread ransomware outbreaks.

The most recent and talked about breach is Equifax and it is confirmed as quoted "around 400,000 UK customers' data may have been accessed by hackers as part of the massive data breach that hit the firm in July this year (2017). Last week, the US-based credit rating firm announced that it was hit by hackers in what is now considered one of the largest data breaches of the year. The attack saw data of around 143 million U.S. customers possibly having been stolen by hackers. However, Equifax confirmed that the data affected did not include residential address information, password information and financial data. The firm also said that the "nature of the information" accessed suggests that "identity takeover is unlikely for the UK consumers who had their data potentially accessed in this incident". However, the firm said that it will offer affected customers a free comprehensive identity protection service, which will allow consumers to track their credit information, personal data and alert them of any potential signs of fraudulent activities..."

Did you sense the repair within this proposition or compensation? The offer that could have saved and protected the privacy and data of around 400.000 UK customers from going into the hands of the hackers as well as a well-known and recognized credit bureau from crashing! "A free comprehensive identity protection service". When 400.000 customers pay Equifax $19.95 per month, Equifax makes $7,980,000 a month, now times that to 12 will bring the yearly income of $95,760,000. And by the way, I didn't even add the 143 million U.S. customers possibly affected by this crash. Do we really think throwing that service @ $19.95 was not worth it? Anyways it's too late now; I don't even want the services from Equifax not even for free or @ $0.00, because I lost my trust. Do I have an account with Equifax? Quite honestly, I remember looking up online many times to track my current credit score, but I don't recall making an account, even though it is a required step, as they email you the report. And besides what difference would it make now anyways? Damage has been done!

Where Are My Rights Of Freedom?

The President of the United States Donald Trump has signed a "bill blocking online privacy regulation". As quoted in the Chicago tribune "The bill scraps a Federal Communications Commission online privacy regulation issued in October 0f 2017 to give consumers more control over how companies like Comcast, AT&T and Verizon share that information. Critics have argued that the rule would stifle innovation and pick winners and losers among internet companies. Supporters of the privacy measure argued that the company that sells an internet connection can see even more about consumers, such as every website they visit and whom they exchange emails with, information that would be particularly useful for advertisers and marketers".

What is wrong with the people in power, authority and supremacy? Who gave them the right and sanction to sign off people's privacy by passing a bill and making it legal and official? So, in layman's terms at the rate of an assigned cost, anyone can go to my internet carrier and buy my internet activity report, since the carrier holds my files, cookies and search history. Whereas on the other hand, the Trump administration announced this year in April of 2017 that it would no longer publicly release White House visitor logs, citing "grave national security risks and privacy concerns of the hundreds of thousands of visitors annually." Is this discrimination between the rich and the poor? Trump's White House visitors' logs are to be kept concealed, and my daily log of activity on the internet can not only be invaded but also be vended to anybody?

I found the answers to my rising questions and concerns on page 93 of the book I read this week by Christine Zuchora-Walske, "Internet Censorship". As quoted by the writer "Security and privacy are, to some extent, competing goals. U.S. society struggles to balance them. The editors of *USA TODAY* framed this debate in a June 2008 editorial. They wrote: "The question has never been whether terrorists are a threat to this nation (they are) or whether U.S. intelligence officials should be able to spy aggressively on them (they should). It's how to achieve those ends without trading away the privacy of Americans."

So, what is my hypothesis? Where do I stand on this topic? What kinds of research sources do I have? With all due respect to my readers, but I just could not think of any better way to explain the sensitivity of what we are dealing with here, so my starting point till further investigation is as below:

- Remember in the late 1990s when Internet pornography became accessible? It wouldn't permit one to excess, unless the viewer in interest made an account, paid a certain fee, and provided their age, since the underage users were prohibited to view the content. In doing so, the user would fear off and exit the site completely, as he or she didn't want to be traced, while looking up for sexual content online. That is exactly what needs to be done when online users look up for links to searches such as: ways to hack, phishing, how to decrypt sensitive transmissions, data information of such and such enterprise. The website should ask for the same exact questions that pornography sites asked prior to giving the excess.

Questions such as, are you a student, an employee, an employer, or a service man? The reason why you want this tutorial or information? Is it for a personal use or work related? And even a charge, a fee would push away the unwanted traffic.

- Let the FBI, the CIA, the police department, the forces, the law and officials that work to protect the security of a citizen from the threats have the excess to my information, let them wiretap my conversations or anyone they suspect, let them monitor my activity on social media for cyber bullying, but please please don't make it accessible to public, don't put it up for sale!
- Don't make it available to anybody who can pay $14.95 for a full report, or $0.99 for a 7-day trial. If they are my loved ones they will find me, but don't put my information for the unwanted and unwelcomed, to excess and obtain. The information is robed, stolen, unauthorized and misused more than just for a purpose of a reunion.
- We need to have cyber police, crimes are not only taking place in the streets, but now the online world and internet has also become an area of occurrence and illegal acts. Just how one dials 911 for an emergency, we need to have a helpline available when accounts are hacked, when privacy of our personal information is disbursed. Because it leaves the victim with the same feeling of incompetence, which one feels when attacked, robbed or even raped in the midst of the street.
- Lower down the costs of soft wares, apps to defend, fire walls to protect one's PC and the best anti-virus soft wares, so that everyone can easily purchase them and have their PC's protected and secured from the unwanted attackers, better yet even throw a free cd upon a brand-new purchase, thus keeping their consumers satisfied and safe.
- At home users are strongly advised to follow prevention measures in order to protect themselves. Beware of Phishing emails: Always be suspicious of uninvited documents sent over an email and never click on links inside those documents unless verifying the source.
- Backup Regularly: For a backup on all your important files and documents, keep a copy on an external storage device which you disconnect from your PC once the backup is complete.
- Keep your Antivirus software and system up-to-date to protect against the latest threats.

"The right of an individual to conduct intimate relationships in the intimacy of his or her own home seems to me to be the heart of the Constitution's protection of privacy"

~~ Harry A. Blackmun, Associate Justice of the Supreme Court of the United States

The Forgotten Amendments

Judicious and self-explanatory words of Sir Harry Andrew Blackmun, who was appointed by the Republican President Richard Nixon, served from 1970 until 1994, and ultimately became one of the most liberal justices on the Court. I find myself questioning the digital age, where the whole kingdom is under surveillance, "what happened to the constitution? The fourth amendment, that grants "people the right to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." The Fifth Amendment where "no person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand jury". Do these Federal officers even believe in "warrants" anymore? Remind me was the constitution categorical to been temporary or optional?

Seems like the National Security Agency (NSA), is unable to maintain the balance between justice, technology, surveillance and civil liberty of the people. Or else on the contrary we the Americans are back to square one, fighting for our human rights, that theoretically and lawfully we conquered when the founding fathers signed the Declaration of independence in 1776, two hundred and forty-one years ago.

I originate confidence in my intellectual thinking when I recited the dissenting opinion of Justice Louis D. Brandeis in Olmstead v. United States, as quoted "When the Fourth and Fifth Amendment were adopted, "the form that evil had theretofore taken" included the government forcing a person to incriminate themselves. The government could "secure possession of his papers and other articles incident to his private life-a seizure effected, if need be, by breaking and entry. Protection against such invasion of 'the sanctities of a man's home and the privacies of life' was provided in the Fourth and Fifth Amendments by specific language."

Justice Louis D. Brandeis appeared to be far in advance of his time in fighting for freedom of speech and the right to privacy even way back in 1928, as he was concerned with how privacy could lose out against "modern" technology being used by the government against the people like during prohibition times with telephone wiretapping. His words as quoted "Decency, security and liberty alike demand that government officials shall be subjected to the same rules of conduct that are commands to the citizen. In a government of laws, existence of the government will be imperiled if it fails to observe the law scrupulously. Our Government is the potent, the omnipresent teacher. For good or for ill, it teaches the whole people by its example. Crime is contagious. If the Government becomes a lawbreaker, it breeds contempt for law; it invites every man to become a law unto himself; it invites anarchy. To declare that, in the administration of the criminal law, the end justifies the means 'to declare that the Government may commit crimes in order to secure the conviction of a private criminal' would bring terrible retribution."

"We need to encode our values not just in writing but in the structure of the internet"

~~ Edward Snowden

May well be Edward Joseph Snowden, a thirty-four-year-old, former Central Intelligence Agency employee, and a former contractor for the United States government who copied and leaked information from the NSA in 2013 without authorization, in saying what he did, recollecting his precise words, "I don't want to live in a society that does these sort of things, surveillance on its citizens ... I do not want to live in a world where everything I do and say is recorded ... My sole motive is to inform the public as to that which is done in their name and that which is done against them."

During my readings on Snowden I found that it all began on June 5th of 2013, when the media reported the documents that held existence and functions of classified surveillance programs and their scope. The first program that was revealed was PRISM, it allows for court-approved direct access to Americans Google, Yahoo, AOL, Apple, Skype, Microsoft, YouTube and Facebook accounts. Reported from both The Washington Post and The Guardian that published one hour apart. Barton Gellman of The Washington Post was the first journalist to report on Snowden's documents.

He said the U.S. government urged him not to specify by name which companies were involved, but Gellman decided that to name them "would make it real to Americans." The original reports included details about NSA call database, Boundless Informant, and of a secret court order requiring Verizon to hand the NSA millions of Americans phone and internet records daily, and those of "high-profile individuals from the world of business or politics." XKeyscore, an analytical tool that allows for collection of "almost anything done on the internet," was described by The Guardian as a program that "shed light" on one of Snowden's most controversial statements: "I, sitting at my desk (could) wiretap anyone, from you or your accountant, to a federal judge or even the president, if I had a personal email."

This is so scary! I watched the movie "Snowden", as he has been the subject of my hunt throughout this week, whether it is googling or YouTube. I scrutinized and observed all his interviews and paid attention to all the evidence he conveyed and it felt like I am under a cyber-attack while in the privacy of my home. Or let me rephrase that: "while I assume I am at home alone!" There is no eavesdropping, no thieves coming through my windows or from a door left unlocked. Deskbound in a state of shock I am inaudibly discerning to me personally, "do these federal officers disconnect while wiretapping, when they track a conversation where two people in love, are confessing their frame of mind to each other on the phone? or when they are video chatting on skype, may be even divulging their physiques to each other to boot out the desire and longing, in the meantime, as they are not with each other in person, due to travel, long distance or whatever the reason may be for God's sake!" Or do they listen and watch and comment and laugh and make fun of a natural and by standard an emotional state of the human being? Like some directors of a movie.

I am not just exaggerating or going nuts, for the reason that the leaked documents did show that NSA agents also spied on their own "love interests," a practice NSA employees termed LOVEINT. The NSA was shown to be tracking the online sexual activity of people they termed "radicalizers" in order to discredit them.

Since when an acquiesced sexual activity between two people required a third party's ruling or judgement whether it is unadulterated, untainted or ridiculous? And if NSA's purpose is "the security of the Americans" then why were they not able to save the thirteen-year-old Megan Meir of Dardenne, Prairie, Missouri who hung herself with a belt in her bedroom closet and died the next day, after receiving disturbing messages from her online acquaintance, who later on was discovered to be non-existing. It was a parent in the neighborhood, who despised Megan as she had broken her friendship with her daughter. And thus, she made an account under "Josh Evans", as a sixteen-year-old, so that she could track Megan's online activity, to see if she was bad mouthing her daughter. Not to mention becoming Megan's cyber friend.

If security is NSA's reason of "surveillance" then why were they not able to sojourn the Boston Marathon bombing on April 15, 2013? In which two homemade bombs by two brothers killed three people and injured several hundred others, including sixteen who lost limbs. As Snowden said in one of his interviews "When you are collecting everything you understand nothing." And why are the records on law abiding people under examination anyways? I thought we were protecting the Americans from the terrorists. "Have we moved from exceptional surveillance to everyone's surveillance?" (Snowden)

If protecting the Americans is NSA's foremost vital of "surveillance" then why were they not able to protect me? I was engaged to be married to a person residing back in Pakistan. I filed a fiancé visa for him in 2009, which got rejected and remained in pending from 2010 till 2013, without any further evidence on to why it's been rejected. Helplessly and relentlessly I found out on my own after six months that he was a married man, and was seeking to come to America. Upon which I ended my six years of an affair that was once my whole world. Was NSA watching us? Were they wire-tapping our phone conversations, skype chats, pictures, messages? Why didn't I get a knock on my door from a federal officer to inform me that I am a target of a scam and to save me my time, money not to mention my heart that I put on the line for this affiliation?

What are they even doing with all this data they are attending to, in millions on a daily base? When they can't even save a life, a terrorist attack, online fake accounts, cyber thefts, cyber killings. Where is NSA, when you need 'em?

A NSA mission statement titled "SIGINT Strategy 2012-2016" affirmed that the NSA had plans for continued expansion of surveillance activities. Their stated goal was to "dramatically increase mastery of the global network" and "acquire the capabilities to gather intelligence on anyone, anytime, anywhere." Leaked slides revealed in Greenwald's book "No Place to Hide", released in May 2014, showed that the NSA's stated objective was to "Collect it All," "Process it All," "Exploit it All," "Partner it All," "Sniff it All" and "Know it All."

Snowden stated in a January 2014 interview with the German television that the "NSA does not limit its data collection to national security issues, accusing the agency of conducting industrial espionage. Using the example of German company Siemens, he stated, "If there's information at Siemens that's beneficial to US national interests - even if it doesn't have anything to do with national security- then they'll take that information nevertheless."

In May 2015, Snowden's lawyer Ben Wizner said that Snowden's main source of income was speaking fees, which sometimes exceeded $10,000 per appearance. In November 2015, Snowden said that he does not intend to play any role in Russian politics and wants to devote his focus to U.S. issues. During a panel event, he said, "people say I live in Russia, but that's actually a little bit of a misunderstanding. I live on the Internet."

So, Edward Snowden broke the policy and procedures that he swore to comply to and abide to. NSA broke the constitution, the fourth and the Fifth Amendment. Snowden is in exile, to be arrested at sight found whenever and wherever, so should NSA!

Snowden opened a Twitter account on September 29, 2015, amassing over a million followers in the first 24 hours; he followed only the NSA. His first tweet received 121,728 retweets and 117,750 favorites. I searched him up on Twitter, messaged him without any care for a comeback, and now I, also follow him on Twitter!

"The law to-day is absolute and inexorable — it has even set itself above Justice, whose instrument it was intended to be. In earliest times, there was no elaborate code of law; there was but a simple idea of justice. As the race moved forward, its conception of justice kept pace with the changing standards of customs of the times. As society became more complex, a caste arose whose duty it was to administer justice. In the course of time, however, the law grew up out of their decisions and accumulated a stolid mass of outworn tradition, until to-day legality has become so encumbered with lifeless relics of the past that the courts no longer express living social standards and the ideal of Justice, but merely the dead weight of legal precedents and obsolete decisions, hoary with age."

~~ Margaret Sanger, "Shall We Break This Law?"

In qualifying the constraint of my broadsheet, as I was scrolling through quotes and words of astuteness, which were eternally vocalized to sojourn the injustice and exploitation, the passage above detained me. A feminist and founder of the Planned Parenthood Federation of America, Margaret Higgins Sanger who battled the government and the Roman Catholic Church to establish the legitimacy of birth control.

Social And Economic Effects Of Technology

At times I feel as if there is no law or control even placed to defend the cyber insecurities. In the earlier times a bandit or a robber had to plot, arrange a gun or a weapon, a mask, a sack to hold all the looted property, an escape passage, a backup program. And even if he magnificently accomplished his undertaking or assignment, it was not even close to the figures and records these breaches cause.

