DETERMINANTS OF INTERNET CRIMES IN USA

BY

Deniz ARSLAN

SUPERVISOR

ASST.PROF.MANU DUBE

MASTER THESIS

INSTITUTE OF SOCIAL SCIENCES

DEPARTMENT OF MANAGEMENT INFORMATİON SYSTEMS

Yeditepe University

FEB,2020

APPROVAL

Approval of the Institute of Social Sciences

Prof. M. Fazıl GÜLER
Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master.

Prof. A. Simon HACINLIYAN
Head of Department

This is to certify that we have read this thesis and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Arts.

Asst. Prof. Manu DUBE
Supervisor

Examining Committee Members

Asst. Prof. Manu DUBE [Yeditepe University]

Prof. Gülay BAŞARIR [Mimar Sinan University]

Asst. Prof. Asım KAZANCIGİL [Yeditepe University]

PLAGIARISM

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

04/02/2020
Name, Last name : Deniz Arslan
Signature :

ABSTRACT

DETERMINANTS OF INTERNET CRIMES IN USA

Because of the improved technology and easiness to getting an information, nowadays, a regular increase at cyber crimes can be observed in every year. In every year, many people and organizations, financially suffers from it. Because of the topic' main subject is human (perpetrator), and because of the difficulty for proving its aim, purposes of activity are trembles in balance. This work will examine cyber attacks which caused financial loss across US states in light of analysis reports and cyber security practices in between 2009-2018. And will try to harmonize these datas with demographic features and statistics of these states in order to find an answer for these crimes. We also compare our results to effect of these factors on other types of crime.

ÖZET

ABD'DE Kİ İNTERNET SUÇLARINI BELİRLEYİCİ FAKTÖRLER

Günümüzde, teknolojinin gelişmesi ve bilgiye ulaşımın kolaylığı sebebiyle, siber suçlarda her yıl düzenli bir artış gözlemlenebilir. Her yıl, birçok insan ve kurum bundan finansal olarak etkilenir. Bu konunun ana öznesi insan olduğundan ötürü ve amacın kanıtlanmasının zorluğundan dolayı, bu aktivitelerin amacı asılı kalmaktadır. Bu çalışma, ABD'deki eyaletlerde finansal kayba yol açmış siber saldırıları, analiz raporları ve 2009-2018 yılları arasında ki siber güvenlik uygulamaları ışığında inceleyecektir. Ve bu hususları ülkelerin demografik özellikleri ile açıklamaya çalışıp, istatistikler ışığında, genel hatları ile bu yıllar arasında gerçekleşmiş bu suçlara neden veya nedenler arayacaktır. Ayrıca, bu faktörlere etki eden sonuçlar, diğer suç tipleri ile karşılaştırılacaktır.

ACKNOWLEDGEMENTS

It is with immense gratitude that I acknowledge the support and help of Mr. Manu Dube. Pursuing my thesis under his supervision has been an experience which broadens the mind and presents an unlimited source of learning.

I also thank Mrs. Sema Dube and Mr. Aşkın Demirağ for their helps.

Finally, I would like to thank my family for their endless love and support, which makes everything more beautiful.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

1.1 BACKGROUND

Technological developments in the area of IT, offers us many advantages in our daily routines. Nowadays, it takes matter of seconds, carrying out complex tasks. This helps users to gain significant amount of time advantage in their daily routines. In the other hand, this rapidness can also brings some potential disadvantages which is where the cyber security topic comes up. So, we can say that technology can be our best friend our worst enemy. According to Solange Ghernauti (2013),

"Information and communication technologies (ICT) allow huge amounts of information to be stored, processed, accessed, searched, transmitted, exchanged, and disseminated, regardless of geographic distance. These unprecedented possibilities lead to new services that can improve economic development and the dissemination of knowledge. But at the same time, new types of crime have appeared, as well as old crimes committed with new Technologies (p.1)"

We can think that cyber crime and cyber security like united parts of a wheel. Both of them 'needs' another one to exist. Security techniques emerges from attack types and its impacts. Level of an attack can be differ. It may targets small to big businesses or it may focuses on national level. Degrees of threats can create international protocols against cyber crime or can make cyber security companies rich. Also, unlike many disciplines, this area of IT, going to develop itself automaticly because of the technology. In every new period of time, users can face new 'challanges' in all around of world. According to Symantec Group's 2017 Global report, (Symantec Corporation, 2017) 978 million people in 20 countries were affected by cybercrime in 2017 and consumers who were a victims of cybercrime globally lost $172 billion. It is hard to find a "general" motive or purpose of a cyber attack. Achivements can be generalized certain aspects like money, control ego, fame etc. Or the nations statistical datas like GDP, gini rate, educational level can effect it. So, it is wrong to putting forward a single motive for attacks. Because, every case is different. Crimes can be done by an organization or it can even done by

state (directly or indirectly). Every perpetrator whether is a “lone-wolf” or works with an organization, has a diverse point of view. In their work, Gragido, Molina, Pirc and Selby states (2013);

“As we mentioned earlier in this chapter, perpetrators of organized crime are focused on control, power, and wealth. State-sponsored cybercrime is no different, as these criminals focus on control, power, and wealth at the national level instead of at a small group level.(p.30).”

Besides all of this, in order to explain the topic better, we have to define and understand the complex meaning of cyber crime.

2. CYBERCRIME

2.1 DEFINITION OF CYBERCRIME

Defining cyber crime can be challenging due to its wide range of understability. It can be seen as a frame which we can put many types of paints in it. This occurs mainly because of the wide range of types of cyber crimes. Also, all of these different types of attacks, can be done by in a different way. For example, when a perpatrator wants to know what was written down his/her target's mail, he/she can done it by two ways. He/she can just look at secretly or he/she can do it by various hacking softwares. So, there are various ways and techniques to commit a cyber crime. In their work, Sarah Gordon and Richard Ford explains this situation like (2006);

"Despite the fact that the word "Cybercrime" has entered into common usage, many people would find it hard to define the term precisely. Furthermore, there is no catch all term for the tools and software which are used in the commission of certain online crimes."(p.1).

In addition to that, because of the continous development of technolgy, even a definition which can be accepted today, may not be enough at tomorrow to cover new types of cybercrimes. This situation reflects on the laws which are about cyber crime. It is clear that defining and regulating laws for cyber crime, is a challenging task for juristiction unlike any other sector. It happens because of ; the laws are "created" from terms which are belongs to the sector/are which is going to be regulated. And secondly, the word association in the IT area. For the second part, we can say that terms which could be using for making laws can become "meaningless". In his work, Jonathan Clough underlines this situation like (2010);

"If taken literally, each term suffers from one or more deficiencies. Those definitions that focus on 'computers' may not incorporate networks. Others such as 'cybercrime' or 'virtual crime' may be seen as focusing exclusively on the Internet. Terms such as 'digital', 'electronic' or 'high-tech' crime may be seen as so broad as to be meaningless. For example, 'hi-tech crime' may go

beyond networked information technology to include other ‘hi-tech’ developments such as nanotechnology and bioengineering.”(p:9).

These arguments puts us in a path which we needed to past in order to describe the term of cybercrime efficiently. We have to generalize the terms which I stated because there are many of them and they became complicated. This process can be done by classification of cyber crime acts. In this way, we can get away with term confusions and we can take precautions of juristical “openings” which I stated. Three-stage of classification which was done by the US Department of Justice can be an example of this (2010);

“1. Crimes in which the computer or computer network is the target of the criminal activity. For example, hacking, malware and DoS attacks.

2. Existing offences where the computer is a tool used to commit the crime. For example, child pornography, stalking, criminal copyright infringement and fraud.

3. Crimes in which the use of the computer is an incidental aspect of the commission of the crime but may afford evidence of the crime.

For example, addresses found in the computer of a murder suspect, or phone records of conversations between offender and victim before a homicide. In such cases the computer is not significantly implicated in the commission of the offence, but is more a repository for evidence.”

As we can see the three-stage classification in the above, during the defining process, pc and its axis were placed in the center and from there, the scope of cyber crime was tried to be classified with some kind of classification method. In this way, a frame was drawn to the confusion of definition which I stated before and it provided wide meanings not permitted to going out of frame. In brief, a definition which “summarize” cyber crime with its main lines will be more coherent than a single and standart definition. But, we have to keep in mind that, because of the continously developing technology and variety of cyber crime types, the classification definition which I talked about may become insufficient to define the cyber crimes in the future.

2.2 "PROBLEMS" OF CYBERCRIME

It is more difficult to track and find evidence for cyber crimes than physical crimes. Most of the time, evidences are "clear" and tangible in physical crimes. For example, in the case of a person who became a victim an assault, camera recording, assault reports which can be obtain from a hospital or witnesses can be shown as a physical evidence. Also, because of the technology today, perpetrator's ID can be confirmed via even a single hair strand or a cigarette butt which is around the crime scene. On the other hand, it is hard to In her work, Marjie Brings talks about this situtaion like (2013);

"The lack of physical boundaries and the removal of traditional jurisdictional demarcations allow perpetrators to commit multinational crime with little fear (or potential) of judicial sanctions. For the first time, criminals can cross international boundaries without the use of passports or official documentation. Whereas traditional criminal activity required the physical presence of the perpetrators, cybercrime is facilitated by international connections that enable individuals to commit criminal activity in England while sitting in their offices in Alabama. (p.7)"

Obtaining evidences and juridical processes (if we ignore expections) are more faste than the processes of cyber crime. Also, cyber crimes are more "new" than the physical crimes in human history and because of that, its laws are not wide and inclusive as physical crimes'. In addtion to this, cyber crime perception of legists who are related with this topic, are differant than the physical crime perception. This perception leads a thinking that cyber crime can be seen as "simple" and "worthless" and perpetrators are "not guilty". Nowadays, we can say that this perception is somewhat broken. However even a huge example like John Edward Robinson a.k.a "Internet Slavemaster" who is the Internet's first serial killer, this perception still in peoples minds (2013);

"Many stereotype computer criminals as nonthreatening, socially challenged individuals (i.e., nerds or geeks) and fail to see the insidious nature of computer crime; 36.3 percent of officers believe that the investigation of computer crime interferes with their ability to concentrate on "traditional" crime.(p.8)"

Educational process and qualification of staff is another problem. Even with the helps of developing technology on covering these deficiencies, there is a still (especially countries which

are developed below at a certain level and some rural parts of a developed countries) a qualified staff deficiency. So, there are few number of staff who has the knowledge and experience enough to execute procedures during a cyber attack or potential cyber attacks. For example, in Turkey, many firms (especially small-sized firms) do not have an IT team or any personnel who can provide system and network or cyber security services. Even some firms which are using these services (again especially small-sized firms) are taking these services via outsourcing and it causes another security problem. All of this situation is an obstacle in front of reporting of an attack and recording it. And because of that, the attacks and the losses are not reported because of some unexpalined reasons and it makes hard to preventing potential attacks (2013);

"Although estimates vary, most experts agree that the vast majority of Fortune 500 companies have been electronically compromised to the tune of at least $113 billion/ year, and 81 percent of all businesses have experienced some victimization, with 21 percent of that stemming from unauthorized access by insiders. However, early studies indicated that only 17 percent of such victimizations were reported to law enforcement authorities."(p.10).

Another problem arises in the area of e-commerce in parallel to the developing technology. It is clear that e-commerce brings many advantages to the table in terms of making easy, fast and secure transactions. However like every new technologic advancement, the area e-commerce brings disadvantages together with advantages. Control over this area is lesser than than the other banking operations. So, it is more difficult to track down a cyber crime during transactions because of the shopping has been done from internet. This situation effect people who are have no intentions to commit a crime and does online shopping. It also causes making difficult for tracking down money transactions which are belongs to the terorrist organizations. In brief, we can summarize e-commerce area which has both advantages and disadvantages like in the below (2013);

"Like all other emerging technologies, the implications for e-payments are both positive and negative. Consumers have benefited, for example, from the enhanced services and efficiency offered from e-banking. In addition, the low overhead associated with online financial institutions has increased competition, resulting in lower interest rates and higher yields. On the other hand, the criminal element

has embraced a variety of new payment methods which are often anonymous, involve multijurisdictional transactions, and exist in an environment which lacks regulation and government oversight."(p.20).