As we declaim and perceive, the wave of data breaches continues to roll on. The next few sheets of my research will be boredom, a copy/paste blog looking study with many bullets, but I find it enormously essential and significant to discuss and reference to my readers, as to the extension of social and economic damage caused by cyber insecurities. Let's take a look back at some of the largest and most damaging data breaches on record. TechTarget defines a data breach as "an incident in which sensitive, protected, or confidential data has potentially been viewed, stolen, or used by an individual unauthorized to do so. Data breaches may involve payment card information (PCI), personal health information (PHI), personally identifiable information (PII), trade secrets or intellectual property."

But how long have data breaches been a concern for companies and consumers, and what kinds of impact have data breaches had throughout the history? I will briefly go over few Breaches and charts that read the statistics.

Studies show that majority of the largest breaches recorded result from hacking attacks, while one of the earliest reported data breaches, impacting AOL and compromising 92 million records in 2005, is reported as an inside job. Another AOL breach in 2006, resulted from accidental publishing of sensitive data; this breach compromised 20 million records. A data breach impacting the U.S. military is another notable exception to the rule, with 76 million records compromised in 2009 as the result of lost or stolen media. There were a total of 980 data breaches reported by ITRC, (Interstate Technology & Regulatory Council) in 2016. Compared to 2015 data breach statistics of 781 data breaches, it is quite clear that people's identities are still unsafe in the digital maze.

U.S. companies and government agencies suffered a record of 1,093 data breaches last year (2016), a 40% increase from 2015, according to the Identity Theft Resource Center. While data protection remains a big challenge in modern multi-faceted businesses, many bigwigs have coped to get a place in the top data breaches of 2016. Here is a hasty synopsis of the "biggest data breaches in the past 10 year",

Breaches:

- TK/TJ Maxx: 94 million records compromised in 2007
- Sony PlayStation Network: 77 million records compromised in 2010
- Sony Online Entertainment: 24.6 million records compromised in 2011
- Ever note: 50 million records compromised in 2013
- Living Social: 50 million records compromised in 2013
- Target: 70 million records compromised in 2013
- EBay: 145 million records compromised in 2014
- Home Depot: 56 million records compromised in 2014
- JP Morgan Chase: 76 million records compromised in 2014
- Yahoo: 500 million user accounts were made public in 2014
- Anthem: 80 million records compromised in 2015
- Southern New Hampshire University-SNHU: 140,000 data records in 2016

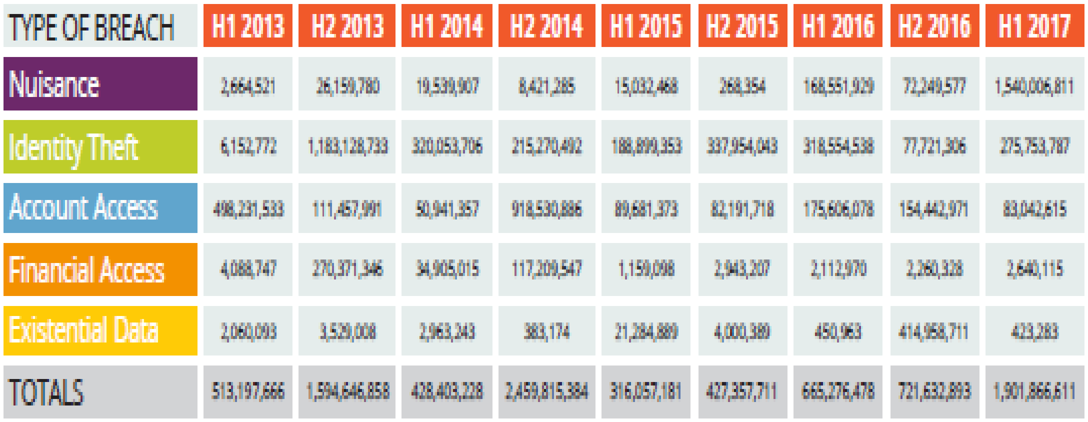
- Centene Corp Health care: 950,000 records of the individuals in 2016
- Department of Homeland Security/ FBI: 9000 employees' info leaked in 2016
- Washington State Health Authority (HCA) / Medicaid: 91,187 Washington Apple health clients in 2016
- University of California Berkeley a criminal data breach 80,000 students' records in 2016
- 21st Century Oncology a data intrusion of 2.2 million patient records in 2016
- Verizon Enterprise Solutions 1.5 million customers' data records were stolen in 2016

The terms "data breach" and "cybercrime" are often used interchangeably, and though closely related they are not synonymous. The simplest definition of cybercrime is "criminal activity or a crime that involves the Internet, a computer system, or computer technology". In the course of most cybercrime, some form of data breach is likely to take place; however, not all data breaches require the use of a computer. With even the world's largest companies suffering massive data breaches impacting millions of consumers, modern enterprises require a comprehensive, full-circle approach to data protection and security. The reactive approaches of yesterday simply don't cut it in the modern threat landscape!

Types Of Breaches:

- Identity theft remains the most common breach type accounting for 74% of all breaches. That's 49% increase from the previous year. The total of records compromised in an identity theft breach increased by 255% compared to last year. 275 million records were involved in identity theft breaches in the first six months of 2017.
- Financial access is the second most common attack vector, accounting for 13% of the breaches. Even though that's a 33% decline if compared to the previous year (2016), the number of records stolen increased by 17% to 2.6 million.
- Account access is the third most common type of data breach, with 83 million records impacted.
- Existential data accounted for 6% of data breaches and 423,000 stolen records.
- Nuisance attacks accounted for only 1% of data breaches but resulted in the compromise of 1.54 billion records, or 81% of the total.

- This represents a 2,000% increase from 720 million in the last six months.

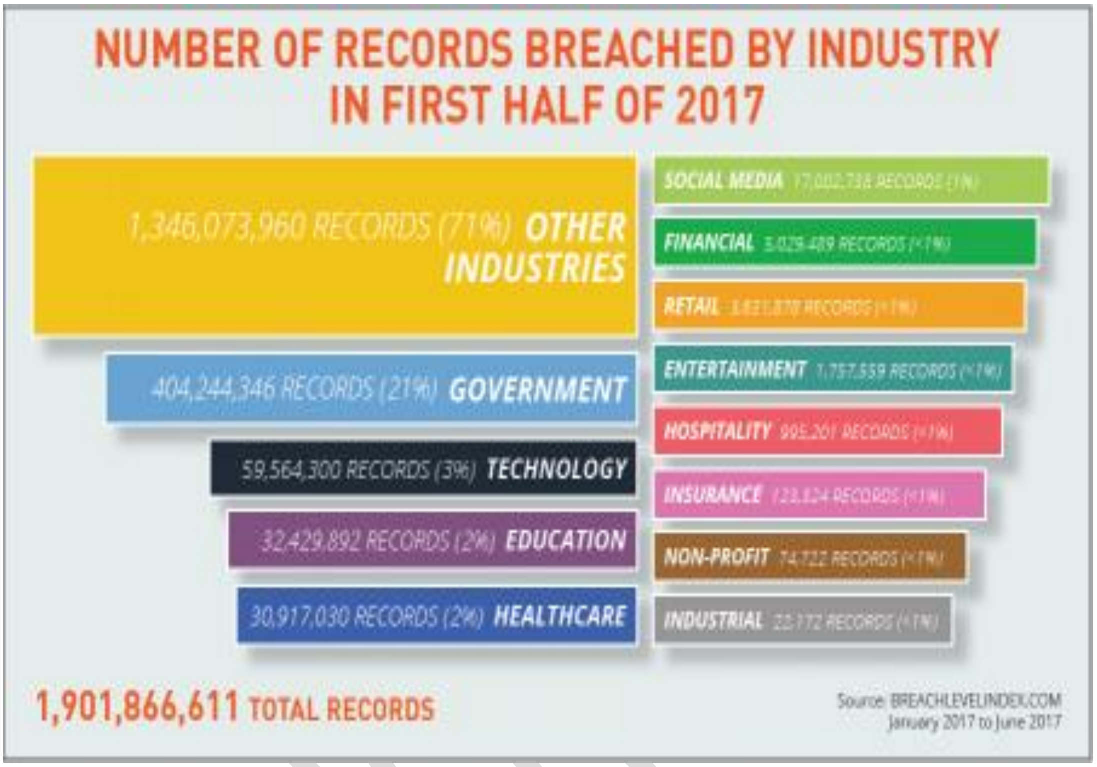


TYPE OF BREACH	H1 2013	H2 2013	H1 2014	H2 2014	H1 2015	H2 2015	H1 2016	H2 2016	H1 2017
Nuisance	2,664,521	26,159,780	19,539,907	8,421,285	15,032,468	268,354	168,551,929	72,249,577	1,540,006,811
Identity Theft	6,152,772	1,183,128,733	320,053,706	215,270,492	188,899,353	337,954,043	318,554,538	77,721,306	275,753,787
Account Access	498,231,533	111,457,991	50,941,357	918,530,886	89,681,373	82,191,718	175,606,078	154,442,971	83,042,615
Financial Access	4,088,747	270,371,346	34,905,015	117,209,547	1,159,098	2,943,207	2,112,970	2,260,328	2,640,115
Existential Data	2,060,093	3,529,008	2,963,243	383,174	21,284,889	4,000,389	450,963	414,958,711	423,283
TOTALS	513,197,666	1,594,646,858	428,403,228	2,459,815,384	316,057,181	427,357,711	665,276,478	721,632,893	1,901,866,611

Most Targeted Industries:

- Healthcare was hit the hardest, with 228 breaches (25%) and 31 million stolen records. Notably, that's up 423% compared to the previous six months.
- Finance is traditionally targeted, with 125 breaches (14%) and 5 million stolen records, up 389% from the previous six months.
- Education experienced 118 breaches (13%), with 32 million stolen records, a 4,957% increase from last year's 641K.
- Retail sector experienced 112 breaches (12%) and 4 million stolen records.
- Public sector breaches account for 10% with 89 breaches and staggering 404 million exposed records, which is 714% up from last year.
- Tech companies experienced 76 breaches (8%) exposing 60 million customer records.
- Entertainment services had 32 breaches (4%) and 1.7 million exposed records.
- North America tops the list of regions with the greatest total of disclosed breaches (808).
- European businesses only disclosed 49 breaches that resulted in the theft of 29 million records.
- Headline-grabbing hacks, with victims ranging from Wendy's Co. to the Democratic National Committee, are increasing despite regulatory scrutiny and more aggressive cyber-security spending.
- Worldwide spending on security related hardware, software and services rose to $73.7 billion

in 2016 from $68.2 billion a year earlier, according to researcher IDC (International Data Corporation). And that number is expected to approach $90 billion in 2018.



Source: BREACHLEVELINDEX.COM
January 2017 to June 2017

“Breach” is such a small word yet it holds such a catastrophic volume of damage that befalls the HealthCare’s, financial institutions, educational and the industrial domains left alone the millions and billions of dollars in loss but also the invasion of its consumer’s records, privacy, data that transmits all the personal information. Next I would like to share a letter or two where the consumer is informed of the breach, in such a simple vocabulary that it makes me wonder if the consumer even reads the whole letter or disregards it thinking “oh, this notification does not pertain to me!”

Letter # 1:

AG COAKLEY OFFERS ADVICE TO CONSUMERS ABOUT THE SE-CURITY BREACH ANNOUNCED BY TJX COMPANIES, INC.

BOSTON - On Wednesday, January 17, 2007, The TJX Companies, Inc. announced that it had determined that information was stolen from its computer systems that process and store information related to customer transactions. TJX reports that in-formation regarding credit and debit cards sales transactions in TJX's stores in the U.S., Canada, and Puerto Rico during 2003, as well as such information for these stores for the period from mid-May through December 2006, may have been accessed. At this time, Federal law enforcement authorities are investigating the alleged breach. In light of this recent news, Attorney General Martha Coakley offers consumers information on how to protect their credit and debit information against identity theft.

To protect against identity theft, consumers who have shopped at the TJX Stores, including Marshalls, TJ Maxx, Home Goods, AJ Wright, and used their credit or debit card, or a check, to pay for goods purchased, may wish to take the following cautionary steps:

1. Call one of the three major credit bureaus and place a one-call fraud alert on your credit report:

•Equifax: Call (800) 525-6285, and write: P.O. Box 740241, Atlanta, GA 30374-0241.

•Experian: Call (888) 397-3742, and write: P.O. Box 9532, Allen, TX 75013.

•Transunion: Call (800) 680-7289, and write: Fraud Victim Assistance Division, P.O. Box 6790 Fullerton, CA 92834-6790.

You only need to call one of the three credit bureaus; the one you contact is required by law to contact the other two credit bureaus. This one-call fraud alert will remain in your credit file for at least 90 days. The fraud alert requires creditors to contact you before opening any new accounts or increasing credit limits on your existing accounts. When you place a fraud alert on your credit report, all three credit bureaus are required to send you a credit report free of charge.

2. Order a copy of your credit report, and look for unauthorized activity. Look carefully for unexplained activity on your credit report.

3. If there is unexplained activity on your credit report, you may want to place an extended fraud alert on your credit report. In order to do this, you need to file a police report with

your local police department, keep a copy for yourself, and provide a copy to one of the three major credit bureaus. Then an extended fraud alert can be placed on your credit file for a 7-year period. This will mean that any time a user of your credit report (for instance, a credit card company or lender) checks your credit report, it will be notified that you do not authorize any new credit cards, any increase in credit limits, the issuance of a new card on an existing account, or other increases in credit, unless the user takes extra precautions to ensure that it is giving the additional credit to you (and not to an identity thief).

4. Contact the fraud departments of your credit card issuers or bank. You may want to contact the fraud department of the Credit Card Company or bank that you used when you made purchases at the TJX stores. These financial institutions can monitor your account for suspicious activity. You may also wish to cancel these accounts; you can discuss this option with your Credit Card Company or bank.

Additionally, TJX has established a toll free customer help line. Callers from the United States may reach the help line at (866) 484-6978. TJX has also posted information on its web site at www.tjx.com.

If you believe that you have been the victim of identity theft, you will need to take additional steps to protect your credit and your good name. For additional information, consumers may contact the Attorney General's consumer hotline at (617) 727-8400, or view the Federal Trade Commission's identity theft resource, available at www.consumer.gov/idtheft/.

Letter # 2:

Equifax Data Breach Equifax recently disclosed a data breach they experienced which exposed personal information of over 143 million US customers. Equifax stated the breach occurred mid-May through July 2017. During this timeframe, the hackers were able to access:

- Names
- Social Security Numbers
- Birth Dates
- Addresses
- Driver’s License numbers (in some instances)
- Credit card numbers for approximately 209,000 people were stolen
- Dispute documentation with personal identifying information for approximately 182,000

people was stolen.

If you have specific questions about this breach, you can visit Equifax’s website at: www.equifaxsecurity2017.com or contact the dedicated call centers at: (866) 447-7559.

Bank of Sun Prairie is committed to educating you on how you can protect your credit, account information and your identity. Please be aware of further scams such as; fraudulent calls, phishing scams, etc. We offer several tools and resources, such as:

•Card Valet – An application to help monitor debit and/or credit card transactions

•Fraud Text Alerts – Alerting you of suspicious debit card activity

•Identity Theft Video – Learn about various scams and ways to protect your identity

1. If your identity has been stolen, you need to take immediate action to limit the damage and protect your good name.

2. Download our free Identity Theft Emergency Repair Kit (PDF) It provides step-by-step instructions and the necessary forms to help restore your identity.

3. Contact Bank of Sun Prairie and other related vendors immediately.

4. Close any accounts that may have been tampered with or opened fraudulently. Place a fraud alert or freeze on your credit report with the three major credit bureaus.

•Also request to review your credit report for suspicious activity. A copy of your credit report is available free each year from https://www.annualcreditreport.com/index.action.

•Equifax®: 1-888-766-0008

•Experian®: 1-888-397-3742

•TransUnion®: 1-800-680-7289

5. File a complaint with the Federal Trade Commission at https://www.ftc.gov/.

6. File a report with local police.

Thank you for choosing Bank of Sun Prairie as your trusted financial partner. We’re committed to helping you in any way we can. If you have any further questions, please don’t hesitate to contact Bank of Sun Prairie at (608) 837-4511.

Sincerely,
Jimmy Kauffman
President & CEO

I deliberately chose the first letter that asks its consumers to contact the top three credit bureaus to get a credit check if incase one's social security number has been used without authorization, and then the letter that follows informs the consumers of one of the top credit bureau's breach itself. It saddens me to see the consumer's state of vulnerability. As not all the consumers know and understand what a breach could mean for them and their information.

Human Values And Principals On Pilot

News breaks all the time that hackers have attacked yet another company. Media outlets regularly cover cyber events. The President issues executive orders, and Congress explores cyber legislation. With all these events happening, business leaders and end-users that are "us the people" must ask: what does this mean for my business and me? Brian Minick the author of the book Facing *Cyber Threats Head On* looks at cyber security from a business leader perspective. By avoiding deep technical explanations of "how" and focusing on the "why" and "so what," this book guides readers to a better understanding of the challenges that cyber security presents to modern business, and shows them what they can do as leaders to solve these challenges.

Facing Cyber Threats Head On explains that technology is not the answer to cyber security issues. People, not technology, are behind emerging cyber risks. Understanding this brings to light that cyber protection is not a battle of technology against technology, but people against people. Based on this, a new approach is required; one that balances business risk with the cost of creating defenses that can change as quickly and often as attackers can.

- As an example of one initiative undertaken to accomplish its CNCI (Comprehensive National Cyber Security Initiative) responsibilities, the DHS is currently deploying the Einstein Program (2017), within the DHS and plans to expand it to all federal departments and agencies. The Einstein Program is an early warning system that will help "identify unusual network traffic patterns and trends which signal unauthorized network traffic so security personnel are able to quickly identify and respond to potential threats." However, the program isn't sufficiently living up to those goals.
- Hacking and IT security issues, including phishing scams and ransom ware attacks, are still the leading causes for the largest health data breaches in 2017, according to data from OCR. The three largest incidents thus far – two of which are classified as either hacking or an IT

incident – have also potentially impacted 1,497,800 individuals.

- No healthcare provider can ensure that a data breach will never take place, but these incidents further show why organizations need to take the time to regularly review their physical, technical, and administrative safeguards. Comprehensive employee training is also critical, especially with ransom ware attacks on the rise. Entities of all sizes need to feel confident that staff members can potentially recognize an attack, and report it to the proper authorities instead of clicking on or opening a malicious link or email.
- There are also five U.S. government sponsored virtual worlds created in Second Life, two by the National Aeronautics and Space Administration, one by the National Oceanic and Atmospheric Administration, one by the Centers for Disease Control and Prevention, and one jointly created by the Air Force, Navy, and Army.
- While use of social media improves collaboration, streamlines communications, costs little or nothing to use, potentially attracts young recruits into government service, and is highly portable, its use also creates a cyber-security risk because social media make sensitive information publicly available on the Internet, complicate compliance with federal regulations, do not adhere to standards, put employee personal information at risk, and demand a lot of bandwidth.
- An effective national cyber security program requires – as stated in Executive Order 13,010, PDD 63, and subsequent initiatives – the fully coordinated authority and efforts of all federal departments and agencies, state and local governments, the private sector, and the international community.

Brian Minick is absolutely correct when he says above that “understanding this brings to light that cyber protection is not a battle of technology against technology, but people against people”. It is the “people” behind all this ordeal and technical insecurity. Again, this approach sounds fantastic and I am sure they are already working towards its implementation among all the organizations, sectors whether be private or commercial, yet again it’s nothing that protects or even teaches the common man, the end-user, me! Even though I am at home I still have an excess to the internet. That means I am vulnerable to an attack, but do I have the knowledge and information on how to keep myself and my loved ones protected from the terror caused via online?

The Corruption On The Internet

Two Types Of Web

1. The Deep Web:

I searched the types of webs and found out that the Surface Web is the opposite of the Deep web, and is available to the public and can be indexed by standard search engines. The surface web is that web you are most familiar with but the fact is that it is only the 4% of the whole web.

So let's start with our day to day accessing the online world. Did you access your email, checked your Facebook messages and your private Drop box? If you did at least one of these then you accessed the deep web. The deep web isn't some mysterious place as depicted. Instead it is the collection of millions of files on the internet that aren't publicly available. Imagine if anyone could access your email? It wouldn't be moral. So it's "hidden" from the regular web. The deep web is about 95% of all the data available online, which isn't surprising when you think about the amount of private data there really is.

The remaining 96% of the web is what we call "Deep Web". The Deep web cannot be indexed by your standard search engines. To access the contents of the Deep Web you need a dedicated browser. TOR browser is most commonly used to access deep web. Secondly, many websites in the "Deep web" are not legal to visit. Some people enjoy child pornography, snuff films, torture flicks, and other unpleasant kinds of socially unacceptable "entertainment". The deep web is where the dredges of society get their material. The deep web is also the black market for everything you can imagine. Child trafficking, prostitution, drug dealing, organized crime; essentially anything which is illegal on the mainstream Internet relies on the deep web's anonymity to continue operating.

These websites frequently change addresses and need quite an effort to find them. Because of the nature of these websites, their visitors are monitored. Although law enforcement may do their best to have these websites shut down, the deep web is under no legal jurisdiction (hence, the reason for the deep web's existence). People who visit these websites without going to prison are employing certain precautions to avoid being tracked.

There are hardware and software methods to remain anonymous online, and people who browse the deep web with intent, build a barrier of protection around their Internet identity. However, someone who browses the Deep web out of pure curiosity can also get into serious legal trouble (I hope your interest in the deep web is simply curiosity). Your intentions for visiting restricted websites are irrelevant to law enforcement.

Think of it this way, if you went to someone's house out of curiosity to watch a murder, would your intentions for being there matter? Absolutely not, you would be hauled to court with any number of charges against you simply because you chose to be there voluntarily.

The deep web is no different, and the easiest people to catch are the "tourists"; the curious citizens who skip into the deep web without anything in place to keep their identity and location anonymous. Users who are dead set on visiting the deep web look into what software and hardware they need to have in order to browse anonymously.

2. *The Dark Web:*

Now let’s discourse about the horrendous fragment. A Google search explains that the dark web is similar to the deep web in the respect that it is hidden from the normal web. However, the dark web is not information that is not linked, rather it is purposely hidden. To access the dark web, you need to use special tools like Tor or Freenet. These are the only ways to get to this hidden content. Though the deep web makes up 95% of the entire internet the dark web only consists of about .03%. But that small section has millions of monthly users. The Dark Web anonymity attracts criminal activity ranging from the sales of illegal drugs and trading of weapons and even the hiring of contract killers. Infamous examples of Dark Web sites include the Silk Road and its offspring.

The Silk Road was (and maybe still is) a website for the buying and selling of recreational drugs. But there are legitimate uses for the Dark Web. People operating within closed, totalitarian societies can use the Dark Web to communicate with the outside world.

The Dark Web hit the headlines in August 2015 after it was been reported that 10GB of data stolen from Ashley Madison, a site designed to enable bored spouses to cheat on their partners, was dumped on to the Dark Web. Hackers stole the data and threatened to upload it to the web if the site did not close down, and it has now acted on that threat. Now the spouses of Ashley Madison users have begun to receive blackmail letters demanding they pay $2500 in Bitcoin or have the infidelity exposed.

In March 2015 the UK government launched a dedicated cybercrime unit to tackle the Dark Web, with a particular focus on cracking down on serious crime rings and child pornography. The National Crime Agency (NCA) and UK intelligence outfit GCHQ are together creating the Joint Operations Cell (JOC).

Contingent on what you intend to do on the Dark Web, some users recommend placing tape over the laptop's webcam to prevent prying eyes watching you. A tinfoil hat is also an option. The difficult thing is knowing where to look. Some of the content on the dark web consists of sites that sell narcotics, hacked PayPal accounts, fake IDs, etc. There's also child pornography, rape videos, and animal abuse videos; alongside this, you might find strange and bizarre "special interest" forums and social networks.

Here we the parent let this technology babysit our children, if only we knew that not only does it have our child’s favorite cartoons or a show but also an access to all these adult platforms and environments that we pray our children never have to witness or become a part off in million years. Little do we know that this vulnerability is available on the tips of the fingers, one wrong click and our underage child is in the hands of danger and viciousness!

A Bandit In Biological System By Default

The Blue Whale Game:

“A new, dangerous online game referred to as the Blue Whale Challenge is reaching young people and causing harm, first abroad and now in the United States,” the American Foundation for Suicide Prevention said in a statement ‘parents not discuss the Blue Whale topic with their children unless the latter bring it up, so they don’t try to investigate it on their own. But “do check in with your child, ask how things are going,” the foundation said, adding that parents should monitor their children’s online and social media activity for signs of the “game.”

A 21 years Old Russian Philipp Budeikin is the mind behind the deadly challenge. He was a student of Psychology who was expelled from his university. On the making of this game, he says “I want to clean this society from biological waste”. Currently he is in a Russian jail for 3 years. Who takes credit for creating the “game.” After someone joins the group, he told Saint-Petersburg.ru, they would connect over Skype. Then “I immerse him in a trance and find some things of his life and then make a decision” whether to provide instructions, he said. He said he created the game in 2013 under the name F57, combining the sound of the start of his name and the last two digits of his phone number. “Sometimes I start to think that I am doing wrong,” he told the outlet, “but inside there is a feeling that I was doing the right thing.” He added that he has bipolar personality disorder and grew up in an abusive household.

The “blue whale” name is said to come from the phenomenon of the animals intentionally stranding themselves on beaches. Originated in Russia, lawmakers have discussed using legislation to try to stop the “game.” There have also been instances of suicides or attempted suicides related to the “game,” some of which are unconfirmed, in Argentina, Brazil, Bulgaria, Chile, China, Colombia, Georgia, Italy, Kenya, Paraguay, Portugal, Saudi Arabia, Serbia, Spain, Uruguay and Venezuela.

The Blue Whale Suicide Game, also known as Blue Whale, A Sea of Whales, A Silent House and Wake me up at 4:20am is a highly dangerous and influential game targeted towards suicidal teenagers on social media sites. It tasks 'players' with completing 50 tasks the last of which results in asking them to commit suicide. Blue Whale has been responsible for over 130 teenage suicide acts in the past few years and has become widely reported upon throughout popular media sites and newspapers in recent months.

They first present “simple tasks that do not shock anyone,” the investigator said, and later introduce the more “unpleasant and scary” tasks. By that point, according to the investigator, the participants “have already fallen under the influence.”

Family members have linked at least two suicides in the United States to Blue Whale. A 15-year-old boy in San Antonio named Isaiah Gonzalez took his life on, and his parents have publicly blamed the phenomenon. “This is a warning to you and your loved ones,” one of his parents posted on Facebook. “If you have not heard of what the ‘Blue Whale Challenge’ is, please look it up and teach your kids about it.”

When a Radio Free Europe/Radio Liberty reporter posed as a 15-year-old girl on VKontakte and pretended to be interested in participating in the “game,” an apparent administrator responded, “Are you sure? There is no way back.... You can’t leave the game once you begin.” That person later told the undercover reporter not to tell anyone about the tasks and to send a photo of each completed task to the administrator. “And at the end of the game you die,” the person said.

“There are unfortunately always online sites and activities in our society that are pro suicide and increase risk, particularly for vulnerable individuals,” says Dr. Christine Moutier, chief medical officer at the American Foundation for Suicide Prevention. “This one I think is much more of a twisted version,” she adds, because “it manipulates young people into engaging in a game, and they may not understand how it is increasing their suicide risk”.

Dan Reidenberg, executive director of Suicide Awareness Voices of Education, the suicide prevention nonprofit whose guidance for the Netflix show 13 Reasons Why appears on a Netflix website, told CNN, “There is no need to panic, because this is not yet a crisis, rather a caution to alert people in advance.” But he said parents should watch for warning signs that are specific to the Blue Whale “game.” Those include drawings of blue whales or statements such as “I am a blue whale.”

In the U.S. in recent weeks, school districts, police departments and suicide prevention organizations have issued warnings and guidance.

Did reading about this game scare you as much as it scared me? What has this platform become and why all these dangerous and daring sites are available on the deep web? By default, the search engines must block access to these internet exploitations for fanatic purposes such as radicalization.

- These acts should be aggressively criminalized and prosecuted.
- Internet service providers should have a statutory duty to prevent their servers and networks from being used for such criminal activities.
- Just bring down any website that broadcasts corruption or provisions exploitation.
- We must have Cyber Police. A crime is a crime whether committed in the streets or online, and so a penalty or a punishment must be put in place for these sick maniac criminals to get charged, sentenced with zero tolerance until served.

IT Value Is In The Eye Of The Beholder

Thus bringing I personally to my first interview with Dr. Antonio Saravanos who is a Clinical Assistant Professor at DAUS, Information Systems Management at NYU, he currently coordinates the Bachelors of Science in Information Systems Management and the Bachelors of Science in Applied Data Analytics and visualization. He has been an asset to NYU since the fall of 2013.I par took my respects of discussion with Dr. Antonios in allusion to all my queries and trepidations that ascended in the course of my research and exploration.

I feel the necessity of in scripting the entire interview and missing nothing as everything Dr. Saravanos alleged was enormously significant and essential. I recorded our conversation with his consent, and typed it wholly, that procured two days. The interview lasted for a little over an hour.

Q). Cyber Security, what bell does that ring?

A). Growing field in the IT world, as we put more information online, obviously there is a greater need to insure it's secure.

Q). Are we secure?

Pause.

A). Yes! I believe to some extent we are, if you take an Intro to Computer Security course the first thing they will tell you is no system is unbreakable, it's just a matter of time and resources. So if you have enough time and resources any system can be breakable.

Q). Equifax Breach, what are your views on it? CEO Richard Smith taking his early retirement, abandoning (I feel) his company and consumers, how do you feel as a consumer towards that? Do you feel any sincerity in Equifax's acts?

A). Something went wrong otherwise the information wouldn't have been stolen. Very sad if they are resorting to those kinds of tactics, it's not easy to speculate, we shouldn't speculate, at the end of the day this is a highly sensitive information; no one can even argue why our government wasn't placing regulations in these organizations at the first place. You keep hearing me say organizations and companies, because at the end of the day they are not fully equipped and are private companies that are performing a public service, and they should be supported by the government. Occasionally when these things happen someone needs to be held accountable, and it would have been nice that he didn't resign but rather take measures and addressed the problems that have caused for this to happen.

Q). President Donald Trump's "Bill blocking online privacy", meaning at a certain fee any one can go to my phone carrier and get my "online activity record, from cookies, files to searches, everything. The bill has already passed and begins this month of October 2017. In April of 2017 Trump announced, "no longer publically release White House visitors log for the privacy of its visitors". Do you think this is fair under the constitution, the 4th and the 5th amendment to invade the privacy of the user?