Lastly, advantages of technology comes also with disadvantages. Especially, in the area of cyber crime, even the technological developments, %100 safety is not provided yet. In addition to that, human factor (which I talked about before) makes some situations even more complicated. In my opinion, in order to solve these problems, spotting of "blind sides" and fixing them is necessary.

2.3 IMPACTS OF CYBERCRIME

One of the most challenging topic at cybercrime is determining its effects. Because of the definition problem which I talked about above and the low rate of the recording these crimes it is nearly impossible to making a %100 percent analysis on the impact side. In his work, Nir Kshetri talks about this topic like (2010);

"Estimating economic, social, and political impacts of cybercrimes and web attacks to a reasonable level of accuracy has been a challenge. One view is that since many web attacks go unreported, such impacts tend to be underestimated. The opposite argument is that there may be vested interests among security companies to exaggerate the level of cybercrimes." (p.4)

Nevertheless, it is a irrefutable truth that cybercrimes which are recorded caused serious socio-economic results. Also, because of the because of the development of nowadays technology, cybercrimes are generates more impact and becomes more threatening than other crimes. This situation caused serious damages to the targets who were become a "goal" of these crimes and also intimidates them. Statistically, according to the 2007 PricewaterhouseCoopers'biennial Global Economic Crime Survey, over 43% of the companies interviewed reported suffering one or more significant economic crimes. The average loss from fraud per company increased nearly 40% in 2 years from roughly US $1.7 million in 2005 to approximately US $2.4 million in 2007 (Kshetri, 2010). All of these actions made some questions in the head of parties who were become a target of a cybercrime. And this caused them to fear and anxiety. The concept and form of crime are seen more different in people's minds than from past. People didn't think that they

will not be effected from cybercrime concept in the past, however now it becomes a big and dangerous threat for society. In parallel of this, rise on cybercrimes are justifes this concern. In his work, Nir Kshetri touches on this matter like (2010);

"An IBM survey released in 2006 also found that there were three times more Americans who thought they would be victims of a computer crime "in the next year" than of a physical crime. Likewise, according to a survey conducted by University of Calgary's Rozsa Centre, the average citizen is more likely to be a cybercrime victim than that of a physical crime. Another survey conducted by TNS Sofres indicated that about 60% of Americans were fearful that their passwords would be stolen when they bank online, and 38% do not trust making payments online"(p.6)

As it can be seen, impacts of cybercrime aren't stay only with economic damages. It also caused psycological impacts too. Another example of impacts of cybercrimes is cyberbullying. Cyberbullying is equal to the physical abuse in the cyberworld. Cyberbullying is equivalent of physical abuse in the cyber world. It mainly done by verbally and supported with specific materials (pictures, videos, etc.). Cyberbullying, which is mostly performed verbally, is supported by certain materials (pictures, videos, etc.), and more often through abuse of online services, leading to serious psychological and sometimes even suicidal consequences on its victims. Especially with the development of mass media today, this situation becomes more global and dangerous and has periodic or permanent effects on young people and their families. According to a research about this topic (2010);

"Cybercrime's adverse social impact is felt across all social and age spectrums. One estimate suggested that 20–25% of young people have been victims of cyberbullying. According to WiredSafety.org, more than half of 9–13-year olds "have either cyberbullied or been cyberbullied, or had a close friend who was"(p.5).

If we look in terms of economically, scale of attacks changes according to the attack types. For example, between 1999-2003, there were nearly 30 million credit cards has been stolen and this brought 15 billion USD loss in USA (Kshetri, 2010). Phishing attacks can have more wider scope and have more effect diameter. By definition, Phishing can be defined as the person in the target trying to seize that person's personal information (identity, bank information, personal information, etc.), or trick the target into a fictitious purpose, to gain financial gain from the

attacker's personal accounts. A good number of phishing cases starts with an e-mail. Contents can be vary. It may look innocent and not-demanding or it may full with a list of demands. So, some of them looks “clearly” as a spam mail which can harm you and some of them don’t. In these type of attacks, the attackers acts like tigers at haze, and they attack towards their victim as soon as they have the opportunity. Every one of them wants to get the “big prize”.

High profile breaches/phishings are another major phishings that can cause disastrous effects. These kind of attacks aims at big sized companies and tries to get big informations about their accounts, customers, internal datas etc. Coca-Cola had suffered this kind of an attack in 2009, when an e-mail which looked like it came from executive, had spread malwares and keyloggers to the system when it opened(2015:9). Similar type of this kind of an attack, happened to the Target Corporation which costed them 200M USD. In this story the attack actually was not targeted to the Target Corporation, but when the one of the staff opened a e-mail and it loaded malwares. After that, hackers got the valuable information.

In brief, impact of cyber crimes cannot be observed in one perspective. Because there is not only one “impact type” of cyber crimes and the effects of cybercrimes can differ from one sector to anoter. So, in order to analyze its effects, we should be observe impacts more inclusively and also we should not gather the datas from one side of it.

2.4 CYBER TERRORISM

Terrorism has been a common problem all over the world for years. Although the concept of terror and terrorism is still internationally discussed today, certain organizations carry out actions which targets innocent people for their own purposes or interests. This issue, which was historically affected and still influences millions of people, was more physical than before (in terms of technological developments). Terrorism which has been more physical and more demanded on manpower was evolved. And it putted cyberterrorism topic which is a subheading of cybercrime.

As I have just mentioned, cyberterrorism, which is essentially a subheading of cybercrime, is important because of the financial losses it has caused and is still causing. These damages, which may be on a large scale, will harm the affected country both economically and socially. Before touching on this part of the subject, first of all I want to mention is the problem of definition of cyberterrorism.

2.5 DEFINITION OF CYBER TERORISM

Just like the definition "problem" in the concept of cybercrime, the same problem exists in this area too. This is due to both the terrorism and the complexity of the subjects which are subjects to cybercrime, as well as the inability to generalize the actions that may or may be taking place in this field, as in cybercrime. One of the first accepted definition is the definition which was in the report of Center for Stragetic and International Studies, Cybercrime, Cyberterrorism, Cyberwarfare, Averting an Electronic Waterloo entitled (2006);

"Cyberterorism means, premeditated, politically motivated, attacks by subnational groups, or clandestine agents, against information and computer systems, computer programs, and data, that results in physical violence where the intented purpose is to create fear in noncombatant targets."(p.66)

In his study, Andrew Kolarik criticized this definition and concluded that the individual was defined as a terrorist (even if the state had a wrong attitude) in this definition (Colarik, 2006, p.66). According to this definition, the freedom of thought and non-harmful expression were put under some kind of pressure. Also this definition is based on physical violence, and other possible harmful consequences are ignored. In summary, I think that, definition has openness to potential attacks and detection problems. It is important that the definition which is going to be based on the juristical side, should not have any "deficits". In addition, although cyber terrorism often flashes a physical loss in peoples minds, social and psychological losses should be stated and should be included to the definition. In this context, Marjie Britz's definition of Cyberterrorism is like this (2013);

"Cyberterrorism may be defined as a deliberate, politically or religiously motivated attack against data compilations, computer programs, and/or information systems which is intended to disrupt and/or deny

service or acquire information which disrupts the social, physical, or political infrastructure of a target”(p.90).

As we have seen, this definition is more inclusive than the previous one and has tried to provide legal expanse in some terms. As the motivation of attack and the types of casualties are explained more clearly and comprehensively, it can be facilitated during any future legal process. Besides these definitions, of course, many other definitions are available in the literature. The aim of all the definitions is to eliminate the gaps and to ensure that the definition is inclusive..

2.6 SOME CYBER-TERRORISM CASES

As I mentioned in the definition section, it is necessary to learn the purpose of a cyber attack to determine whether it is an act of cyber terrorism. Not every cyber attack is an example of cyber terrorism. For an attack to be accepted as a cyber-terrorism attack, it must comply with the definition of cyber-terrorism. For example, if a hacker attacks on a multinational organization for trying to make a name for himself/herself, is not going to considered a case of cyber terrorism. On the other hand, actions of organizations or individuals which can have a political, religious or financial purposes that have the purpose of harming the instutions of countries or companies which may affect the whole country's economy can be considered as a cyber terrorism cases. For example, the SEA organization, which emerged in Syria in 2011, carried out attacks on the countries, and the companies in those countries for political reasons. This organization consists 8 people who are beliving that that they are protecting their homeland and strongly support the reforms of President Bashar-Al Assad and they are against the western and arab media which are not in favor of Bashar Al Assad (Eleanor Lockley, 2014).

As I mentioned above, cyber terror attacks can be carried out to major companies or organizations in the targeted country. In this context, SEA organization attacked Angry Birds and Microsoft. In the Angry Birds attack, the organization changed the company's logo (Eleanor Lockley, 2014). In the case of Microsoft, SEA has infiltrated into the company for a long time using the pshing method, and finally, they seized the social media and e-mail accounts of its employees (Eleanor Lockley, 2014). Another attack by the SEA was Saudi Arabia. They blamed

the Al Saud regime for terrorism and targeted the government's website and seized their several domains (Eleanor Lockley, 2014).

Another example is the Stuxnet virus. Stuxnet virus, which emerged in 2010, attacked Iran's national facilities, including nuclear facilities. At first, it was not known who or by whom this virus was created. However, the United States and Israel were later referred to as perpetrators, but no official explanation was made from either country. It is believed that this virus, which has a very complex structure, cannot be the work of a group or organization without support. Certain authorities have expressed their views as follows (2014);

"Security specialists (Kaspersky, Sysmantic, Cherry, 2010; Langner, 2011) believe that due to the complexity of the virus implementation and its sophisticated nature, it was more than likely conducted with "nation state support."" (p.111)

Today, the US and Israel are generally regarded as the creators of Stuxnet.

In addition, the attack on HSBC in the UK in 2012 could serve as an example of cyber terrorism. In this attack, the attackers identified themselves as Fawkes Security and claimed that the banks were corrupt and carried out these attacks. In their articles, Eleanor Lockley and Babak Anghar mentioned this attack as follows (2014);

"In October 2012, a group of hacktivists did lay claim to the DDoS attack on HSBC which impacted millions of user's ability to access their online accounts around the world. Following these kinds of attacks it is commonplace to see banks defending customer data—usually insisting that the attacks did not compromise personal information. A hacking group who call themselves fawkes security on Twitter and who act in association with the "Anonymous" ideology (see section below) laid claim to the DDoS attack on HSBC their justification being that the banks are corrupt and have caused the global economic crisis. The group tweeted counter information suggesting that personal data were affected: When HSBC said "user data had not been compromised" This isn't entirely correct. We also managed to log 20,000 debit card details. #OpHSBC"(p.112)."

As can be seen, cyber terrorism incidents took place and still takes place within certain frameworks. At this point, the point that we have to focus on, are the reason or reasons of the

actual event or events. From the cause-and-effect relationship, we can determine whether a cyber attack belongs to a subset of cyber terrorism.

2.7 FACTORS AFFECTING CYBERCRIME

Reasons of crimes are always becomes a curiosity for everyone. In regular crimes we can at least guess or learn the actual reason of factor effecting it even in the end crime. For example, in a homicide case, we can learn the reason which was behind of it, if the perpatrator gets caught up and confesses. Or we can at least guess poverty and unemployment when a man or woman tries to rob a store. Even the reasons maybe not clear as this, there are some economic factors are effecting financial cybercrime. While, I will be talk about some of them in more detail in this part, Folashade Okeshola and Abimbola Adeta summarizes the motivating factors affecting cybercrime like (2013);

"The motivating factors that encourages or drive individuals into cyber crime according to respondents varies and it is determined based on a number of different factors such as money/ financial gain, recognition/fame, low rate of conviction or even being caught, easy to perpetrate, intellectual pursuit, frustration, revenge, display of wealth by corrupt politicians and yahoo yahoo boys, laziness, unsatisfaction from what they earn, lack of good moral upbringing from parents and guardians (p.110)."

It is known that a good number of cybercrimes were done with financial purposes. So we can say that, nowadays cyber crime's main goal is making money like the organized bank robbers in the past that perpetrate large scale raids on financial instutions (Wori, 2014). And over the years, this situation shifted to a hunger for "success" especially in the new generations who had a predisposition to act a cybercrime. Okechukwu Wori talks about this situation like (2014);

" Now, instead of being inspired by a need to prove their art, cybercriminals are often motivated by financial gain. As a consequence, the old stereotypical image of the kid living on Skittles, while doing seventy-two hour hacks, has been replaced by a much darker and more complex approach, which is well organized and much more focused on making trouble (p.52)."