A). This is America, and everything is for sale, and to some extent I don't find it necessarily wrong, what I do find wrong is that it's not transparent. So if Verizon has files or have cable connections and if they use my information they should inform me. An alternative, another service provider, perhaps that could say "Listen I don't sell your information, my service does not support any of that but it costs $10 more", and then I have a choice, that's the problem we are not informed. So right now we are not in a true market economy, which is the American way. It feels we have been hijacked by the cooperations and I think the government needs to intervene. There needs to be some form of privacy.

He (Trump) is a public official and as such people who visit him on our behalf should have a visible log, so I think that's very wrong public figures traditionally share their public calendars and so on. This is really bizarre and worrisome. Well his cookies can be accessed in the same way ours can be.

We laughed at that possibility.

Q). NSA already has our information and now it will be accessible to public? I paused there...

A). To establish National security NSA needs to have access, the problem is it's not regulated. Anyone can look at anyone's information. So let's say my neighbor is a CIA officer and I have annoyed him, he can go to his computer and say "O that's what Antonios been watching", and then go back up to me, so that would be wrong, right! There should be a mechanism where a CIA agent goes and says "listen I want to look at Antonios records because he has done this, this and this", and there is some kind of panel that reviews, and acts accordingly, right! If I am a threat then they should have excess to my data and if I am not a threat then how are they disposing my data? Are they going to delete it, how are they going to delete it? It tends to rabble.

We need an over sight, someone needs to investigate. No one cares!

I responded “at the moment no one cares”!

Q). Edward Snowden! Says “We need to encode our values not just in writing but in the structure of the internet", he further says “I don't want to live in a society that does these sorts of things, surveillance on its citizens. I don't want to live in a world where everything I do and say is recorded. My sole motive is to inform the public as to that which is done in their name and that is done against them" Edward broke the policy and procedures that he swore to comply to, and abide to, NSA is breaking the Constitution, the fourth and the fifth amendment, how would you compare and contrast these actions to being fair or unfair?

A). I think he is very naïve! The fact that now we have technology that can record everything and ever since the technology store has been developed people are using it and it’s not necessarily bad. The way it is used is bad. I don’t understand who authorized the people Snowden was working for to collect and analyze this information, right! Some elected body should have authorized it, and I am not sure if that took place, I think what needs to happen is an enquiry, to determine who is at fault, and what’s going on? Like if they were illegally obtaining this information then it was Snowden’s responsibility to act! Whether he acted appropriately, I imagine that there is some publicly elected body that should have been informed; perhaps its duty of its peers to judge what have to be done. American System is the Jury. Elective officials should intervene and ensure that everything is executed according to the laws of our country. Rather making laws to suit them, if that’s what you (he means I) are aiming at, elected bodies can resolve what ought to be done!

Q). You think there should be some kind of block to these activities prior to them been successfully uploaded online?

A). Not necessarily! As long as there is a way to rectify something and perhaps keep tabs of the offenders. Like if I have done this three times, my rights should be restricted. And if I have never done anything wrong then why do I have to go through these hurdles? So we actually need writing, we need laws and so on to determine how it is supposed to be used. To control how it is used! So let’s say someone takes a picture of someone that’s naked, do they have the right to upload it to the internet? Can they be asked to take it down? Should they have that right? So it’s more about the law, which needs to be placed to resolve these problems. And not saying the camera is evil, let's break the camera. We can't go back but we can be more responsible.

Dr. Antonios refers back to his earlier example and continues saying:

The problem is if person X's picture is uploaded. How can he intervene? How can the person Y be stopped? How to take it down? It is incorrect! There is no way for person X to appeal it. That's a problem!! I am thinking more of very open public hearings, there need to be panels, who have the whole picture, know what is going on, who then are able to judge whether they are protecting us or not. And thus make a call on behalf of us. To address this problem and find solutions.

Q). What do you think of cyber police, since all the corruption is moving to the online platform? Don't you agree when I say "We must have Cyber Police, exactly like 911, where a user who just got hacked, or had his account compromised, or cyber bullying which is very common now, even ransom threats online, could just instantly dial a number on his/her smart phone and file a complaint? And an online dispatcher could immediately trace the IP address and stop the incident, or at least isolate it. Or even track the IP address of the other party who now controls the access? No police cars no ambulance, all online, on the tip of the finger since our life has moved to this platform and so has corruption, then mind as well should the police!

A). Well not all the corruption, a portion of it. It's moving but it's also emerging.

It would be interesting to conceive of such a mechanism to support citizens, who have to deal with these situations but… ya!

Q). Have you heard of "Blue Whale"? Its inventor's motive is to "decrease biological waste", anyone depressed or suicidal plays this game and commits suicide at the end as instructed or his or her beloved will be kidnapped and killed. Since the inventor does his survey of the user and his contacts. Is NSA doing anything to end this completely? The inventor is arrested but the game is still going on...

A). No! But I hear suicide, and I hear murders taking place, so this is a police matter, not an IT matter and I am hoping the authorities are tackling it or doing something to stop it.

Q). Deep web? What is NSA doing to protect its victims?

A). So deep web is just a subset of the internet. To me this is again a problem that needs to be addressed by the government. It sounds like they are targeting individuals who have depression, so how is our society helping these individuals so that they don't have to resort these cruet games?

Q). Clay Shirky says "It used to be expensive to make things public and cheap to make them private. Now it's expensive to make things private and cheap to make them public" Do you agree?

Dr. Antonios smiles and says:

A). Well it depends, right! Certainly it's a lot easier to share information or data electronically and online and our capacity to do that has grown. Before you had telegrams that took time to arrive. Now you can send more information in less time. But then again those are my thoughts, but again there is still a possibility for privacy. Let's say I have a gold watch, I can put it in a safe and lock it. Older mediums are still there. Grab an empty book, grab a pen, write what you want to, put it in the safe, how is that more expensive? As long as you have no electronic devices in use it remains private.

Q). Is it true that they are wiretapping hotel rooms?

A). Anything that is connected to the internet can be supervised. We could be recorded right now. If they are recording it, that is fine. What I am more concerned about is how they are using it, and not abusing it?

Q). But isn't that scary? When we think we are home alone and we are not. Are we home alone?

A). I think it's only a problem if you have a private side that you don't want revealed. Right! I interrupt and ask,

Q). What about private moments?

A). There are no "True private moments", if you believe there is such a thing as 'private moments' you are probably misunderstanding the world we live in.

For next few minutes we had an unsystematic dialogue and Dr. Antonios emphasized how we are archiving our whole lives on Facebook. It can also be beneficial, to stay in touch with our family. It's a great tool that is enhancing our life. A car is polluting, but is it not nice to be able to drive around and not walk? We shouldn't get rid of the car; perhaps we can address the problem of pollution. To which I asked him if he had a Facebook account? I do have Facebook but I don't really use it, I am not into social media, I like in person communication.

Q). Last question, does NYU have Cyber Insurance?

A). I imagine they must, I can enquire!!

And on that note I turned my recorder off, exhibited my gratitude to Dr. Antonios for giving me over an hour of his time, and promised I will not misinterpret his words and that he will declaim his interview in my research paper as I intend to publish it. Dr. Antonios Saravanos is not only a man of wisdom, well informed in technology but also owns a humble personality which itself is priceless!

"As we play with these shiny new toys, how much are we trading off convenience over privacy and security?"

~~ James Lyne

An Aftermath Of Technology: My Privacy For Sale

The more I scoop into my research focus, the further I find myself jammed with this query, "how much are we trading off convenience over privacy and security?" Global Head of Security Research at Sophos Certified Instructor at SANS, Founder and Director of Helical Levity. A self-professed 'massive geek' and renowned cyber security expert, James Lyne is an information security speaker committed to educating those outside of the industry on security threats and best practice. His sagacious words instigate my analysis as I further determine the veiled data and information on cyber insecurities.

Earlier in my works I stated the Breaches, the types of Breaches, tagged along with one or two examples of the letters that are sent out to the consumers upon publication of the Breach. I also discoursed the most targeted industries such as the health care, entertainment business, and the Tech world. Not leaving behind the educational sectors, the retail companies and of course the Finance departments. I highlighted those all-inclusive foci not because I am heading to solve these larcenies and thieving or even coming up with a solution. I categorized them, to make a point!

How much has a human, a citizen, a consumer or an online along with the offline user sacrificed to these manifestations and events? A courtesy of technology! And the answer is "millions and billions of dollars" The idea behind the idealization of computation was convenience, who knew it will be exploited, misused, demoralized and become a comfort for the robber and an assaulter as well, who possibly carry out these acts of misery from the comfort of their family unit or settees, writing desks or even while sitting against the bed head board with their legs resting under a warm blanket, drinking their hot chocolate milk.

So now what do we do? How do we get away from becoming a target or an object of violence? I know the answer. And I identify a very astute and a sensible man who endorsed and validated it. Antonio Rutigliano, who since 1982, has directed and taught seminars abroad for SCPS (School of professional studies), now known as DAUS (Division of applied undergraduate studies) at NYU, on Greek and Roman civilization in Sicily; Etruscan civilization in Latium and Tuscany; He has received Gallatin's Student Choice Award as well as the SCPS Award for Outstanding Service. He is an honorary Member of Casa Dante in Florence, and he has received Italy's Gold Medal for Civic Merit from the Commune di Bitetto. His publications include Lorenzetti's Golden Mean (Peter Lang Publishing, Inc. 1992).

I had the honors of being his pupil for three of my semesters, among which I along with the other undergraduates toured with him to Italy and Spain to addition a hands on acquaintance of the Renaissance world. I emailed him asking for his words of wisdom and thoughts on cyber insecurities. And his statement on the 10th of October 2017 determined I for one the solution "Razia, as you know I deal with the inside of human mind and imagination where no cyber-attack can really get into unless we allow it!"

How considerably further self-explanatory can it be made to my readers? Use the internet for its expediencies and services; don't turn into its dependent and reliant on. Many might say "O it's easy said than done!" And to them I will say "it actually is!" I am sure Professore Rutigliano has excess to the internet, and avails it to the supreme for the benefits it delivers but then there is a borderline, a limit, and one needs to know, and must know "when to stop? When to turn off the technology? When to say, this I can handle while been offline too!"

My dear bibliophiles take control of your life and hold on to your independence. Don't give up your rights of freedom to technology; don't submit to technology, like we don't have a choice. Because we do! And only we can control and elect how much technology's interference is necessary in our day to day life.

Thus taking me to my ensuing sequence of this issue, I availed technology for my next interview since an engaged schedule and calendar arbitrated in unifying our meet-up in person.

Dr. William P. Burns, a Ph.D. Internship coordinator, at NYU, whom I could not find in my google searches in order to give attribute to his credentials and throughout life achievements, thus befits a great example of my research. Obviously Dr. Burns is a private man, and uses technology only when required, and is not published in google data hunt. He was generous and benevolent to email me back his vision and opinions on my enquiries. And I benefited the copy/paste option provided by technology, for my convenience.

Q). A little bit about yourself, any book, any article, any cause or change you voiced in your field?

A). Always an idealist--served in the Peace Corps in Africa. Loved literature and read a lot to gain an understanding of the world and a broader understanding of human nature. Loved to travel. I see both the need for Cyber Security and the dangers in government or corporate over stepping limits.

Q). Cyber Security or like I phrase it "Cyber Insecurities" which bell does that ring for you?

A). Cyber security necessary for protection of important personal information, financial and health information, for example. The lack of sufficient cyber security resulted in our elections being hacked, our political system being shaken. And in the case of numerous other hacks, Equifax been the most recent, our personal information being available to the highest bidder.

Q). Equifax Breach: Does Equifax stands to profit from their recent breach by offering a $14.95 comprehensive report for free in return of a consent form not to go ahead with the lawsuit? Management's behavior towards its consumers, CEO Richard Smith taking his early retirement, abandoning (I feel) his company and consumers, how do you feel as a consumer towards that? Do you feel any sincerity in Equifax's acts?

A). I am not sure if Equifax can recover from this recent breach since the public's confidence is shaken. Most see it as a failure of responsibility, especially not to have seen this as a possibility that needed to be addressed daily.

Q). Trump's "Bill blocking online privacy", meaning at a certain fee any one can go to my phone carrier and get my "online activity record, from cookies, files to searches, everything. The bill has already passed and begins this month of October 2017. In April of 2017 Trump announced, "no longer publically release White House visitors log for the privacy of its visitors". Do you think this is fair under the constitution, the 4th and the 5th amendment to invade the privacy of the user?

A). Trump: I don't know how Trump's policies--many of which damage the country as well as individual citizens--go unnoticed. Or at least, unchallenged. He, like many republicans, supports the interests of big business. Allowing our personal heath or financial information to be bought is only one of many examples.

Q). Edward Snowden says “We need to encode our values not just in writing but in the structure of the internet", he further says " I don't want to live in a society that does these sort of things, surveillance on its citizens. I don't want to live in a world where everything I do and say is recorded. My sole motive is to inform the public as to that which is done in their name and that is done against them" Edward broke the policy and procedures that he swore to comply to, and abide to, NSA is breaking the Constitution, the fourth and the fifth amendment, how would you compare and contrast these actions to being fair or unfair? Do you think it will be only fair to allow Edward Snowden back in the United States, give him his right of a fair hearing and let the Americans decide what ought to be done to him?

A). Snowden woke people up to the extent that their privacy was compromised. Some objected to the situation, others felt it was a necessary evil to protect them and the country from dangerous elements. I think that both the government and its citizens need to abide by the law and the constitution but, as this case shows, that doesn't happen. Justifications and rationalizations come out on both sides. I would like to see Snowden and his case treated fairly. There is still much we can learn from this.

Q). Have you watched the movie Snowden?

A). I did not see the movie.

Q). How old is "deep web"? What is NSA doing to protect its victims?

A). I know what the deep web is--I would assume it is as old as the internet, but not sure. I don't own a smart phone yet so I am not the best person to judge the pros and cons of its use.

Q). Have you heard of "Blue Whale"? It’s inventor’s motive is to “decrease biological waste", anyone depressed or suicidal plays this game and suicides at the end as instructed or his or her beloved will be kidnapped and killed. Since the inventor does his survey of the user and his contacts. Is NSA doing anything to end this completely? The inventor is arrested but the game is still going on.

A). I know what the Blue Whale games are but haven't really looked into it. I think the idea of such a thing is terrible.

Q). Any interaction with "Cyber Insecurities" of your own, and what you had to do? Your personal suggestions to what a common man like me can or should do to protect the home front?

A). My only Cyber Insecurity worries have to do with having my financial resources hacked. I am, however, concerned with Big Brother getting out of control and into the wrong hands. I think there needs to be some research in this area to understand both the good and bad of it.

Professore Rutigliano and Dr. Burns appear to be prodigious and phenomenal examples of independence and people living to the fullest without indulging their lives completely into the hands of this machinery and are definitely not giving up or submitting their privacy to technology, not yet for sure!

Child Safety And Public Morality

As I mentioned the "Blue whale game", and its side effects that have taken away lives, and continue doing so. To me that appeared way over board and sick! Resolution still lies in children been supervised by their elders or an adult, even when baby-sited by technology in the safety of one's home. When we ask our children, "What are they watching or trolling online?" we are just converting our format of supervision from when we are at a park to the online standard. As a parent we should not feel like we are being interventionist or too controlling. Is that how we feel when we ask our underage child not to leave home after dark? No! Then why do we become cognizant and mindful before hindering and becoming an obstacle when they are surfing online? Is it because we are just indolent and drained in our day to day life or are we just discerning by telling ourselves "well at least they are not outdoors"?

I have news for my adult readers and parents: our children and all the underage online users are in danger more than ever. This technology has an identical rigorous layout that our once upon a time life had. Just like our offline life, our online animation also has friends and correspondingly has foes, online has family and also subsists of strangers, comprehensive outsiders just like the ones at a store, or a park, or the ones that just passed by us in the street can be the ones and even are the ones liking or following our children on Facebook or Tweeter or Instagram and so many more mediums that we don't even have track or know trail off.

And unfortunately us, our families and our friends, the so-called adults have also become a target of making strangers, our friends online, who can see our pictures, comment on our accomplishments and triumphs, know how many children we have, what we had for lunch today? Know our whereabouts, directly from when we check-in our locations on Facebook, know how many bedrooms our home has and where is the backdoor? Which room does the garage door connect to? (because we take selfies and portraits all over the home and post them), our child's graduation ceremony, and the viewer even know off our intimate vacations that we take with our family or even unaccompanied. Everybody knows when we will be leaving for our trip, who is going with us? How long will we be gone for? What airline are we taking? And they didn't even have to ask!

So we pertained to technology, but this technology never asked us to stop using our intelligences, our wit, or to stop using our common sense, or to stop believing in our sixth sense, or to give up our privacy, or to stop demanding from our loved ones of their whereabouts while they are on their phone or desktop or laptop or an iPad, my God all the open ports and entrances for vulnerability and personal endangerment!

I understood while growing up, that only our close and intimate family and friends knew little details as such. As a matter of fact, what mom knew, dad knew half off that. Even within siblings we had a favorite with whom we shared our personal life and then there was a sibling with whom we just shared our blood relationship and the family dinner. We had friends, best friends and then the formal friends, and we chose who knew what and how much about us and our family. Then why do we have open online accounts? What happened to the traditional and safe way of living? What happened to picking up the phone and telling only the specific next door neighbor and a family member that the house will be empty because we are taking a trip? Why are we not considering our privacy and safety anymore? Is ADT alarm system our sole trustee and really enough? Or do we find it cool for the whole world to know our whole family's personal business and happenings and endeavors? Just because we post something online doesn't mean it won't affect our lives. Are we not real? Do we not exist? Than how can we be so careless about ourselves and our loved ones? Ask yourself these questions and determine your own answers. It's a one-man show, make your own decision!

A quick break with another great interview!

Edward Kirkorian who is currently a Deputy Chief Auditor covering Client Technology Solutions at BNY Mellon, in greater New York city area started his career in the audit department of Morgan Stanley after graduating in Computer Science degree, where he persevered and sustained for 22 years. He has been mastering in his field since his early twenties. From being a Programmer to an IT Auditor, Vice President, IT Audit Director, Executive Director, and currently delivering his knowledge as an adjunct Professor at NYU while maintaining a full time job, he has done it all!

While he resided in Japan he also contributed to a number of articles in Application Review for ISACA (Information Systems Audit and Control Association). 19th of October 2017, I had the privilege to sit with Mr. Kirkorian and ask him the unchanged scrupulous inquisitiveness I continue to withhold about "cyber insecurities". He speaks:

"Cyber Security is a huge topic. A term that really caught on, sort of a sexy word that everybody was easily able to label. Information Security has existed since the beginning of time, main frames were used exclusively, had many packages implemented files systems were in place, and were always aggregated. In the early days' people were not threatened by the external threats. It was mainly about the internal, making sure all controls are in place to manage one's data. As the internet evolved, the ability to get data became "a lot easier". In the late 80s and early 90s the criticality around making sure that your perimeter is safe became more important. Back then the "kid in the basement" syndrome did not exist, No tools! Then people were able to get degrees and be able to hack, just to make a point, opened up a Pandora box of insecurities. The threat was individual, a single actor trying to make a point as to how well they knew, to get around the controls that were in place. What has happened in the last few years is from "kid syndrome" to an organized crime, to trying to make a point, threat actors and now it is really about state sponsored actors. It's become a weapon of war if you will in today's day and age. A vulnerable threat, people get trained, resources are unlimited. Government is spending a lot of money in building cyber security.

I ask: Don’t you think we are 176 years behind securing?

You are correct! (Mr. Kirkorian) It all started as curiosity, nuisance, individuals wanted to prove a point, “Hey, I can break into the main frame” the kid who hacked Pentagon in the 90s, when he was caught he was very proud, and it has gotten worst.”

We spoke about Korea, the $81 Million Bangladesh Bank heist, Mr. Kirkorian said:

“It’s not a habit, but is also the idea of learning through time. Pentagon has millions of hack attempts a day! Actors are after the big fish, they don’t use the credit cards, they sell them!

Me: Equifax Breach, does Equifax stands to profit from their recent breach by offering a $14.95 comprehensive report for free in return of a consent form not to go ahead with the lawsuit? Management’s behavior towards its consumers, CEO Richard Smith taking his early retirement, abandoning (I feel) his company and consumers, how do you feel as a consumer towards that? Do you feel any sincerity in Equifax's acts?

Mr. Kirkorian: It’s interesting! I believe ultimately the guy or the gal at the top has to pay the sacrifice; it is almost like the captain of the ship. The ship goes down, the captain should go down with it, and making sure he does everything to make sure everybody else is safe. This applies to cooperations also. It is right or wrong? I don’t think so, sometimes you need a fresh pair of eyes to come in and deal with the problem, without having any intimate connection to the issue at hand. If the problem has opened under your watch, you are protective of your friends and responsibilities; a new person assesses the analysis.

I interrupted respectively: In the beginning you said a captain should sink with the ship but now you seem to be supporting him?

He simpered and countered: “But it is different, the boat has not sunk yet!” I giggled.

He continues: “The CEO reports to the board, made up of an odd number in order to swing the vote one way or the other. And it is the board that makes the decision to hire or fire a CEO. I don’t have an insight scoop but, Board has played a key role in his retirement, obviously they did not trust him.”

Mr. Kirkorian brought up Tom Hank’s movie Sully here as an example, where the committee sits, And Sullen Berger (Tom Hanks), does not give up. (based on a true event)

Has the individual made the point? A perfect example! He adds.

Moving to my next question: Trump's "Bill blocking online privacy", meaning at a certain fee any one can go to my phone carrier and get my "online activity record, from cookies, files to searches, everything. The bill has already passed and begins this month of October 2017. In April of 2017 Trump announced, "no longer publically release White House visitors log for the privacy of its visitors". Do you think this is fair under the constitution, the 4th and the 5th amendment to invade the privacy of the user?

(We laughed), Mr. Kirkorian: I don't want to get into politics, but there is a double standard at point. The reality is as we are more dependent into technology the more we are giving up our privacy. These phones can track, but today we are walking around with these phones, that are constantly tapped. How do you continue to ensure privacy when we give our rights away, when we sign up the terms and conditions? It's the little guy, you and me who pay the price. If you didn't do anything wrong, then don't worry about it! There are cameras in the city, there is no privacy!

Mr. Kirkorian has watched the movie Snowden.

I read: Edward Snowden says "We need to encode our values not just in writing but in the structure of the internet", he further says "I don't want to live in a society that does these sorts of things, surveillance on its citizens. I don't want to live in a world where everything I do and say is recorded. My sole motive is to inform the public as to that which is done in their name and that is done against them" Edward broke the policy and procedures that he swore to comply to and abide to, NSA is breaking the Constitution, the fourth and the fifth amendment, how would you compare and contrast these actions to being fair or unfair? Do you think it will be only fair to allow Edward Snowden back in the United States, give him his right of a fair hearing and let the Americans decide what to be done to him?

Mr. Kirkorian: A double edge sword. Did he do wrong? Yes! Because it put the U.S. at a great competitive disadvantage, preaching and asking to be a whistle blower, yes he did the right thing! Government is breaking their own law that they are supposed to abide to, Government is not about the law, and it needs to operate accordingly, it exposed the U.S. mischiefs, putting the U.S. at stake. It created a whole new way of looking at things. A vicious circle, U.S. is doing it to China; China is doing it to the U.S., so on and so forth…

What about the citizens? I asked.

It is absolutely true! Theoretically the device is listening to us right now! No warrants, no permissions. Do I like it? I don't like it, but it is the reality. He continues, "I was personally disappointed when he wasn't pardoned by President Obama, because the flip side of it is we encourage the people "when you see something, you say something" double standard… I would have pardoned him if I was the President! The right to courts until proven guilty…"

Me: Do we have cyber police?

That is an interesting term, how did you come up with it? There is a number, F.B.I does have a branch you can call, but they have limited resources and are not too public. They will probably say "no" but they will take your number, and track the area, and the activity pattern, not different from burglary at home, the police comes, does nothing but makes a report, then trace the pattern! People back then wore masks and attacked; now they do it online. This country is way behind inventing smart chip.

Mr. Kirkorian emphasized: "skimmers, you heard of them? Crooks have made a device to record your card. They are able to register your card, your cvs number, your pin, everything. Do not use your debit card at no mom and pop delis; go to the branch, only during work hours, or from the Bank ATM machine. Never ever, go to an ATM in the corner. Chances of your bank branch are a lot less than the delis. Bank is responsible, delis are not!

I asked Mr. Kirkorian about the deep and the dark web, he actually explained me how they worked.

"Dark web is not mapped, the streets, the servers are not mapped, and you have to be invited to join it. Deep web is searchable; anything you can find in searches is "deep web", with dark web you need to know where to go!"

"Blue whale, have you heard about it? I asked.

"Yes" Mr. Kirkorian responded, how is this related to cyber security?

I wonder if the government knows all this, I held….

Mr. Kirkorian: You cannot have it both ways, you don't want the government to track you, yet you want them to know of this. It's like a catch 22. I think reality is it's a completely different problem; it's manipulating depressed people, just like cannibalism. A percentage only likes it. Be careful what you ask for!" (We chortled) while he continued with a story of his father. "My father saw a commercial on TV and bought something, now he couldn't call them back, and in anger and annoyance he says to me, “how come the government is not shutting it down?” (I laughed hard) The government has millions of other things to worry about; you think they care about your 100 dollar? You should be an educated consumer, who should not buy things like that on TV. There is no prevent control, no process in place to prevent scammers as long as they are abiding to the seller agreement, they can advertise and sell whatever they want, and they cannot be stopped!”

This is where I felt gratified and asked my final question that I developed while hearing Mr. Kirkorian’s assertions.

Do you think you agree when I say “the government cannot catchup”?

Mr. Kirkorian: corruption is too fast for them!

I asked for his overview and he returned:

“There is always a way around it, nothing is full proof, cyber security has gone expediential in the overall last few years, as a tool to steal, a ciaos creator.

- Make sure you have strong passwords.
- Make sure you always take care of your finances from a bank branch, hopefully from the comfort of your home.
- Shut it off when you are not using it! (he points at his phone)
- It takes two minutes to boot computers, turn them off when you are not using them, they cannot be located if turned off!

I turned off the recorder, could not thank him enough for his time that he availed from a long day of work, and not to mention his family that be waits at home.

More addition to our solutions is added from my conversation with Mr. Kirkorian. “Turn it off!” It can be that simple, and as a matter of fact that was exactly what Shamla Naidoo, the information security executive with more than 25 years of experience also uttered at the cyber security conference, “Power it off!”

Women Leaders In Cyber Security:

Emerging technologies present intriguing challenges and exciting opportunities that require innovative thinking and diverse perspectives. I had the privilege to attend the Women Leaders in Cyber Security on the 3rd of October 2017, and I have cultured an interdisciplinary approach to exploring critical issues, such as:

- Security Vulnerability Management
- Artificial Intelligence
- Block chain Technologies
- The Internet of Everything
- Building a Global Cyber Security Strategy and Team

A stellar line-up of leading women experts in law, technology, business, and policy, some of the famous names were Lisa Monaco who has served as Assistant to the President Barrack Obama for Homeland Security and counterterrorism, Shamla Naidoo an accomplished information security executive with more than 25 years of experience, Anne M.Roest, appointed as the eight commissioner of the New York city Department of information Technology and Telecommunications by Mayor Bill de Blasio in May 2014, Susan Poole, a Block chain advisor and consultant, Tarah Wheeler (MS,CSM, CSD, CISSP), also an author of bestselling book “Women In Tech” and many more joined for a day of fireside chats and panel discussions on these important topics. Audience included women and men from business, government, and academia.

Many queries that enthused, within me in the course of writing my research paper were answered by the connoisseurs, consequently giving me the self-assurance to preserve and carry on. Since we had the opportunity to ask the panel questions I stood up and got in the queue, upon my turn I inquired: “What do you think of cyber police, since all the corruption is moving to the online platform? Don't you agree when I say “We must have Cyber Police, exactly like 911, where a user who just got hacked, or had his account compromised, or cyber bullying which is very common now, even ransom threats online, could just instantly dial a number on his smart phone and file a complaint? And an online dispatcher could immediately trace the IP address and stop the incident, or at least isolate it. Or even track the IP address of the other party who now controls the excess?”

Shamla Naidoo instantaneously responded:” What a phenomenal idea! I would say, write that as your thesis statement. And it would be wonderful if we had something like that.” I sensed invigorated, I felt enhanced, and looked-for the next panel so I could ask them my added query that’s been tilting my cognizance. As the masterminds on stage spoke about cyber-attacks and giving awareness to the people, my question to them was “wouldn’t it be rational to just drop in a free firewall or a windows defender software cd, with a brand new purchase of technology, so that the user has the protection his or her computer needs?” Rinki Sethi a Palo Alto Networks Senior Director of Security Operations and Strategy took my query and believed “I think that’s something we should be able to offer our consumers at no cost, and to save money in the long run.”

I had the rectitude to shake hands with Miss Lisa Monaco and very hastily put my query in front of her as she was walking out of the hall. I opened my diary page and read out loud:

The President Donald Trump's "Bill blocking online privacy", meaning at a certain fee any one can go to my phone carrier and get my online activity record, from cookies, files to searches, everything. The bill has already passed and begins this month of October 2017. In April of 2017 Trump announced, "no longer publically release White House visitors log for the privacy of its visitors". Do you think this is fair under the constitution, the 4th and the 5th amendment to invade the privacy of the user? and Miss Monaco responded, “absolutely not! But then again anything is possible under Trump’s administration”.

"Four be the things I am wiser to know:

Idleness, sorrow, a friend, and a foe.
Four be the things I'd been better without:
Love, curiosity, freckles, and doubt.
Three be the things I shall never attain:
Envy, content, and sufficient champagne.
Three be the things I shall have till I die:
Laughter and hope and a sock in the eye."

~~ Dorothy Parker

An eloquent quote spoken by Dorothy Parker who was born on August 22, 1893 and died on June 7, 1967, an American poet, short story writer, critic, and satirist, best known for her wit, wisecracks and eye for 20th century urban foibles, she was also called a "True New Yorker". Women who made it both to the historical database and non-historical, are remembered for their courage that they believed in voicing regardless of the consequences has always intrigued me. I look up to them in my down time and get up because of them. What is it that a man can do and a woman cannot? It is my only curiosity in this moment, and at times it is clearer!

My parents share same grandparents, as they are first cousins, and they take pride in their elders and the lives they lived. Mom tells us that their grandma worked in the family-owned fields during the day along with many other woman of the village. And on a one regular field day she went into labor, no doctors or nurses around, just the women working in the field. All of the females circled around her with their backs towards her to give her privacy, whereas the two wiser and bolder women helped her in the process of delivering the baby boy. A perfectly healthy baby boy, whom they loaded in the same basket that was used to carry crops for the day, great grandma rested in the open field while the women sanitized her as much as they possibly could do, and at the end of the day great grandma walked home with the basket on her head, and as she reached home, and great grandpa reached out to take the basket off her head, she whispered "carefully, there's a baby in there!"