Because of the developing technology and the rise of internet usage in every part of the world, nowadays it is not a challenge to do the tasks which we usually accomplished in a long period of

time. It also reverberates on banking operations like transfering money to another account or paying your bills with your smartphone in seconds. On the other hand, technological developments can effected this “traffic” of data in a negative way. Because just like normal users of these applications, there will be individuals or organized groups who are want to getting their “share” from these transactions. In addition to that, some technical developments makes it possible for the perpatrator to cover up himself/herself. He or she can show his/her location even in a different continent even he/she robs the store which is next to him/her. So today, the virutal nature of cyberspace allows that commiting a crime a like bank robbery from the safety of a location 6,000 mikes away from the actual scene of the crime (Wori, 2014). Another important point about internet usage is its “population”. Nowadays, it is a very rare thing for a household which has no internet usage. Because of this widespread effects of it, internet comes everybody whether they are criminal or not. So, while the developments on cyber security now can reach everybody, this aspect of internet usage brings an open door for potential crimes. In USA, cyber-attacks on machines which are connected to the Internet have increased by 260% since 1994 and estimated loss is 1,290 million dollars annually in the U.S. whether the technology is advances but no one is safe from the hacker’s attacks (Methmali, 2016). So, in brief we can see that, aside from the positive sides of it, the internet usage and its promptness can be a factor of a financial cybercrime.

Another important factors are unemployment and poverty. It is clear that when a country’s economy goes bad, there will be consequences of it. In many cases these consequences stars wtih dismissals. Because of lack of resources, owners of companies tends to making retrenchments. It causes dismissals and creates unemployments within the subject country. So, when a “hole” carves a country and getting bigger at every day, it would be inevitable for its citizens not affecting by it. And this situation will bring even more trouble like a long-time unemployment in the whole of the country which may cause even a nationwide riot, if a solution don’t come up quickly. Long-term unemployment can come up with a serious level of a crime rate because of the despair and losing trust of the people to its government. For example, if an individual is affected by long-term unemployment, he or she starts to be affected by the consequences of such a situation, namely a sense of exclusion, injustice, and finally the lack of hope of finding a

legitimate source of income (Pieszko, 2016). So, basically when a path closes or stuffed with a many blocks, people naturally will look for other roads for reaching their finish, even these roads are dangerous. This brings crime on table and it would be widespread if there is a big rate of unemployment. In this case, people will have more courage for acting a crime, because if they don't they think will suffer more. Especially among the younger people who may experinced the effects of long-term unemployment like fights, divorces, unrests and despairs in the family, tendency of commiting a crime will be more higher. Grzegorz Pieszko talks about this situation like (2016);

"Because of the social and demographic factors, such as gender, age or education level of people affected by the unemployment, there may be various relationships and impact on criminal activity. An analysis of police statistics shows that the highest intensity of crime occurs among unemployed people who are under thirty years of age (p.19).

Just like in the regular crimes, in the cyber-world, unemployment factor comes into play by becoming an actor on cybercrimes. For example, one of the main reasons of cybercrime in Eastern Europe and Russia is the levels of high unemployment and low wages (Kshetri, 2010). And many of these people who commits, commiting or had commited cybercrime, doing this because of the psychological impacts of these factors on their lives. In addtion that, in some cases, there will be much more opportunities in terms of payment when people agree on committing a cybercrime. Nir Kshetri explains this situation like (2010);

"Beyond all that, a financial crash in Russia in 1998 left many computer programmers unemployed. In Russia top university graduates are paid up to 10 times as much as they would earn from legitimate IT jobs by organised criminals "(p.1071).

Poverty is not only a factor of financial cybercrime but is also in bound with unemployment. Poverty can come from various reasons in household like general bad influence comes from countries' economy, high inflation rate or unpaid personel debts but it is also a result of unemployment rate. And just like unemployment, poverty can effect crime rates. Because like I stated before, people will look for sources for income even they are illegal. So, poverty has long been the factor which has been strongly associated with criminal activity. As it was indicated by Alain Peyrefitte, "crime is the child of poverty" (Piezko, 2016).

Gini rate is another important factor which we have to emphasize on when we looking out factors of not only for cybercrimes but crimes in general. This gap may not be the primary reason for committing a crime but because of the clear view of inequality between people in the society can make some people to committing a crime. This factor can be combined with other factors such as graduation rate, unemployment and poverty rates because all of these factors can make the levels of inequality even more visible. As a result of this, there will be various mixed feelings like anger, grudge, despair and etc. And these feeling can drive the person who is suffering from bad economy to commiting a crime. In brief, if the gap between poor and wealthy is wide enough, and the other factors such as poverty and unemployment are on the table, people who are in a bad position in terms of economy, will look for a solution even it is against the law for reducing that gap. Regarding this topic, Piezko states like (2016);

"The increase in the gap between levels of wealth causes an increase in inequality between people. The bigger differences between the wealth level of social groups, the bigger possibility of social uneasiness and discontent. Inequality does not cause a growth in crime among the wealthy but has a higher impact on criminal behavior of those who have lower social stratus. The analysis of dependencies between social groups shows that if only a small percentage of people received very high income, and the majority of the population much lower, the vulnerability of the majority of those who earn less to commit a grime would be bigger (p.20)."

Another factor is about education level. It is clear that a good level education can make a solid difference at a person's life. Not only a solid education gives person a proper general culture, it can lead him/her, his/her goals in the future. In the area of crime, education level has two faces. In one face, it can reduce crime rates. In the other face, a solid and detailed education (especially in the area of IT), cen lead some people commiting crimes. It's known that majority (60%) of the youths who engage in cyber crime are university students (Adeta & Okeshola, 2013). It does that with the combination of bad economy, high unemployment rate and poverty. In a scenerio like this, a person who are skilled and educated about IT skills, can look for different type of "opportunities" if he or she couldn't find a legl job. And just I stated before in some places, people will get much more higher salary then they get from regular jobs. So, all of this good level education and lack of jobs because of high unemployment rate can make illegal types of cybercrime careers attractive (Kshetri, 2010).

3. SITUATION IN USA

3.1 GENERAL ANALYSIS

USA one of the major countries in terms of technological, educational and economic level. Some of their multinational (but also national) companies business volume are probably larger than many other multinational companies around the world. But, the country with this size, can have problems which has same size as it is. Like the mortgage crisis in 2012 which started as a "national" crisis, it rapidly became a "global" crisis in a short period of time. Any major cybercrime happens at their big-sized companies that costs major numbers, direclty effects other multinational companies and its countries' economy. Other than nationwide view, on the peoplewide, according to the Internet Crime Report which covers USA's 2017 cybercrimes, over than 84.000 people has became a victim of non-payment/non-delivery scam. List continues with personal data breaches and phishing attacks which effected over 25.000 people per case (FBI, 2017). Like every country in the world, the importance of cybersecurity on cybercrimes has increased over the years. Because of the technological improvements, and the capability of creating larger impact, cybercrime issue climbed the ladder of top threat list in the USA. In his work, Nir Kshetri talks about this situation like (2016);

"In the early 2000s, cybercrime and cyber-terrorism were the No. 3 priority for the U.S. behind counterterrorism and counterintelligence. In 2013, the U.S. director of national intelligence declared that cyber-threats were the greatest danger facing the nation. General Martin E. Dempsey, chairman of the U.S. Joint Chiefs of Staff, declared that cyber-attacks had "escalated from an issue of moderate concern to one of the most serious threats to national security"(p.89).

So, in parallel to the cybercrime acts and potential threats, government of USA takes series of prevention measures. These measures can sometimes be a plan, sometimes an organization and sometimes a report. All of these measures has the same purpose which is strengthening USA's instutions against major cybercrime and cyber terrorism acts and also protect civilians against these crimes. Nir Kshetri lists these measures with the years which they taken like (2016);

"-2003 National Strategy for Securing Cyberspace (NSSC) was issued.
-2006 National Infrastructure Protection Plan (NIPP) was released.

-2008 Comprehensive National Cybersecurity Initiative (CNCI) was released.

-2009 The Obama administration released Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure.

-2009 The Pentagon established the U.S. Cyber Command.

-2013 President Barack Obama issued an EO, "Improving Critical Infrastructure Cybersecurity. (p.90)."

All of these measures taken one after another becuse of the continuing threats. Like we can see the historical ranking of the measures, we can say that every government tries to make some adjustments and improvements in this area. Like I stated in the cyber terrorism part, impacts of attacks can be crucial when the attack targets national buildings. It also causes major problems when the attacks targets places like multi-national companies and national instutions which holds classified informations of citizens identities, their personel informations or financial informations. According to PricewaterhouseCoopers' (PwC) 2014 U.S. State of Cybercrime Survey, due to high profile data breaches at companies such as Home depot, Target and JPMorgan, data and information of about half of U.S. adults have been stolen (Kshetri, 2016, p.91). This situaiton causes a huge stolen critical information which can lead to a major financial and other losses. On this subject, we have to talk about secuirty against these attacks. In the previous chapters, I stated about the "problems" of cybercrime and the lacking of enough preventive measures by giving examples in Turkey. In USA, this situtaion is similar. Many companies do not spends on cyber security or do not have any kind of strategy about how to cope with it. Also many of them do not have any personnel who can cope with it. This creates a open space and invites hackers into these organizations to gather valuable informations such as classified company infos and banking accounts. Nir Kshetri explains this situation like (2016);

"More broadly, according to PwC, less than half of U.S. companies had taken enough precautions to protect consumer data. Only 38% had prioritized CS investments based on business risks they were facing, and only 31% had a CS strategy for the mobile sector. Likewise, 54% of the businesses did not provide CS training to employees. A survey conducted by CSO of over 500 private and public sector executives and security experts in the U.S. led to similar findings. Most organizations lacked a strategic approach to CS and had failed to adequately assess and understand supply chain risks. Most organizations were also found to have inadequate mobile device security. The report emphasized the importance of collaboration to share experience and knowledge of threats, strategic spending, especially on CS training for employees (p.92)."

So we can see that there is a "loophole" for cybercrimes against intutions in the USA like other countries. Especially when we look at the sectors of USA and think about how big they are, we can guess that any kind of attack on these sectors will causes nation-wide problem. For example, if we look at power sector of USA, we can say that any kind of terror attack can effect whole country. Attackers can shut down even electricity and leave many states without power until a solution. It also means that closing down many factories (because of the electricity shut down) any causes maybe millions of dollars in a short period of time. In addition to that, it also creates a nation-wide or state-wide security problem because of losing power at military bases. In November 2014, in his testimony before a Congressional panel,the head of the NSA and U.S. Cyber Command said that China and "one or two" other countries possess the ability to launch a cyber-attack that can take the entire U.S. power grid and other critical infrastructure down (Kshetri, 2016, p.92).

Situation in the financial sector is critical as well. If we remember Mortgage crisis which made domino effect and inevitably bringed a worldwide economic crisis, we can see the importance of security in that area. Multinational financial companies are not rare in USA. Any kind of hijacking of personal information of customers can lead millions (maybe billions) of dollars loss. It will not only stays with the instution or company which is victim. It will effect other firms as well like in the mortgage crisis. Even a small number of credit card frauds, can cause big impact. And nowadays, attacks on financial firms are increased. Nir Kshetri underlines this importance in his book like (2016);

"Cyber-treats facing the financial sector are an issue of critical importance. In his annual letters to shareholder in April 2014, JPMorgan CEO described hackers' efforts to attack the bank's computers were becoming "more frequent, sophisticated and dangerous". In a "worst case" scenario, in which cyber-attacks lead to a deletion of records, a drain of the account balances and freeze of networks, will produce shocks that will have a severe impact on the economy, which will be on the scale of the attacks of September 11, 2001 (p.93)."