Who were these women? Were they made out of metal? Did they not fear fear? Did they not ache pain? What motivated them to work shoulder to shoulder along with the men, not to mention they covered their bodies in these long drapes, picked up crops, bared children, took care of their elders, responded tenderly towards the needs of their husbands while on the clock 24/7. When did this trend change? When did the woman decide to be either a home maker or a working woman? Who was behind the concept that the woman either stays home or goes to work? And who tagged the women that were active employees to be looked at as a self-independent, selfish or in laymen terms "does as she pleases"?

Because when I look back at the "Herstory" rather than the "History" women always played a key role in the strengthening of family, wealth, protecting the values and assets while providing stability, multiplied whatever the man gave her. Controlled and managed her family and children in the absence of the man, and made sure everyone is safe. Then when did women become so impassive and carefree towards their loved ones? And what makes them think that in the today's era they don't need to administer their family and children, just because they are physically present at home and seemingly only engaged in computers or on their phones, does not mean they are protected. Are the mothers and the female head holders of the families not aware of all the ridiculous excess this online platform provides? If not, then it is now time to give them the "Cyber Hygiene" awareness and make them digitally literate so that they can protect their families and loved ones from the online threats and exploitations.

Razia al-Din or Razia Sultana (1205-1240) was one of the rulers of the Delhi Sultanate. She was the first and last Muslim lady to rule Delhi. She was said to be a brave, kind and just person. She ascended the throne in 1236 A.D. But the nobles who did not like to be ruled by Razia soon killed her in a war on 14th October 1240 at the age of 35; she was a member of the Mamluk dynasty. Razia was an efficient ruler and possessed all the qualities of a monarch. Women are known for their strength and a durable charisma, and this world of Tech seems unsecure and frail without them. This Land of Integers needs women, it needs a motherly touch, it is unsecure and is like a homeless child that now seeks a roof over its head, and that my dear readers a father, a man can never provide. As he is known to build houses, but it has always been a woman who made that house safe and feel like home!

Prophet Mohammed says "man and woman are equal" let's not change and modify that. Why aren't there women in the "land of integers"? Let's not accept that the women don't belong in this domain or that they could not learn the language of the digits. Because if the woman can cut crops, work under the sun till dawn, use swords and shields, ride horses then one better believe that she can work her way in front of the computer screen, or inside the network, or behind a clean code that can create a safer software too. Prophet Mohammed's first wife was a business woman, owned a trade, a divorcee thus far independent, yet women still make up only a quarter of the Tech industry workforce in the U.S. according to the Bureau of Labor Statistics, and we need to play catch-up to fill them all.

Alan J. Zausner a CIO at industrial Evolution whom I randomly remembered seeing at the Cyber Security Conference on the 16th of October 2017, has served for over 25 years and continues his efforts for the Privacy of Domestic and International Consumer Interactive Systems domains and supporting IT infrastructure. I met him again in the "Homeland Security in the Twenty-First Century conference held at Lipton Hall on November 13th 2017. I recognized him instantly, and he remembered me as well through my questions that I asked from the panel, he said "what are you doing here?" Thus our conversation began and continued as we walked through the lobby to check-in, sharing our thoughts and concerns about cyber insecurities, we settled down.

The conference began with Jeh Johnson a former Secretary of Homeland Security and Lisa Monaco a former Homeland Security Advisor to President Barack Obama and current distinguished Senior Fellow at CLS (The Center on Law and Security). Both the seniors respective of their life practices emphasized that the vulnerability is expanding rapidly to the surfaces and that we have to educate the communities. That we are not as much as we should be concerned about cyber security. Cyber space is a new issue and it is going to get worse before it is going to get better. It should be held as a National Security issue. They further said that the best defense is a good offense. Educate the user!

Mr. Jeh looked at the attendees and asked "how many of you would know how to recognize a phishing attack?" Towards the conclusion I was able to shake hands and briefly exchange dialogues with both of them, and requested their interventions in my thesis. I believe, due to privacy purposes Mr. Jeh only motivated my work as I write my paper, and asked me to refer to his secretary for his contact information, as he was getting late for his train. I accepted that as a sign, and moved to Miss. Monaco, as she remembered me from the last conference and suggested that I could find her contact information on the NYU website, and definitely email her.

Mr. Alan and I continued our conversation after the conference and I was successfully able to get his contact information as I mentioned to him about my research and that with his consent I would love to add his vision in my work. He laughed and granted me the permission.

Upon my first spare moment I emailed him with my only concern at the moment and below I benefit from the copy/paste option provided by technology.

I wrote to Mr. Alan: “I am very curious to know how do you look at the woman’s involvement in the cyber world and why do you think it took this long for the women to join the “Land of Integers” as I call it? Do you think women can play a role in making Cyber Space secure or do you think “nah, it’s the man’s zone, stay out of it?” He responded: “While the question you pose is a deep one involving cultural moirés with very little to do, in my opinion with the complexity of the subject. I strongly believe it has nothing to do with the brains ability to understand the intellectual composition of the subject. Instead women are limited in the cultural groundings of a male dominated world which shunts them some time in getting through. I know I am an outlier in my blindness of color, racial, ethnic and gender perceptions of people. With that said I appreciate the spatial thinking that most women possess which as you know is one of the traits necessary in designing and administrating cyber security systems. I feel it is up to the individual to make a compelling case, regardless of whether it is a women or male, for why they should be offered a seat at the table. Unfortunately, as amplified by the recent harassment and abusive discloses within the media gist, it is one more barrier that a woman has to overcome. That is a difficult barrier to transcend and I hope the public discussion now might ameliorate its stifling impact for so many women.”

Mr. Alan continued “I always say to a young woman starting out is to be you… Don’t try to be overly aggressive or very flirty. Don’t try to be one of the guys, cause you’re not... Show your own power and competence and gender barriers will come down and you will be listened to for what you know and don’t know.”

Further in the email he wrote “for a musical break from your thesis work, have a look from this clip from “My Fair Lady” and the song “Why Can’t a Woman Be More like a Man” I always felt it was so telling on so many levels!” I enjoyed watching the song and attached the link in the bibliography for my dear readers to pleasure from as well.

I also emailed Miss. Monaco that follows below:

Good Evening Ms. Monaco,

Hope all is well. I attended your event on November 13th 0f 2017 at Lipton Hall and we exchanged few dialogues briefly. My name is Razia Sultana, I am 4 weeks away from becoming a junior at SCPS NYU (DAUS) campus majoring in Information Systems Management and my area of concentration is Cyber Insecurities, as I call it. I am a Project Co-Coordinator in the IT Department of NYU (campus anonymous). I have attended two other conferences of the same domain, exchanged my ideas with the panel respectively and was able to get their contact information.

From Information Technology & Telecommunications to authors and Speakers, for some reason they love my ideas on the floors of the conference room, but as I contact them they connect me to their supervisors. Who ask me to write a detailed email of exactly what my idea is, or highlight my questions while they respond me with only a "yes" or a "no". But that is not what I want!

I want to be put through, to a department who can listen to me not because they are getting paid in doing so, but because they also have the same sense of mission as I do, and I connected with you the instant you said " I miss having a sense of mission" in the conference in October. Not for publicity purposes, but to actually make this online platform that me, you, us, our beloved, our children, our friends along with our foes have moved to.

As I research and write my thesis I happen to mention the social media as the weakest point of privacy invasion, looking at the history the greatest warriors, the kings, the rulers who had their downfall in record, was due to a betrayal, a deceit, a deception that was single handedly caused and led by one of their own, the one they trusted, the one who was the closest to them, possibly living in the same castle. Not an outsider!

As the U.S. continues to introduce the latest, the shiniest the finest, the thinnest, the lightest of Technology not to mention the upgrades, the consumer has absolutely very little knowledge of what that technology in hand is capable off, and how the consumer’s privacy is online rather in line, as once upon a time. An American not completely but definitely is back to the Stone Age when it comes to having the knowledge of this "era's inventions".

I strongly believe that United States strength does not lie in being the "super power", based on its weapons of mass destruction, military, self-defense border lines anymore, as all of that now can be "shut down" as soon as the system gets broken into. The "online world" does not necessitate borders, needs no visas, or any particular government's permission to enter the country. All the users of technology can travel around the world through their iPhones, iPads, desktops, laptops, Androids whatever the medium be on the tips of their fingers.

Thus I believe teaching the consumers, the end users who are unaware of what this seemingly very safe medium is capable off, calls for an urgency. My research does not talk about NSA, NIST, CIA, FDA or any government schemes, as I believe they are doing a wonderful job. My concern is right here, at home, my children, my friends, my parents, my privacy, our privacy as a nation. And I am becoming a firm believer in giving a key knowledge to the users of this technology at home front, as the opponent will use that as a weak point to attack. If the Americans don't have the knowledge to protect their families, how can we imagine America as a "safe land" anymore?

All seem to be giving and pinpointing at the safety of the State, the Government from potential threats. Why attack physically, when the opponent can corrupt, weaken and destroy a nation from the privacy of his/her home, as long as an internet whether be a wireless connection, is available?

I don't intend to only get your views in this matter, as then I will be no different than those speakers who give a great speech, take pictures, make it to the media, and continue the same process on upcoming presentations. I want to be heard, as I know I can make a difference. I am the people, I am the end user, I am not familiar with what the technology is capable off, and I am very scared! As I feel been under an attack via online, where I have absolutely no protection and security or even awareness. It is as equally severe and threating as witnessing and been a victim of the "world war".

I am sure there are tools in place, but do I know of them? Does any American who has nothing to do with Technology whether be through school or work knows of those tools?

Knowledge is power and it is time every citizen has that power!

Respectively,

Razia

I still wait for Miss. Monaco’s response….

The time has gone by forever when woman can be regarded as a mere ornament, and can be shut out of active life. She is not a doll or a toy. She has her duties and responsibilities. She is not born merely to be married as soon as possible, and from girlhood to consider her wedding as the goal of her life. Thousands of young women will never be married, and yet their life need not be a failure though their fingers are never circled by a wedding-ring. Women have immortal souls. Their heaven does not depend upon being linked with a husband. Every young girl should set for her great central aim in life, to be a woman, a true, noble, pure, holy woman, to seek ever the highest things. That should be her aim, — to realize in her character all the possibilities of her womanhood. Accept your duty, and do it. Accept your responsibility, and meet it. Be true in every relation you are called to fill. Be brave enough to be loyal always to your womanhood. Train your mind to think. Set your ideal before you, — rich, beautiful womanhood, — and bend all your energy to reach it."

~~ J.R. Miller, Girls: Faults and Ideals, 1892

I found an article published on CNBC by Mark Koba, it read:

"Male executives may have to swallow their pride when it comes to which of the sexes do a better job at running a company, according to a recent study. A report on global businesses called "Women Matter" by McKinsey & Company, suggests that the firms where women are most strongly represented at board or top management levels are also the companies that perform best in terms of growth and earnings. The study concludes that "women provide a source of high quality talent in a competitive market and have a positive impact on organizational and financial performance. "Women bring forward a passion that men may not have," says Leslie Wilkins, CEO of isABelt Ltd., a fashion-accessory firm that sells products in more than 1,000 stores.

"That passion is what enables us to not only start and run a business, but to balance it between home and work," explains Wilkins, who started her company five years ago. "I think that's what makes our business run as well or better than if a man did it."

Jacqueline Corbelli, CEO of the interactive television advertising firm Brightline, says the distinctions between male and female executives couldn't be more obvious.

"Women bring two things to the boardroom that some men do not," says Corbelli, who had a 15-year career in the financial services industry before launching Brightline in 2003.

"Women are good collaborators; we do it naturally," Corbelli says. "Even the most competitive women know how to create and motivate teams. Another thing I see is that working women who are mothers know how to get things done and move on to the next task." It's not just women who see contrasts in boardrooms!

"I think women are better execs in that they aren't so afraid to speak up," says Bretton Holmes, who head up his own media relations firm in Austin, Texas. "Women tend to shoot more from the hip, I've found, while guys wait sometimes and the opportunity to say something may pass."

As can be expected, there are those who contend any differences between men and women are just style over substance.

"I think its personalities more than genders that bring something to the power table," says Charley Polachi, a partner and co-founder of the executive search firm Polachi. "Women may be more sensitive to subtleties, but I really don't see all that much of a difference on how they use power."

But just getting a place at the executive table has not been easy for women. While they make up 40% of the global workforce, they represent less than 14% of the corporate executives at top companies, according to a recent report by the research group, Catalyst.

A 2010 report conducted by Mercer says that 71% of the all global companies do not have a clearly defined strategy or philosophy for the development of women into leadership roles. "Women usually fall into three camps," says Xavier, who has worked exclusively with Fortune 500 executives. "There are those who go along for the ride to be accepted, those who become 'one of the boys' and those who are just themselves. The last group is the ones who do things differently and it shows up in better results."

Rochester Institute of Technology posted an article by Scott Bureau saying: Cyber security is a burgeoning area of computing, where the demand for trained professionals is much greater than the supply. However, just like in many other areas of computing, women are alarmingly underrepresented in this male-dominated field.

While at the 2015 Women in Cyber security conference in Atlanta, RIT’s attendees heard keynote addresses from women working at big-name organizations, including Facebook, the Department of Homeland Security and Microsoft. Jennifer Henley, director of security operations at Facebook, even met personally with RIT students to give advice about working in cyber security.

“Jennifer talked about the importance of every woman in cyber security having an ally in their work and efforts,” said Morgan Keiser, a first-year computing security major from Waterford, Pa. “Women have every bit as much to contribute to forwarding the future of security as men do and we should have a natural collaboration.”

Shelley Westman is the Vice President of Operations and Strategic Integration Initiatives at IBM Security and I found her article posted on Security Intelligence, it read:

“The cyber security industry is in an arms race, and the top resource in demand is talent. Experts predict a shortage of 1.5 million security positions by 2020. In the face of an increasingly large and talented network of cybercriminals on the Dark Web — with more and more joining every day — this is a shortage that we as an industry can’t afford.

Security has evolved into a core issue for business and society, costing the global economy $445 billion annually. No longer are just current computer scientists and researchers being enlisted to fight expanding cybercrime rings. The next generation of security workers will have to step in, and they need to possess a broad set of skills and fill roles ranging from product designers to risk consultants and policymakers.

To truly defend against attackers, our industry needs to equip itself with the best and brightest. Recruiting and fostering more women in security presents an enormous opportunity to fill the growing talent gap, as well as bring to bear a more diverse set of skills to fight against new threats.

As security professionals, we must take an active part in driving this change. New York University’s Symposium on Women in Cyber security is aimed at educating, training and encouraging more women to join the security workforce. By teaming up with such an esteemed academic institution, we’re focused on building awareness of the opportunities that exist in security for women of all backgrounds: from high schoolers deciding on a career path to seasoned professionals in other industries who have acumen that can be put to use in security.

Partnering with educators to attract a diverse workforce is critical, but the collaboration to solve the skills gap can’t end there. Security education, such as advanced training on technologies and strategies to fight modern day threats, must evolve to keep up with the ever accelerating pace of attackers.

To that end, IBM recently launched new university programs with the Rochester Institute of Technology and Temasek Polytechnic in Singapore to prepare students for careers in security through hands on training with IBM tools in new, cutting edge security research and operations centers. Working with advanced technologies such as analytics and threat intelligence will help burgeoning security professionals learn how to think on even greater levels than the most successful cybercriminals. They'll also prepare to collect and analyze data on emerging global attacks to uncover and stop them before they inflict damage.

Attracting a more diverse workforce and equipping educators with modern training and tools are two key stepping stones to overcome the security skills gap that is crippling the industry in the fight against cybercrime. All security providers must be committed to helping overcome these challenges and build the cyber security workforce of the future."

Concluding the article….

This article is literally begging for woman's involvement in the Tech world, however explaining just in what way the women can make a potential difference by their presence in this domain that is full of insecurities, our children play in this acreage, as we the adults take a walk…

"Science is organized knowledge. Wisdom is organized life."

~~ Will Durant,

Internet Is The Modern Era

William James "Will" Durant (November 5, 1885 – November 7, 1981) was an American writer, historian, and philosopher and his axiom astounded me. How well said is that? Science is organized knowledge and wisdom is organized life. It is time to get our online lives organized. It is time to get all the women, mothers, sisters, daughters, wives capable or disable to roll their sleeves and step up, not for money, not for fame but to save our children, our families, our loved ones and to take control of our lives and our home fronts. Do what we are known for, what we do best in, protect our children, secure our home fronts and the best part is, this time we will not take the back seat as we take charge of our families and loved ones, but in doing so as a matter of fact we will modernize ourselves while remaining updated with this time of technology. It will put us in the front line of the battle field, the field which now is the cyber space and cyber insecurity transpires at this moment, as I write, as you read!

I google searched my father Shaukat Hussain, to see if I could find any information about him online, and it was an unsuccessful search, as no results were found for that forename who is my father. A self-made man, remains self-employed, did his first successful business transaction at the age of 15, in the early 1960s when there was no technical interference, and his only tool was his "courage" with which he remains armed till today. He dislikes his touch screen phone, as it does not obey him, and does its own thing leaving him stranded and irritated. Same results were found when I googled my mother. Whereas on the contrary my own born, the instant I googled his name, on the screen popped up his Instagram, tweeter and YouTube account activities. I rang him up and as our conversation continued on a casual note I started muttering his comments that I could read on my phone screen. He asks, "What are you saying?" I responded in an ordinary tone of voice, "oh, just reading your comments online."

Please excuse his French as he utters, "Shit, where are you? Which account?" I responded, "Oh I have a famous son, he is all over the internet, which of your accounts comments would you like for me to read?" And I started picking out random comments from his different accounts as I read them out loud to him. He reacted and asked "where are you online?" And I said to him in my lingo "bubuu I can read all your activity thread by thread and all I had to do was to enter your name on google search, and these links popped up. Didn't even have to make an account to find your activity online." That instant he went on the settings of the social Medias he had an account in, and made them all private, and then asked me, "okay go check now" and I couldn't find anything as it prompted me with the message that this is a private user, message them or send them a friend request.

I feel like that moment was a wakeup call for him. Children in the olden times, said things in their teenage years, that had no record, today they write and post how they feel, what they do, and forget about it while it remains like a record in the womb of the Google engine. I was so happy, when I saw him update his settings, and he expressed to me that," He could swear his settings were private" little does the user know that after the upgrades many of our personalized settings go back to the factory settings by default and unless we update our settings again, we are like an open port!

Pick up the phone and call your loved ones, ask them if their online accounts are private or intentionally open to the market? Tell them you love them very much and want them to be safe, tell them what you know now, and tell them that cyber space is not really as safe and simple as it looks and sounds. Tell them, because you would if your loved one's front door or a room window was cracked, and could be possibly opened from the outside, you would have them fix it because you would not want them to get robbed and because you care…

"No thief, however skillful, can rob one of knowledge, and that is why knowledge is the best and safest treasure to acquire."

~~ L. Frank Baum, The Lost Princess of Oz

NYU Tandon School of Engineering offers Masters in "Cyber Security", and thus I found it intriguing to attend its 9th Cyber Security Lecture on November 16th of 2017. As I sat in the auditorium waiting for the lecture to begin, I could see myself in this campus while pursuing my learning in "Cyber Insecurities" as it is seemingly becoming even more personal and a region of my concentration.

Edward Amoroso a distinguished Research Professor, in NYU Center for Cybersecurity holds ten patents in the area of cyber security and media technology. His work has been highlighted on CNN, *The New York Times*, and *The Wall Street Journal*. He enthused all the audiences with his passion and strength of mind and I felt that as much as his work needs to be looked into, unfortunately it is not. He even wrote to the current Trump Administration in power, nevertheless received no response.

I had to ask him roughly how he felt about having cyber police, and I did when it was the audience's time to question. The crowd giggled and someone from the back chuckled "011 is taken, you will have to try some other code", to which I responded "let's come up with a help line together". This Lecture was open to public and I could sincerely feel the inattentiveness, and all talk but no action. Thus I approached Mr. Amoroso during the break time, and he gave me his contact card and said "email me, I want to help you". In the email dialog that we traded Mr. Amoroso signaled saddened and discouraged, as he mentioned to me that he "filmed 16 weeks' worth of 180 lectures for Coursera that are 100% free to anyone with a computer. Very few interested citizens will even bother to log on and watch. The result is that most citizens are ignorant to cyber security and mostly don't even care."

And furtherly said that if I hoped to inspire consumers and citizens by providing great access to cyber security information, then he shares my passion, but it is a limited and highly distracted crowd. He wrote he didn't mean to be negative and to stay inspired and keep working on what I believe in, but empowering and helping citizens with cyber security only works if they are willing to participate - and most today sadly are not.

I looked up Mr. Amoroso online and found a lot of his effort, whether be in Coursera, his books or his lectures, and it felt only mandatory to add his work in my bibliography, so my readers could access it and make use of it.

Solution

"Prevention is better than cure"

~~ Avicenna

I am an end user, and I know how it feels to be intimidated towards just downloading an app or having the shiny toy, just because the other friend or a class mate got it or in plain "everyone is getting it so I will too". The extortion is too powerful. But if we don't deliver the information we have and make it common for the consumer's ears to hear then somewhere in our souls we will remain conscious. As we never passed the awareness that could have, might have saved someone's information from leaking.

Mr. Amoroso's 16 weeks' worth effort went unrealized because it was not advertised. You see how Apple commercials its upgraded version of iPhone months before the delivery and then all want to hunt for it, know off it and even have it? That's the temptation and dedication that our prevention and security products are missing. If we run an advertisement about "cyber insecurities" that knowing these facts will save the consumers information from going in the wrong hands then we will make the viewer alarmed and make him/her think that "hmm I should read or find more on this" or "omg, I didn't even know this was happening!"

I know this will get the consumers attention! A common man is not interested in reading or listening to fat documentaries or boring lengthy articles. But a 2 minute or a thirty second commercial can do magic. I don't believe in pills, but Celebrity's like Oz make me want to buy Garcinia Cambogia, the advanced weight management formula. Let's say I successfully cut through the enticement of not buying it, but then this product will run commercials back to back on Television, radio, even while I am online , a slide will pop up on the side of the screen telling me of a special: "Buy now and get your free supply for 60 days, with no money down, just pay $4.99 for shipping and handling and get your free trial shipped out to you today, if you don't like the product just call us back and we will cancel your subscription, and you keep the remaining supply." Heck ya, I will pay only $4.99 to try out this product for 2 months, I mean it is not like I am paying the full price. What's the worst that will happen? I won't lose any weight, but at least I will not be curious anymore when I see this commercial popup!

Did you also feel the appeal as you read through this commercial? Did a fast and a powerful voice inside you read this ad like it would sound on the radio or on TV? That's the excitement our “awareness of cyber insecurities” education is missing.

If I was to be made a CEO even for 48 hours and asked to “give the awareness on cyber insecurities to the common end user at home your way”, the following is what I would do:

1) Use the media center as my first source of educating the residents of the “cyber space”, the environment in which they now live.

   i) Run commercials of the software’s created for the protection of the user and how a consumer could prevent his information from leaking and account from being hacked.

   ii) Have the famous celebrities involved in giving knowledge to the end user. I don’t watch TV but if I hear that George Clooney will be on abc channel at 9:pm, Thursday night talking about the recent malware attacks and how we can protect ourselves in the future, you better believe I will take an early release from my class so that I don’t miss his presentation.

   iii) Have the famous artists talk about the child trafficking that takes place in the dark web, along with the killing and murders that occur live while spectators watch it and relish it, not only will the artists be working towards their humanitarian efforts, but will also be educating their fans on a very important matter.

   iv) The veteran celebrities, politicians, singers, authors and even the famous poets, have them sit on the panels and discuss these vast new world inventions while comparing and contrasting their lives and how they once lived. These panel discussions are very boring but if it is Clint Eastwood, Alfredo James Pacino, Arnold Schwarzenegger, Julia Roberts, George Clooney, Sylvester Stallone, Harrison Ford, Mel Gibson, Richard Gere, Sandra Bullock and Meryl Streep then it will be a discussion worth watching, and nobody will miss this debate/discussion. (I named veterans as we all love them but not many are active artists anymore but still hold their impact on their fans, we will listen to what they will have to say).

   v) Run commercials that say something like “are you feeling threatened online? Are you been bullied constantly on social media? Has your account been hacked? Do you think your email address has been compromised? If so, call 1800-WEBCOPS or 1800-932-2677 right now, web cops are available 24/7 to help, call now! Or go to our website @ www.webcops.nypd.com (address by State until a global address is implemented) and get the help you need!

vi) Use subways, HRA buildings, doctor’s offices, educational institutes and any facility where an end-user goes and expects a wait period, these slides or discussions should be the topic of education on those big screens where the end-user’s eyes rest as they wait.

2) “Cyber Police” on call available online 24/7.

i) Just like 911 there must be a helpline to protect the end user whose account just got hacked or compromised, or a user who is being bullied online by a random user, an ID theft and stolen passwords case scenarios.

ii) The cyber tech should be trained to trace the activity by locating the callers IP address and take remote control over that IP address thus successfully isolating the IP address and returning the account back to its original owner. All the corruption that takes place in the streets now occurs in the cyber space as well than why is there no option under the term “cyber police” inserted in every social media?

iii) No police cars, ambulances or fire trucks needed, as all this security will be provided by trouble shooting a situation which will get solved by the Tech geeks that are on call.

iv) Facebook, Twitter, Instagram so many other social mediums are under surveillance already by the administrators, why not add a helpline in those soft wares as well? Where one that is been harassed could just message the authorities who are sitting just a click away, and all they have to do is pop up a warning window on the harasser’s account. He/she will back off!

v) Crime is a crime whether it transpires in person or online. The lawbreakers must be arrested and sentenced according to their acts of violence. Zero tolerance attitude must be put in online, if we don’t put a stop to these acts now than before the authorities know it, there will be no crimes happening in the streets as they will all move to the online platform, since the crooks know they have less chances of getting caught and because there are no laws in place to penalize them.

3) “Good touch bad touch”, is a one-time class of awareness given to all the 5th graders towards

the end of the year, as the students prepare to enter the Middle School. Teachers teach them in simple words on behalf of their Parents; even though it is a voluntary teaching and parents have a choice to opt out their children from attending this class, as a written consent is send home prior to the scheduled class. But many parents appreciate their teachers giving the birds and bees' speech, as it saves them the awkwardness.

   i) Teachings on "Cyber Insecurities" must be made a mandatory class from the 5th grade onwards. Students must pass it to go to the next grade. Department of Education should pass a bill that adds this class starting from the next school year of 2018.
   ii) In doing so we are educating our children who are our tomorrow, about how to protect themselves from online bullying, how to prevent talking to the strangers, a step by step guide that teaches how to manage their privacy, stay safe and secure.
   iii) "If you see something, you say something", give our children the confidence and trust where they can share their online lives and events they face while surfing to their parent, an elder, a teacher or anyone who supervises them, unfortunately Technology is babysitting the children while mom and dad are at work, children must be made aware of the cyber space dangers and how to avoid them.

4) A phone carrier company should be introduced that does not support the Trumps, bill.
   i) In doing so like Dr. Antonios Saravanos said the consumer will have a choice, the phone carrier company should offer a complete private package, at the rate of few dollars more than the current carriers and in return provides the user a peace of mind that their online activity will remain secluded and will not be sold to anyone unless it is the authorities in concern and on condition that a search warrant was presented.

5) Free Anti protection systems software dropped in the box with a purchase of brand new equipment.
   i) When the user turns on their device, which ever it may be, he/she should not be able to proceed with logging online. A screen message should pop up saying "please download the Anti protection system first". Doing so will provide all users a protection system.

6) Educate the users talk to me!
   i) Not all the technology users fall among the millennial generation, I am from the

1900s period of time, you cannot pick me up from this earth and toss me on the planet Mars, because that is how it feels right now, you introduced me to this high tech world but gave me absolutely no teachings of these inventions and making it all even more worst for me you made these machines a mandatory and an only way of living and surviving in this world.

ii) You changed my environment and expect me to fit in. For God’s sake I feel like I am in Star Wars, surrounded by technology yet uneducated and illiterate and that is all because of you. You didn’t educate me, prepare me or even warn me.

iii) It’s not my fault that I am unaware; it is your fault you never taught me.

I bet you if you gather all the seniors and the veterans under one umbrella and pass them each a smart phone, they won’t even know that they can lock their phones by pressing the button that is located on the side of the phone. Or ask them to change their phone ringer; they will have no clue of the settings. We have to interact with our consumers in a language they know, use the basic standards of learning and familiarizing that they are accustomed with, communicate with them.

Our seniors taught us how to eat, drink, walk, talk when we were little and dependable on them and now it is our time to pay back and teach them in the same tone of voice and attitude they used towards us when we were a few months old. How could we abandon our senior consumers while here we are aiming for the galaxy? They ignore it because it sounds too educational and perfect.

A common man is not perfect! I am not perfect!

If I had an opportunity I would love to ask the common man, the seniors and the children of today’s era:

- What do they know about technology?
- How do they see technology?
- I would ask my seniors with all due respect, what impact the touch screen and the smart phones inventions had on them?
- Have they accepted the technology's interference in their well lived independent life styles and are they successfully able to adapt to these changes?
- What would my seniors like for to happen when it comes to technology?

- What can the government do so that the end user could conveniently know how to maneuver around these shiny toys?
- How do they figure their way around it? Do they depend on their families, friends or do they search articles online? If so how can this be made easy for them?
- Are they happy, confused, or angry with technology?
- What would the users want to remain unchanged when it comes to communication with another human being? (Since it is all now done via texting, Siri, social medias etc. etc.)?
- What do they miss having from the 1900s?

Knowing how the end user feels apart from the millennial generation who know no other, but just what they see would answer so many of my questions and concerns. The truth of the fact is this invention has left the end-user from the 1900s feeling abandoned, helpless, choice less, and dependable as he/she knows very little of technology, many don't even like it but have no other choice but to accept it. The touch screen and the smart phones inventions negatively impacted the senior end-users, as their existence and their current life style were completely ignored by the inventor of these innovations, thus leaving them dependable.

My seniors would like to live their last quarter of life in the same style they lived all their life. They must be given a choice to accept or reject technology, allow them to choose how much interference from technology is their preference of use? But don't give them technology as the only choice and a way of living. My seniors are not ignorant or illiterate. They gave us engines upon which the convenient source of transportation executed thus making travel easier and less hectic. They provided us with electricity, refrigerators, air conditioners, concrete roads but didn't make this the only way of living, they gave us a choice whether to accept and adapt it or not, they were considerate!