Healthcare sector is another sector which we have to state. It is obvious that these firms has senstive datas which is like patients adresses, health reports, insurance datas and maybe medicine records. So, when an attacker attacks and gathers these information from these instutions he/she not only get the infos of thousends of patients also he/she will have financial insurance records. In USA cases which these informations has been stolen are not rare. In December 2013, cybercriminals accessed a server of Bryan, Texas-based St. Joseph Health System, which contained personal information of 400,000 current and former patients including SSNs, dates of birth, addresses and other medical information (Kshetri, 2016, p.93). These "rewards" draws attention of cyber criminals on this sectors. That's why healthcare sectors are growing target for cybercrime. Studies about this topic are justifies this. For example, a study of Ponemon Institute indicated that, the proportion of healthcare organizations reporting cyber-attacks increased from 20% in 2009 to 40% in 2013 (Kshetri, 2016, p.94). This sector also suffers from security issue like other sectors. Becuase of the main interest and investments occurs at financial and banking sectors, many health instutions and hospitals do not have the enough criteria on cyber security. Most of them lacks support and their systems are not developed well against cyber-attacks. Experts say that healthcare providers and hospitals have weak cyber-defense mechanisms. Some U.S. hospitals were reported to use Windows systems over 10 years old without a security patch. (Kshetri, 2016, p.95).

4. STATISTICS AND ANALYSIS

4.1 DATA

In order to examine the determinants of internet crimes in USA, statewise data for 50 U.S. States on population, GDP, Gini rate, identity theft complaints, fraud complaints, reported fraud losses, unemployment rate, internet usage, poverty rate, graduation rate (for population 25 and over), regular crimes (violent and property), reported cyber crimes and reported cyber crime losses were manually collected for 2009-2018 from ;

- Federal Bureau of Investigation Annual Internet Crime Reports accessed at ic3.gov
- Consumer Sentinel Network Annual Data Books accessed at ftc.gov
- United States Census Bureau Population Estimates accessed at census.gov
- State Population by Characteristics accessed at census.gov
- U.S. Department of Commerce, Bureau of Economic Analysis accessed at apps.bea.gov
- The Disaster Center State Crime Statistics accessed at disastercenter.com
- Criminal Watch Statistics accessed at criminalwatch.com
- Kids Count Data Center accessed at datacenter.kidscount.org

The log sheet of the data (which was done for examining datas at softwares) is like the below ;

Table 4.1 Index of Variables

Name	Explanation
cybercrime_per_pop	Number of cybercrime reports as a percentage of population
ln_cyberloss_by_gdp	Natural log of reported cybercrime loss as a fraction of gdp
fraud_per_pop	Number of fraud reports as a percentage of population
ln_fraudloss_by_gdp	Natural log of reported fraud loss as a fraction of gdp
idtheft_per_pop	Number of identity theft reports as a percentage of population
propcrime_per_pop	Number of property crimes as a percentage of population
violcrime_per_pop	Number of violent crimes as a percentage of population
ln_gdp	Natural log of GDP (in millions of dollars)
ln_pop	Natural log of population
gdp_per_cap	Per-capita GDP (in millions of dollars)
internet_usage	Percentage of households with internet access
graduate_rate_25_	Percentage of population over 25 with a college degree or higher
income_inequality	Gini coefficient
poverty	Percentage of individuals in poverty
unemployment_rate	Percentage of unemployed in labor force
pop_perc_40_50	Percentage of population in age-group 40-50
pop_perc_50_60	Percentage of population in age-group 50-60
Pop_perc_60	Percentage of population 60 and above

4.2 GENERAL STATISTICS

Despite all of the prevention techniques, according to Internet Crime Report which releases every year, there is visible increase in every aspect of cybercrime statistics in USA. According to data

of financial loss by years, we can see that there is a regular increase in every year. Also we can see that 2018's variable is over 5 times than 2012. It means that, if the numbers are going to continue their increase, it will cause much more losses at 2020's.

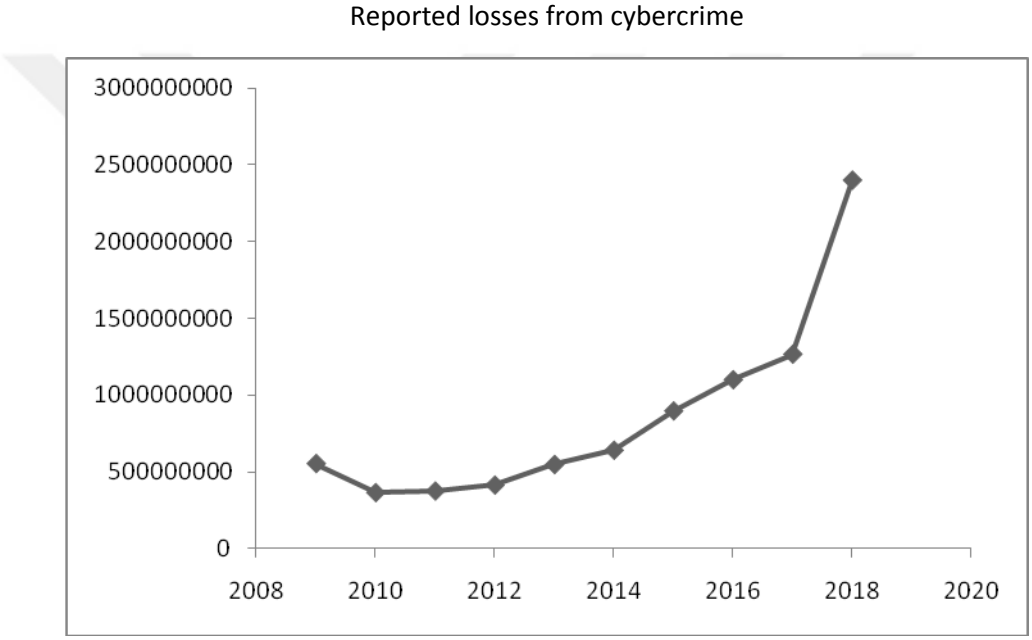


Figure 4.1 Reported losses from cybercrime

There is also an increase at number of victims by years except between 2012-2013. We can say that every year, attacks harm more people and in parallel of this, losses will much more higher. Since 2013 to 2018, victim numbers are increased more than 100,000.

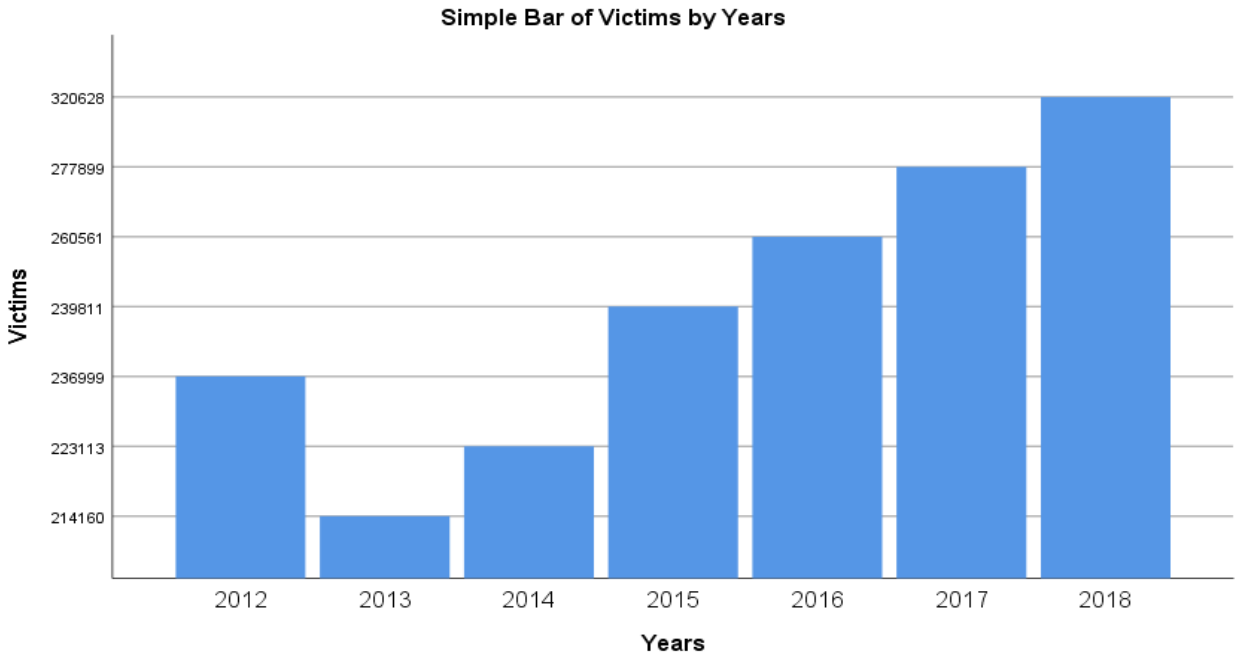


Figure 4.2 Simple Bar of Victims by years

Another interesting statistic which examines organizations more closely. As we can see, there is also a regular increase on the data breaches and its costs.

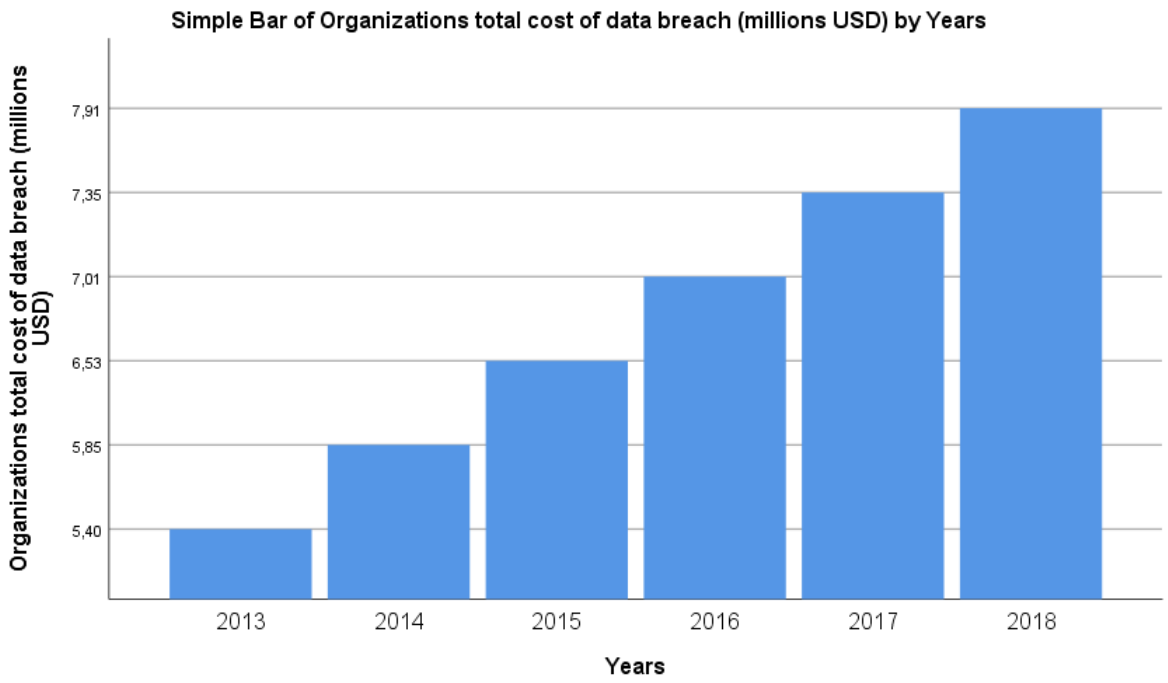


Figure 4.3 Simple bar of organizations total cost of data breach (millions USD) by Years

Another interesting variable is that the per capita cost of data breach by years. Like in the other statistics, there is also a regular increase in this stat too.