End-users had the choice to have their homes equipped with air conditioners or continue living as they were, whether it is the use of fans or the opened windows as their source of air circulation. Refrigerators were available but not made mandatory, compared to the upgraded cable systems today, where all the previous entertainment systems were rejected and the touch screen televisions were made mandatory and the only source for all the home-users as the new cable wire did not support the plugins on the old television systems.

My senior end-users must be given the choice either to continue using their old fashioned phones or convert to the touch screens and smart phones. Apps should not become the only way of networking as presumed, as they are well-immune to their desktop and computer systems. App is a convenience, but we can still log on to the website from our desktops, this means old phones can continue to be the source of connection for the end-users who choose it to be!

The government must pass the “bill of choice”, in doing so the end user will have the freedom of choice. Either adapting to the touch screen life style or continue as they are. Make free “technology awareness” teachings available and common so that the ones who are interested and want to learn and adapt could conveniently do so, thus making the maneuvering around these shiny toys stress-free.

In today’s way of living children move out or become occupied with whatever life is throwing at them, thus parents and elders have to live on their own. The ones who live beside their little ones, families and friends could ask for assistance but the ones who are their own caretakers are literally crippled due to these inventions and they are not happy, they are confused and even angry with technology, as it is not an entity covered under the home healthcare benefits.

Video skyping, WhatsApp and so many more ways of staying in touch with the loved ones are among the best creations of technology. Let’s tutor our seniors, our end-users without having to wait till they ask us for help!

And that my dear readers’ requests for all the womankind to step forward. As a woman is known to be a teacher, an instructor, an educator and a care-giver. Women always chose Medicine as they sensed they could take care and provide their patients with a considerate and a warm touch. Cyber Space is like an abandon planetary and as it continues to be under an attack it beseeches the women to contribute, to teach, to make it a safe playground for children. Technology is our tomorrow let’s all pitch in and fix it. Crime is at its peak in the online world, lets show we care, lets show our concentration and let’s make these cyber insecurities secure!

Bibliography

(2017, 09). Retrieved from thehackernews.com: http://thehackernews.com/2017/09/play-store-malware.html

Allman, T. (2012). *Are Extraterrestrials a Threat to HumanKind?* SanDiego, CA.: ReferencePoint Press, Inc.

Bureau, S. (2015, March). *RIT women meet with inspiring female leaders in cybersecurity.* Rochester NY: Scott Bureau. Retrieved from Rochester Institute Of Technology: https://www.rit.edu/gccis/news/rit-women-meet-inspiring-female-leaders-cybersecurity

Burrington, I. (2016). *Networks of New York.* Brooklyn : The Nation.

Currie, S. (2014). *How Is the Internet Eroding Privacy Rights?* San Diego, CA: REFERENCE POINT PRESS.

Defense.gov. (n.d.). *Cyber Strategy*. Retrieved 10 01, 2017, from U.S. Department Of Defense: https://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy/

Dorothy Parker. (2017, November 18). Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Dorothy_Parker

Edward Amoroso. (2017, Decemeber 04). *Edward G. Amoroso MOOCs and Free Online Courses.* Retrieved from MOOC LIST: https://www.mooc-list.com/instructor/edward-g-amoroso

Edward Amoroso. (2017). *Enterprise and Infrastructure Security*. Retrieved from Coursera: https://zh.coursera.org/learn/enterprise-infrastructure-security

Edward, S. (2014, march 18). How we take back the internet. (Ted, Interviewer) https://www.youtube.com/watch?v=yVwAodrjZMY. Retrieved from www.youtube.com: https://www.youtube.com/watch?v=97MWOERY_dE

Edward, S. (2014, 12 14). The Snowden files – the inside of the world's most wanted man| Luke Harding | TEDx Athens. (L. H. Athens, Interviewer) Retrieved from www.youtube.com: https://www.youtube.com/watch?v=97MWOERY_dE

Gilpin, L. (2014). *The state of women in technology: 15 data points you should know.* Tech pro Research: TechRepublic. Retrieved from https://www.techrepublic.com/article/the-state-of-women-in-technology-15-data-points-you-should-know/

http://indianexpress.com. (2016). *what-is-the-blue-whale-challenge.* Retrieved October 15th, 2017, from Indianexpress.com: http://indianexpress.com/article/what-is/what-is-the-blue-whale-challenge/

http://thehackernews.com. (2017, 09). */equifax.* Retrieved September 23rd, 2017, from thehackersnews.com: http://thehackernews.com/2017/09/equifax-apache-struts.html

http://thehackernews.com. (2017, 09). */windows10-app-permissions*. Retrieved September 23rd, 2017, from thehackersnews.com: http://thehackernews.com/2017/09/windows10-app-permissions.html

http://thehackernews.com. (2017, 09). *equifax-apache-struts.* Retrieved September 23rd, 2017, from thehackernews.com: http://thehackernews.com/2017/09/equifax-apache-struts.html

http://thehackernews.com. (2017, 08). *locky-mamba-ransomware*. Retrieved September 23rd, 2017, from thehackersnews.com: http://thehackernews.com/2017/08/locky-mamba-ransomware.html

http://thehackernews.com. (2017, 09). *play-store-malware*. Retrieved October 3rd, 2017, from thehackernews.com: http://thehackernews.com/2017/09/play-store-malware.html

http://thehackernews.com. (2017, 09). *turkish-coup-bylock-messenger.* Retrieved September 23rd, 2017, from thehackersnews.com: http://thehackernews.com/2017/09/turkish-coup-bylock-messenger.html

http://thehackernews.com. (2017, 09). *vevo-music-video-hacked.* Retrieved September 23rd, 2017, from thehackersnews.com: http://thehackernews.com/2017/09/vevo-music-video-hacked.html

http://thehill.com/homenews/administration. (2017, 03 27). *trump-signs-internet-privacy-repeal.* Retrieved October 3rd, 2017, from thehill.com: http://thehill.com/homenews/administration/327107-trump-signs-internet-privacy-repeal

http://thehill.com/homenews/administration/327107-trump-signs-internet-privacy-repeal. (2017, 03 27). *Trump signs internet privacy repeal.* Retrieved from thehill.com: http://thehill.com/homenews/administration/327107-trump-signs-internet-privacy-repeal

http://thinkexist.com. (n.d.). *intimacy.* Retrieved October 3rd, 2017, from thinkexist.com: http://thinkexist.com/quotes/with/keyword/intimacy/3.html

http://www.chicagotribune.com. (2017, 04 03). *trump-internet-privacy.* Retrieved October 3rd, 2017, from chicagotribune: http://www.chicagotribune.com/bluesky/technology/ct-trump-internet-privacy-20170403-story.html

http://www.datagovernance.com. (n.d.). */privacy-security-quotes*. Retrieved October 11th, 2017, from datagovernace: http://www.datagovernance.com/quotes/privacy-security-quotes/

http://www.ibtimes.co.u. (n.d.). *Cyber Security*. Retrieved October 8th, 2017, from ibtimes.co.uk:

http://www.ibtimes.co.uk/cybersecurity

http://www.idtheftcenter.org. (2016, January 19th). *Data Breaches*. Retrieved October 20th, 2017, from ITRC: http://www.idtheftcenter.org/2016databreaches.html

http://www.jameslyne.com. (n.d.). *James Lyne.com*. Retrieved 10 21, 2017, from Jameslyne: http://www.jameslyne.com/

http://www.ksal.com. (n.d.). *patient-information-breach-at-salina-medical-clinic*. Retrieved October 16th, 2017, from KSAL.com: http://www.ksal.com/patient-information-breach-at-salina-medical-clinic/

http://www.reuters.com. (2016, March 4th). *us-21stcenturyoncology-breach.* Retrieved October 16th, 2017, from reuters.com: http://www.reuters.com/article/us-21stcenturyoncology-breach/21st-century-oncology-says-investigating-cyber-breach-idUSKCN0W629M

http://www.searchquotes.com. (n.d.). *Avincenna.* Retrieved September 5th, 2017, from www.searchquotes.com: http://www.searchquotes.com/quotes/author/Avicenna_/2/

https://brightplanet.com. (2014, March). Retrieved October 14th, 2017, from BrightPlanet: https://brightplanet.com/2014/03/clearing-confusion-deep-web-vs-dark-web/

https://danielmiessler.com. (2015, July 8th). *internet-deep-dark-web*. Retrieved October 13th, 2017, from danielmiessler.com: https://danielmiessler.com/study/internet-deep-dark-web/

https://digitalguardian.com. (2017, July 27th). *history-data-breaches*. Retrieved October 13th, 2017, from Digital Guardian: https://digitalguardian.com/blog/history-data-breaches

https://edwardsnowden.com/. (n.d.). *In support of Edward Snowden*. Retrieved October 10th, 2017, from The courage foundation in support of Edward Snowden: The courage foundation in support of Edward Snowden Retrieved from https://edwardsnowden.com/

https://en.wikipedia.org. (2016). *Blue Whale Game*. Retrieved October 14th, 2017, from Wikipedia: https://en.wikipedia.org/wiki/Blue_Whale_(game)

https://en.wikipedia.org. (n.d.). *clay_shirky*. Retrieved September 17th, 2017, from Wkipedia: https://en.wikipedia.org/wiki/Clay_Shirky

https://en.wikipedia.org. (n.d.). *Edward Snowden*. Retrieved October 7th, 2017, from Wkipedia: https://en.wikipedia.org/wiki/Edward_Snowden

https://en.wikipedia.org. (n.d.). *Harry_Blackmun*. Retrieved September 13th, 2017, from wikipedia: https://en.wikipedia.org/wiki/Harry_Blackmun

https://fossbytes.com. (2017, February 11th). *-deep-web-darknet-dark-web*. Retrieved October 13th, 2017, from fossbytes.com: https://fossbytes.com/difference-deep-web-darknet-dark-web/

https://r.search.yahoo.com. (2017, July 17th). *The Russian Investigation.* Retrieved October 13th, 2017, from CNN: https://r.search.yahoo.com/_ylt=A0LEV1Ct7_dZi0MAvAhXNyoA;_ylu=X3oDMTEzM3R1b3U4BGNvbG8DYmYxBHBvcwMxMAR2dGlkA0I0ODM1XzEEc2VjA3Ny/RV=2/RE=1509449774/RO=10/RU=http%3a%2f%2fwww.cnn.com%2f2017%2f07%2f17%2fhealth%2fblue-whale-suicide-game%2findex.html/RK=1/RS=rG

https://techspective.net. (2017, February 1st). Retrieved October 17th, 2017, from techspective.net: https://techspective.net/2017/02/01/biggest-data-breaches-year-2016/

https://www.csoonline.com. (n.d.). *What the heck happened to the constitution.* Retrieved October 2nd, 2017, from www.csoonline.com: https://www.csoonline.com/article/2220119/microsoft-subnet/in-this-digital-age--what-the-heck-happened-to-the-constitution-.html

https://www.helpnetsecurity.com. (2016, 01 29). *History of cyber attacks from ancient to modern*. Retrieved October 10th, 2017, from www.helpnetsecurity.com: https://www.helpnetsecurity.com/2016/01/29/the-history-of-cyber-attacks-from-ancient-to-modern/

https://www.reference.com. (n.d.). *created-computer*. Retrieved September 7th, 2017, from www.reference.com: https://www.reference.com/history/created-computer-6ba32582e43467b8?qo=contentSimilarQuestions

https://www.reference.com. (n.d.). *History computer invented*. Retrieved October 10th, 2017, from www.reference.com: https://www.reference.com/history/computer-invented-3ea437d4357df85f?qo=leafPageFeaturedContent

https://www.reference.com. (n.d.). *history/computer-invented*. Retrieved September 7th, 2017, from www.reference.com: https://www.reference.com/history/computer-invented-3ea437d4357df85f?qo=leafPageFeaturedContent

https://www.statista.com. (2007-2017). *The Statistics Portal*. Retrieved October 15th, 2017, from statista.com: https://www.statista.com/statistics/290525/cyber-crime-biggest-online-data-breaches-worldwide/

Koba, M. (2011, October 10). *Women & Business*. Retrieved from CNBC: https://www.cnbc.com/id/44687913

Loewe, F. (Director). (1964). *My Fair Lady* [Motion Picture]. Retrieved from https://www.youtube.com/watch?v=Doz5w2W-jAY

McPherson, S. S. (2017). *Artificial Intelligence.* Minneapolis: Lerner Publishing Group Inc.

Minick, B. (2016). *Facing Cyber Threats Head On.* London: The Roman & Littlefield Publishing Group, Inc.

Obee, J. (2012). *Social Networking.* Lanham. Toronto. Plymouth, UK: THE SCARECROW PRESS, INC.

Quotations about Women . (1998). Retrieved from The Quote Garden: http://www.quotegarden.com/women.html

Quotes About Knowledge. (2017). Retrieved from goodreads: https://www.goodreads.com/quotes/tag/knowledge?page=2

Razia Sultana. (2017, November 19). Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Razia_Sultana

Sandra Senft, F. G. (2013). *Information Technology Control And Audit.* Boca Raton, FL.: CRC Press, Taylor & Francis Group.

Sharma, K. (2017, September 26th). *the-reality-behind-the-theory-of-killer-game-blue-whale.* Retrieved October 14th, 2017, from The Times of India: https://timesofindia.indiatimes.com/life-style/health-fitness/de-stress/the-reality-behind-the-theory-of-killer-game-blue-whale/articleshow/59881467.cms

Snell, E. (2016, October 26th). *phi-data-breaches*. Retrieved October 17th, 2017, from HealthIT Security: https://healthitsecurity.com/news/phi-data-breaches-after-unsecure-email-cybersecurity-attack

Snowden, E. (2016, 05 8). State of surveillance with Snowden Edward and Smith Shane. (S. Shane, Interviewer) Moscow: HBO. Retrieved from www.youtube.com: https://www.youtube.com/watch?v=ucRWyGKBVzo

Sr., W. G. (2009, july 10th). *The Past, Present, and Future of Cybersecurity* . Retrieved september[24th, 2017, from jnslp.com: http://jnslp.com/wp-content/uploads/2010/08/03_Sharp.pdf

Stone, O. (Director). (2016, 09 16). *snowden* [Motion Picture]. Retrieved from https://video.search.yahoo.com/search/video?fr=opensearch&p=snowden#id=3&vid=b39c45ff7298f7e2adc38e1c45c05ebc&action=view

(2013). *timeline.* Retrieved from www.nato.int: http://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm

VisionQuest EyeCare, Information regarding Breach. (2017, April 27TH). Retrieved September 20th, 2017, from VisionQuest EyeCare.com: http://visionquesteyecare.com/2017/04/27/information-regarding-breach/

Westman, S. (2015, July 30). *To Better Fight Attackers, Get Women in Security and Close the Gender Gap.* Retrieved from SecurityIntelligence: https://securityintelligence.com/to-better-fight-attackers-get-women-in-security-and-close-the-gender-gap/

Wikipedia. (n.d.). *Boston Marathon bombing*. Retrieved October 13th, 2017, from wikipedia: https://en.wikipedia.org/wiki/Boston_Marathon_bombing

Women in IT Security: Influencers. (2017, July 11). Retrieved from SC Media: https://www.scmagazine.com/women-in-it-security-influencers/article/674103/

Women Leaders in Cybersecurity: Closing the Gender Gap. (2016, October 14). Retrieved from Center For Cyber Security: http://cyber.nyu.edu/events/women-leaders-in-cybersecurity-conference/

Zuchora-Walske, C. (2010). *INTERNET CENSORSHIP.* Minneapolis: Learner Publishing Group, Inc.