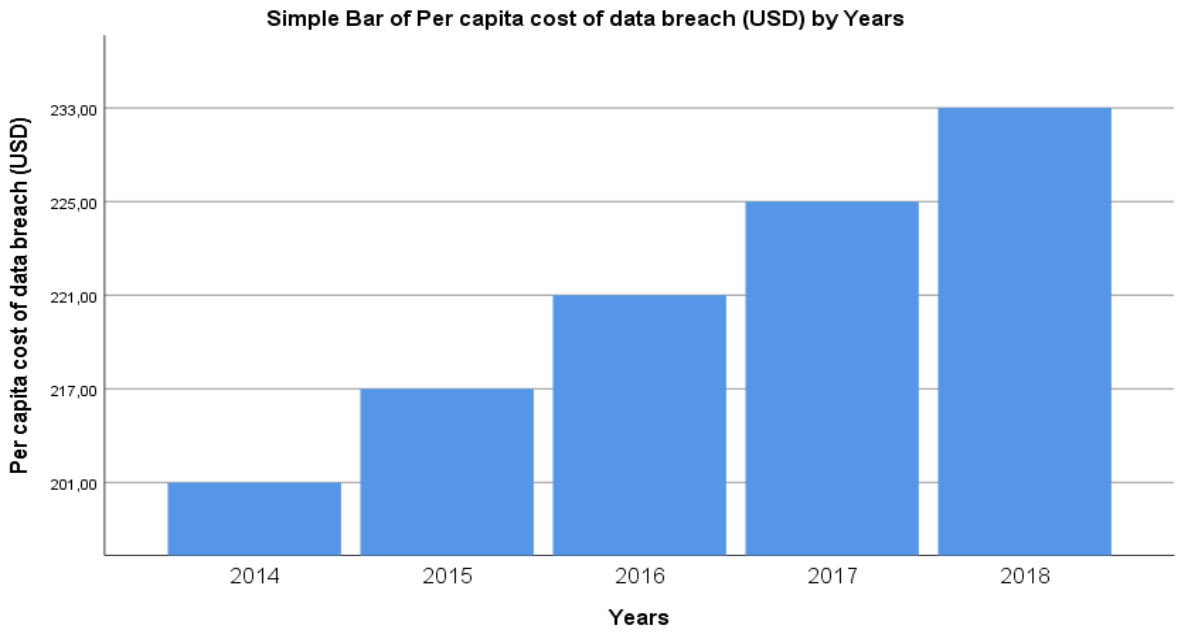


Figure 4.4 Simple Bar of per capita cost of data breach (USA) by Years

According to all of these statistics we can say that there is a significant rise on the numbers. Despite the measures taken by the government, it is worrying for the USA that these numbers increase regularly every year. As I mentioned before, if the numbers continue to increase in this way, it is inevitable that the losses will be higher in the 2020s. In addition to these figures, there are another figures which I like show in order to make it understandable for further analysis are like;

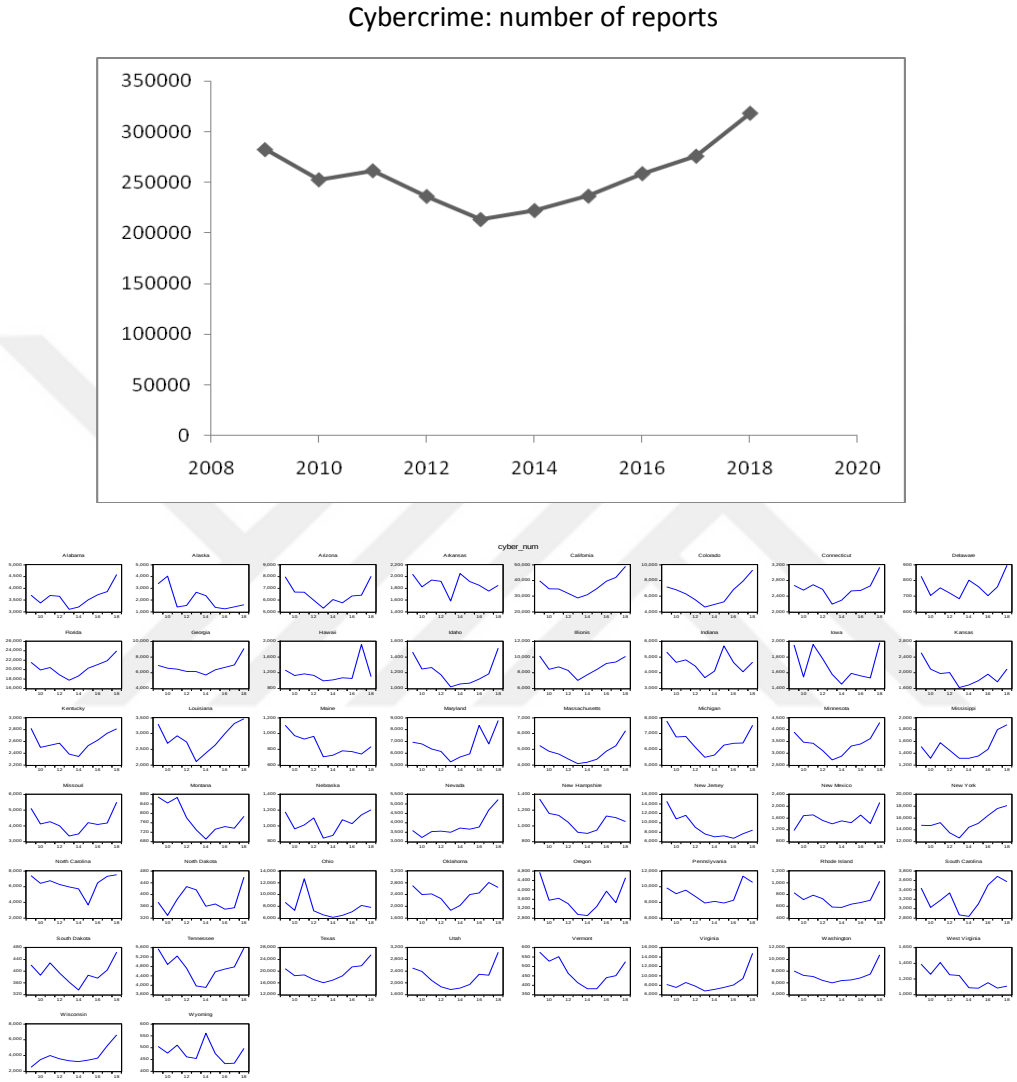


Figure 4.5 Number of Reported Cyber crime reports of USA and per state

Fraud: number of reports

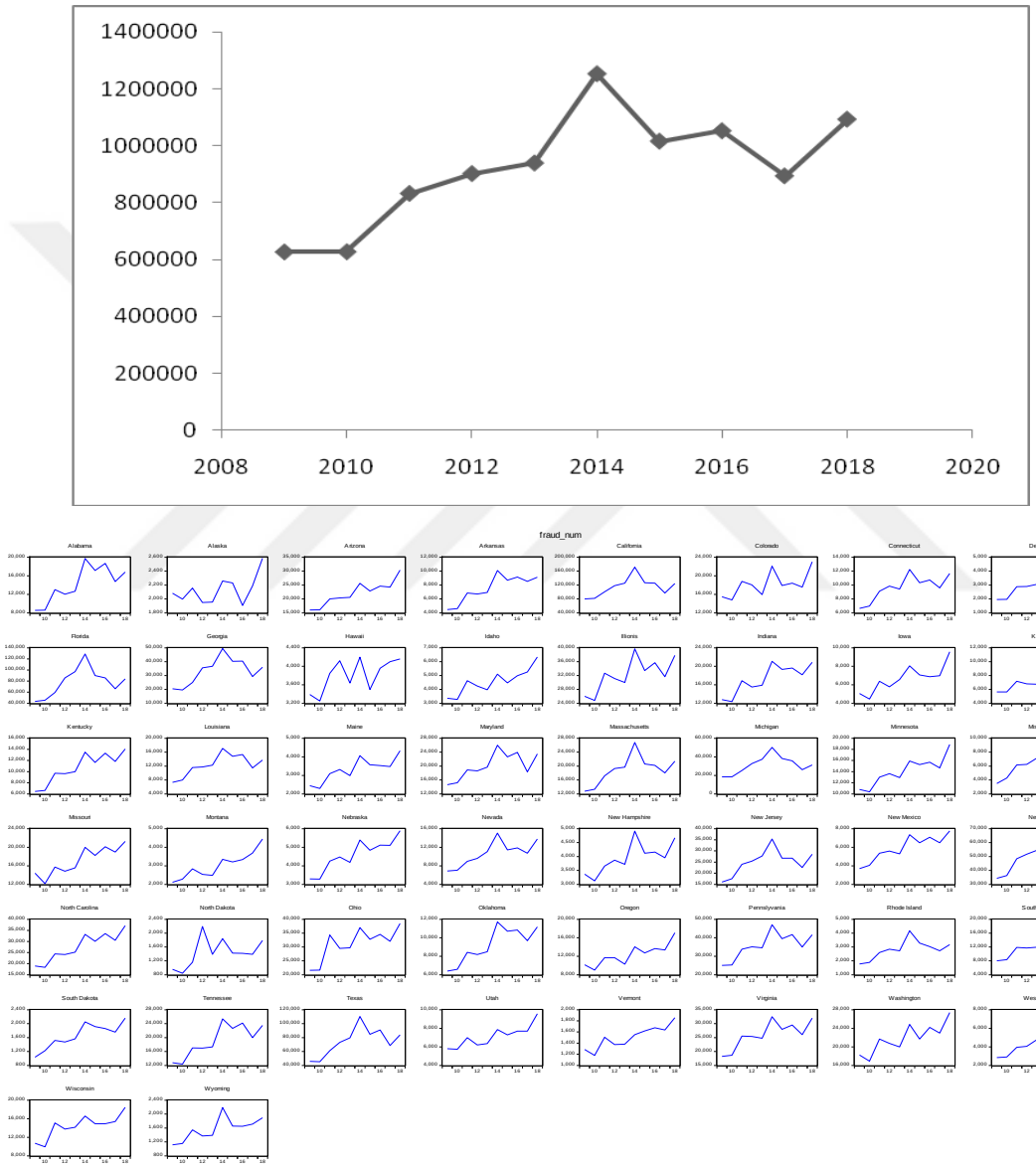
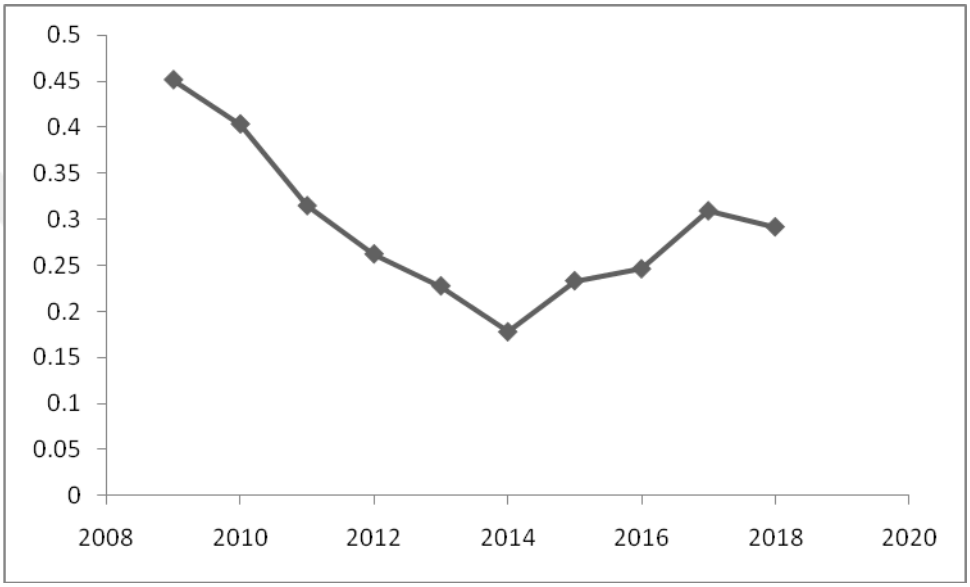


Figure 4.6 Number of reported fraud USA and per state

Ratio of number of cybercrime reports to number of fraud reports



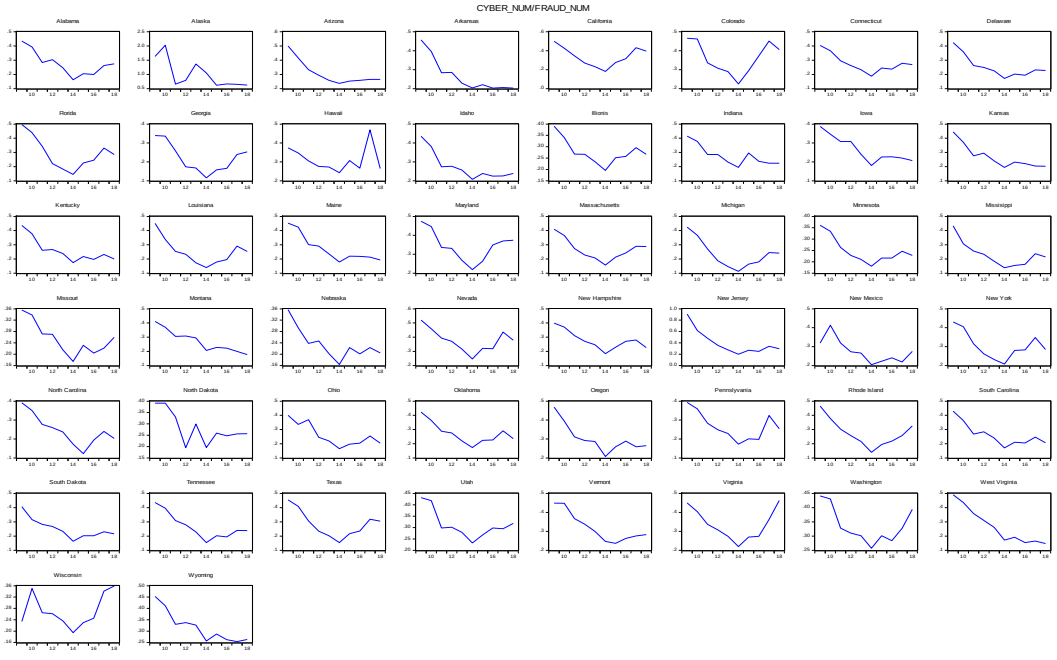


Figure 4.7 Ratio number of cybercrime reports to number of fraud reports for USA and per state

Population

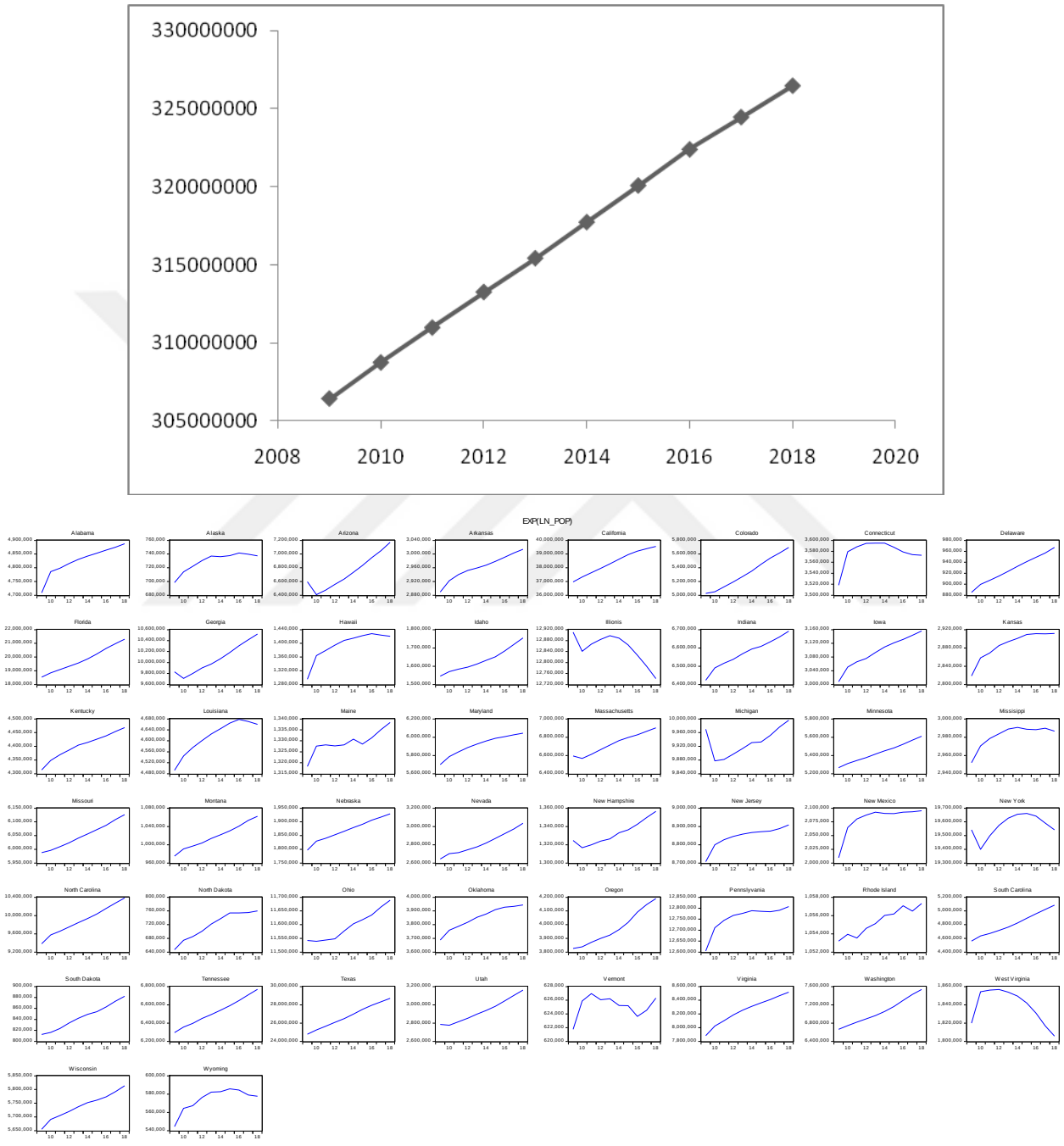
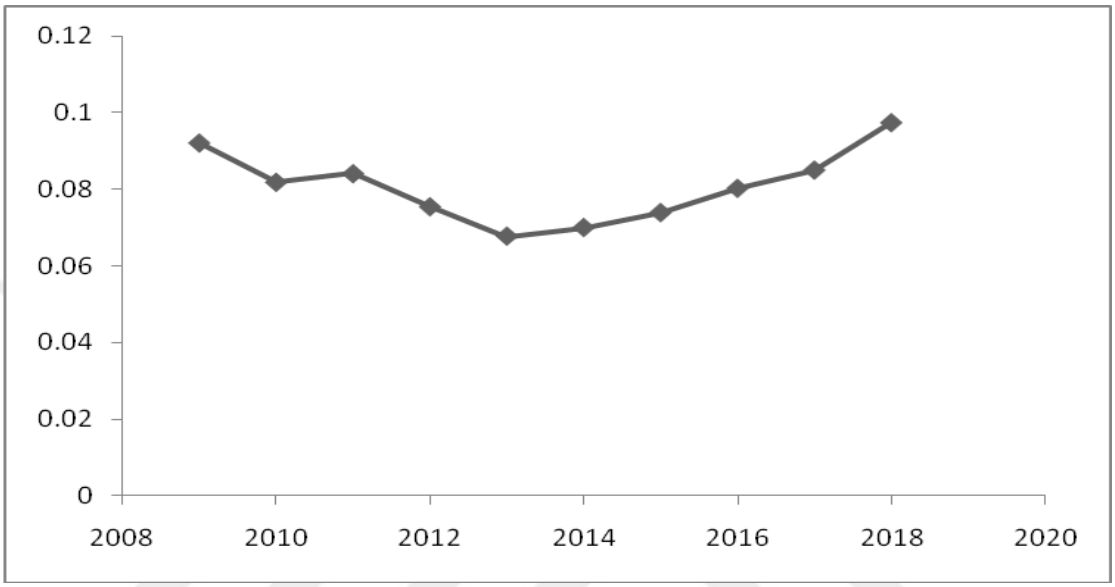


Figure 4.8 Population of USA and per state

Cybercrime per population



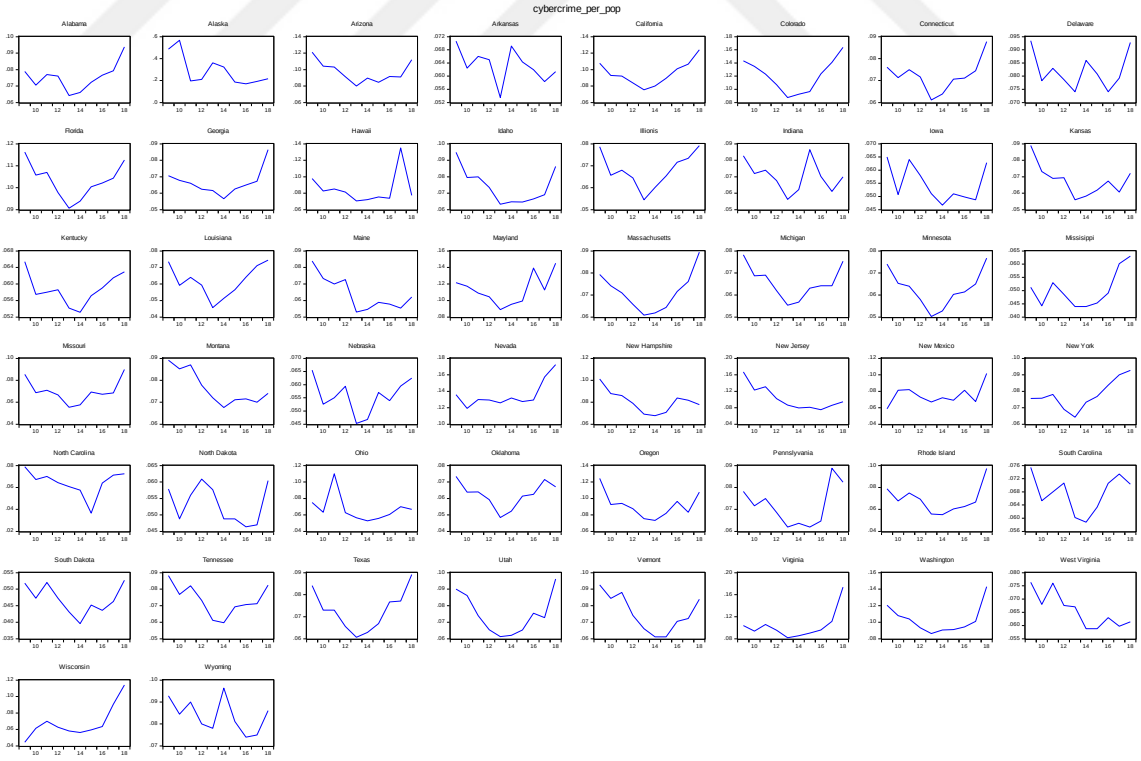


Figure 4.9 Cybercrime per population for USA and per state

Fraud Per Population

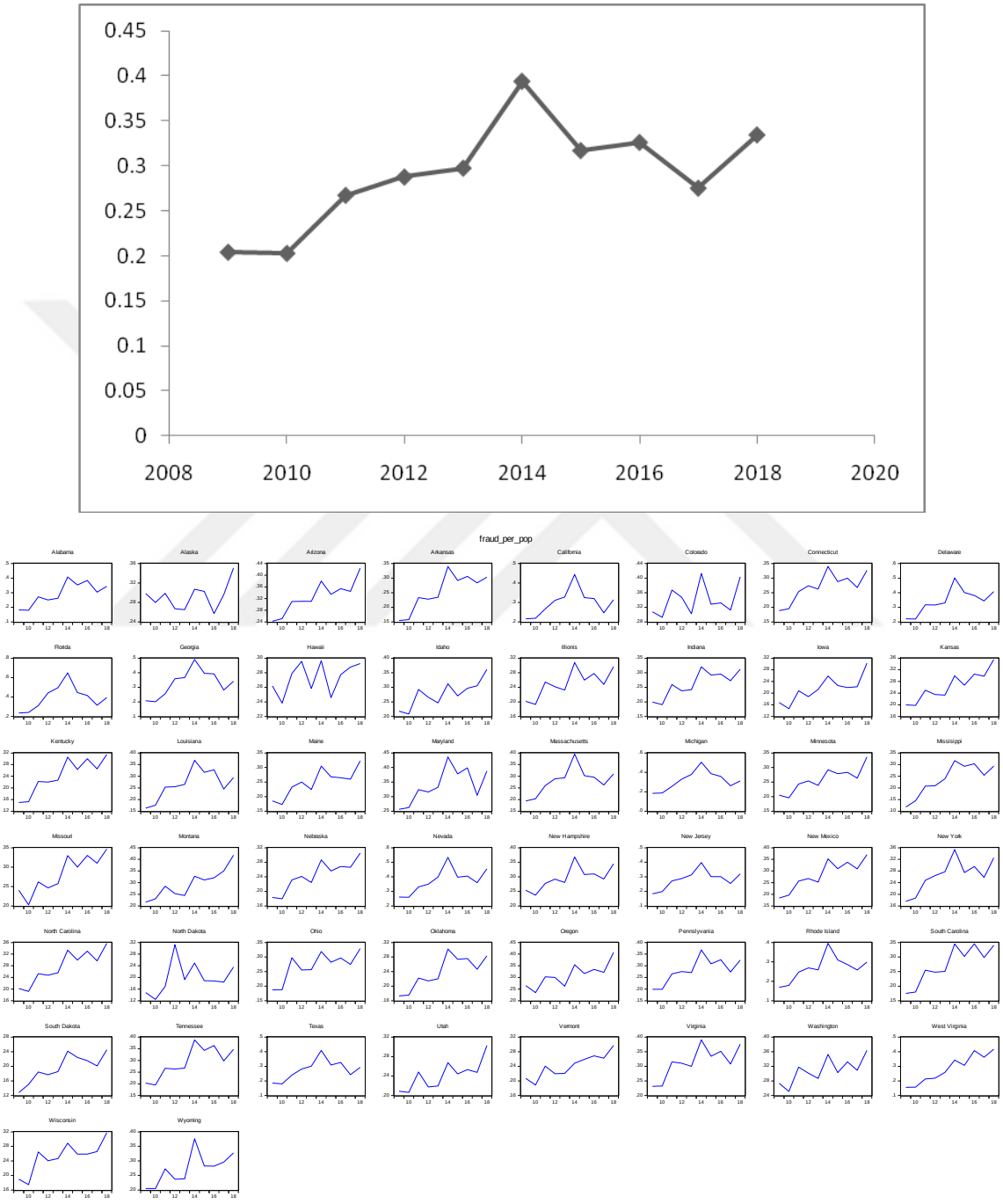


Figure 4.10 Fraud per population for USA and per state

Reported fraud losses

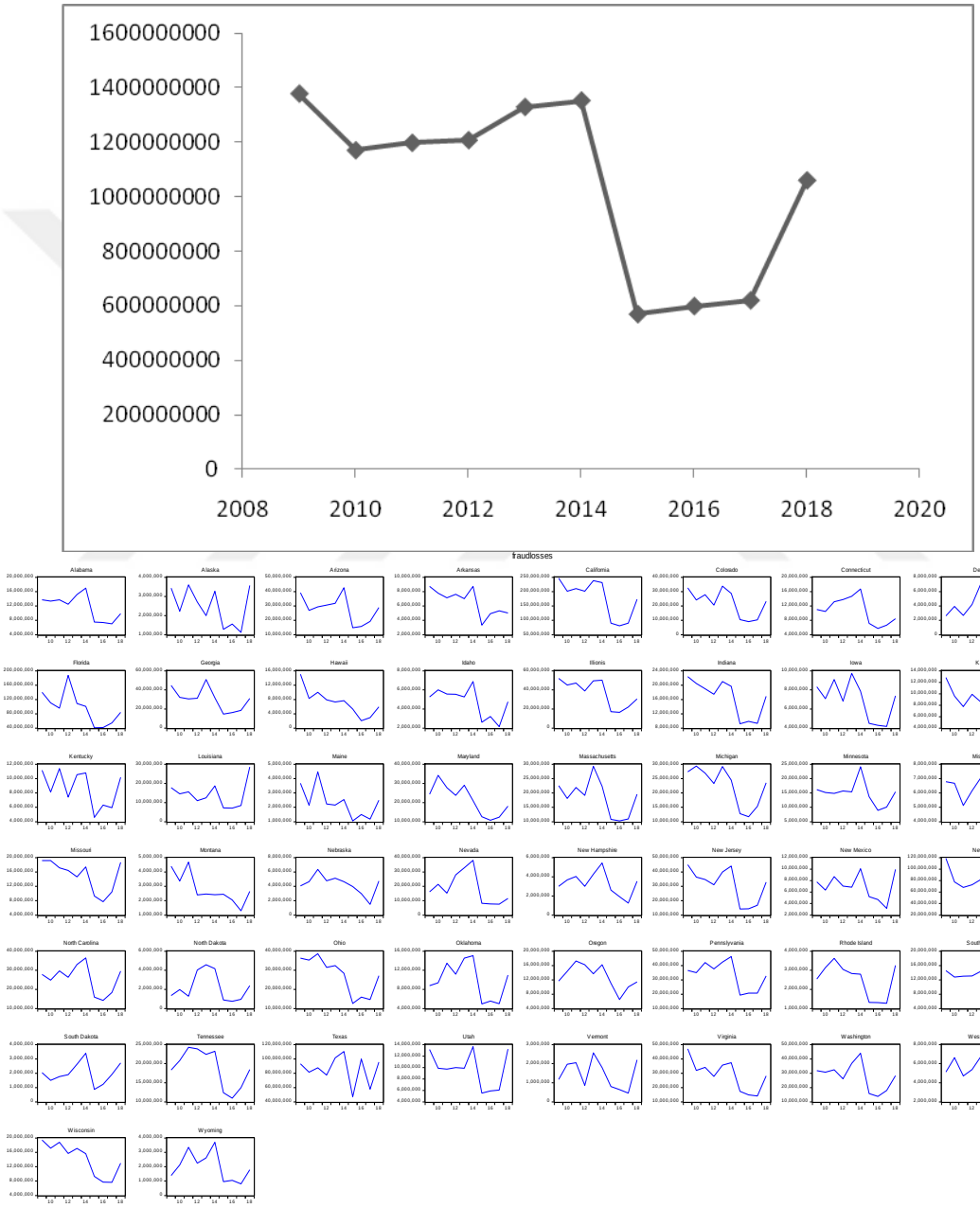


Figure 4.11 Reported fraud losses for USA and per state

Ratio of reported cybercrime losses to reported fraud losses

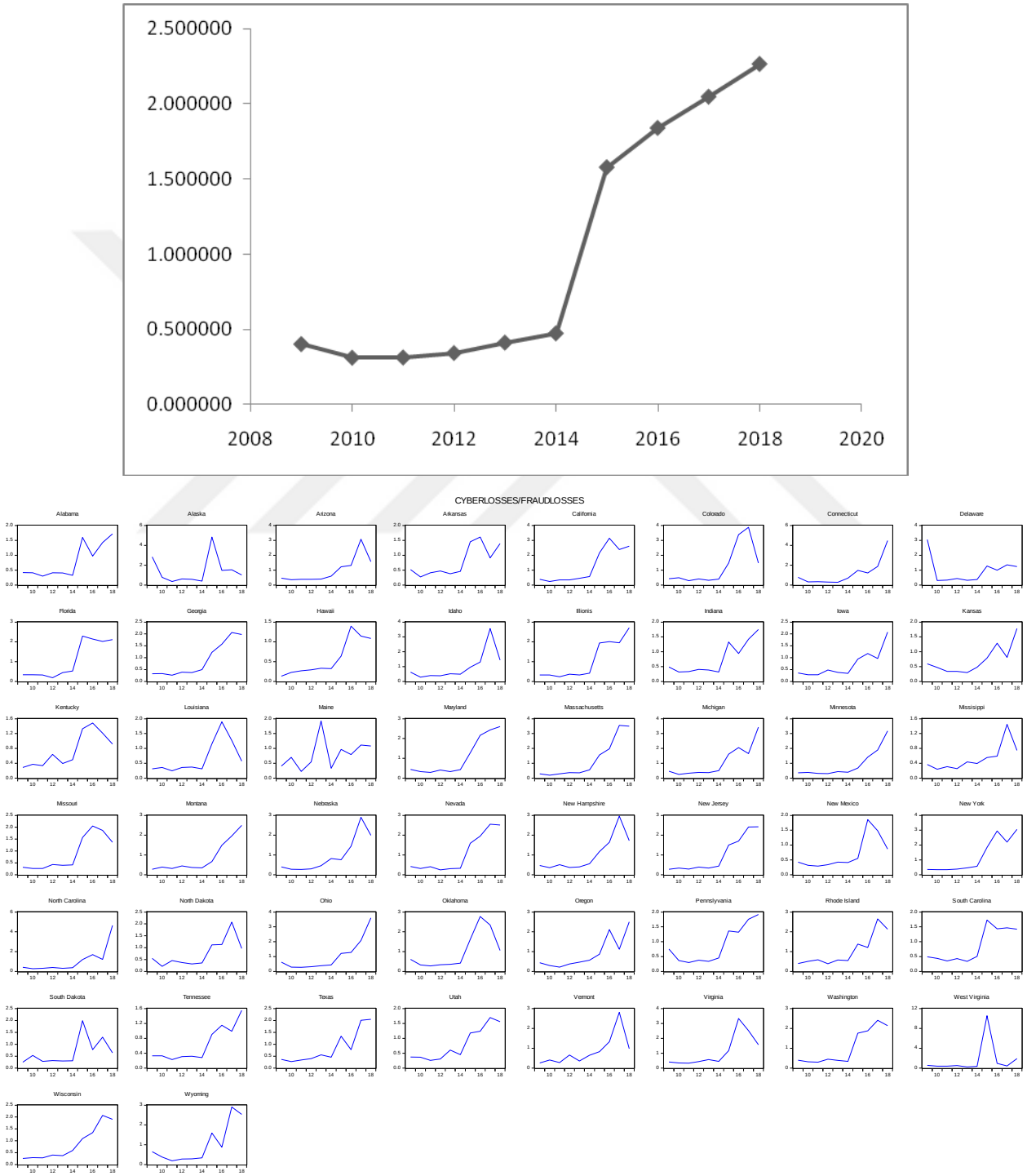
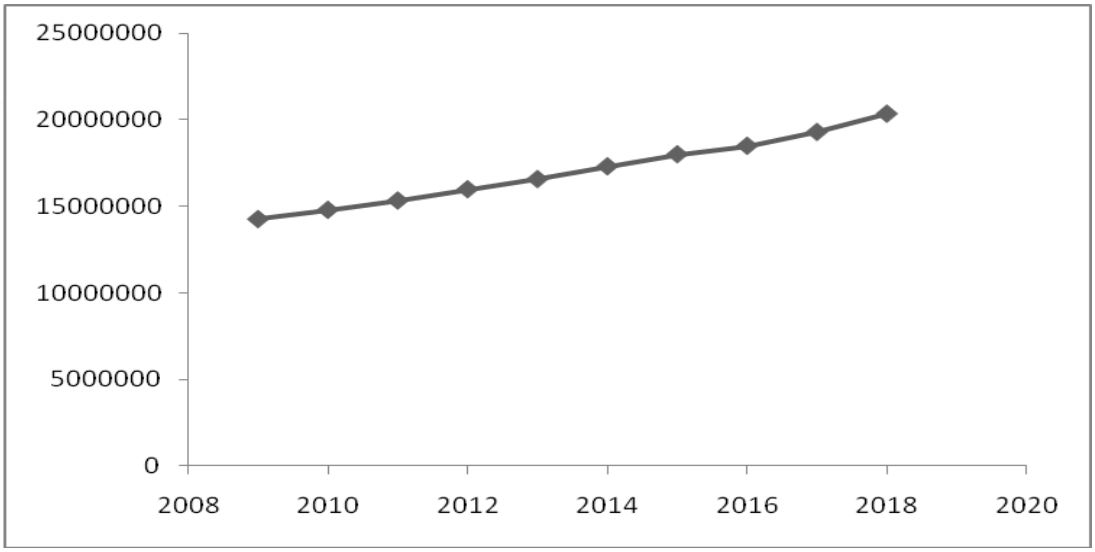


Figure 4.12 Ratio of reported cybercrime losses to reported fraud losses for USA and per state

GDP (Millions of US Dollars)



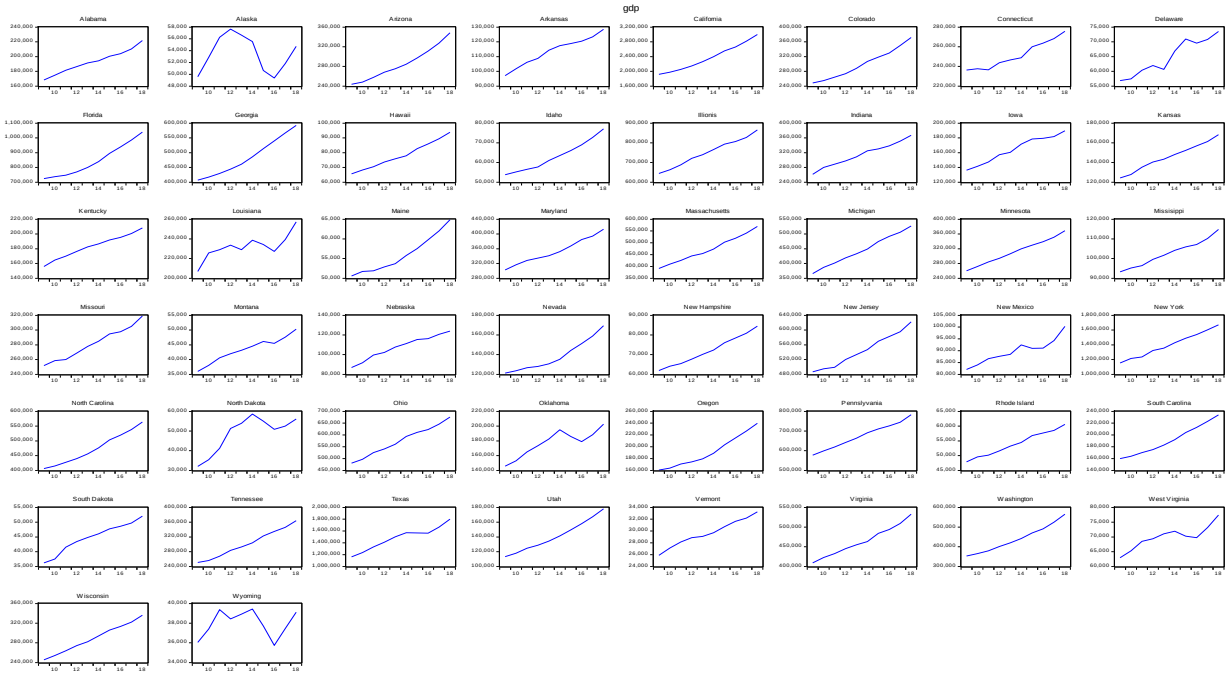
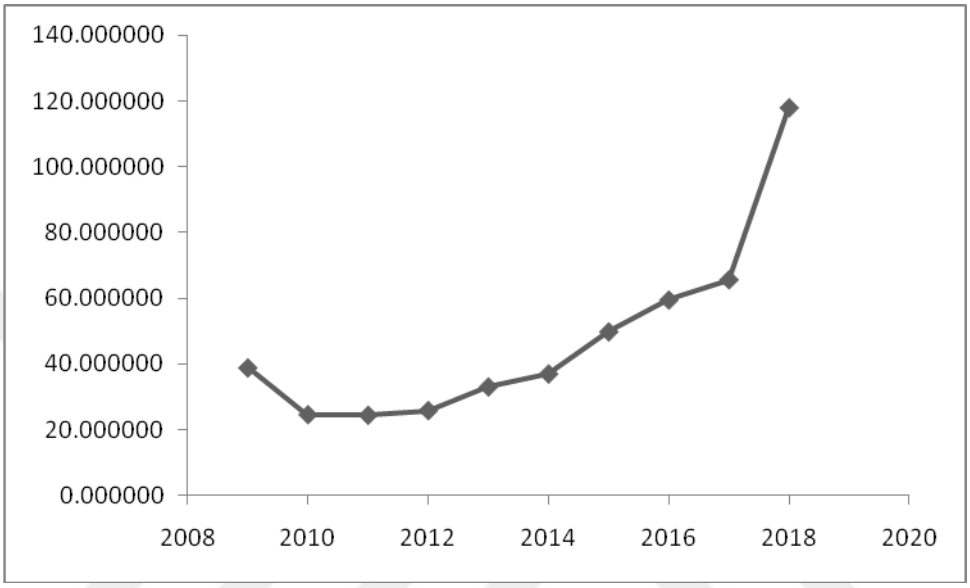


Figure 4.13 GDP for USA and per state

Reported cybercrime losses relative to GDP ($x10^6$)



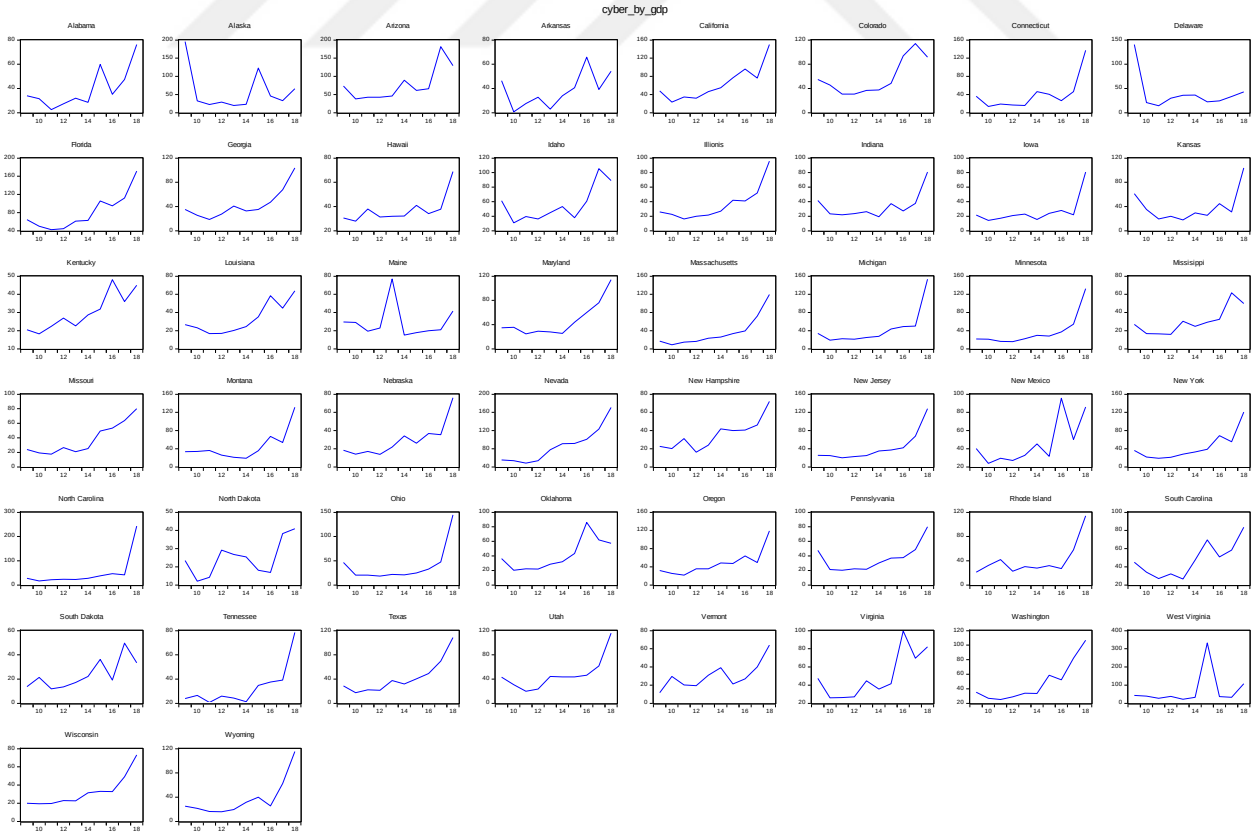


Figure 4.14 Reported cybercrime losses relative to GDP ($x10^6$) for USA and per state

Reported fraud losses relative to GDP (x10^6)

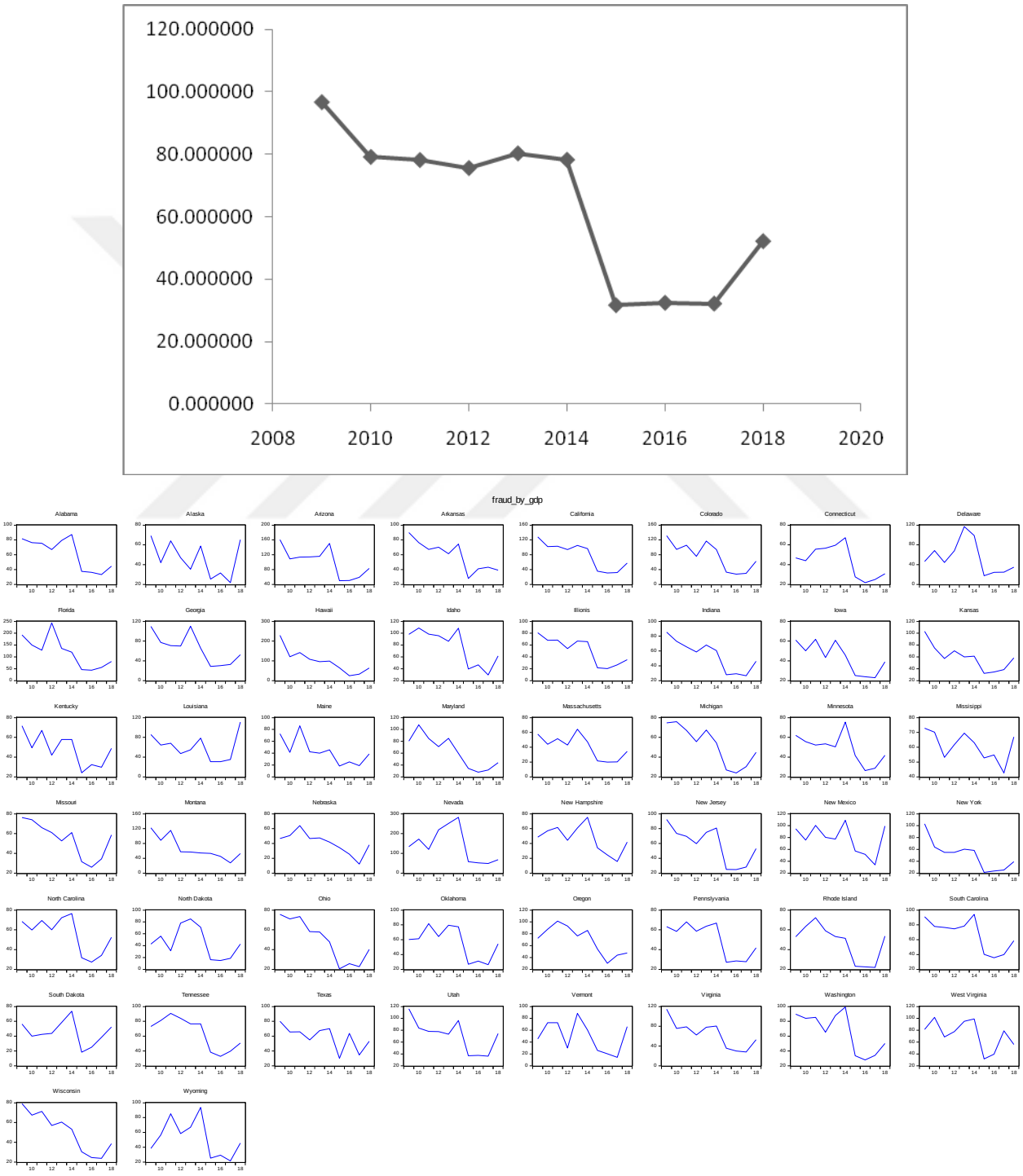


Figure 4.15 Reported fraud losses relative to GDP (x10^6)

4.3 ANALYSIS

Overall covariance results for the pooled sample shown in Table 4.2 would suggest at most moderate correlation between the crime types, the maximum being 0.54 for property crimes and violent crimes. However we cannot draw inferences for a panel dataset based on pooled covariance. The same holds for cross-sectional covariance by year which is also in the same table for completeness. It is important to conduct a panel regression for such data. The graph of correlation of cybercrime reports with other types is in Figure 4.15.

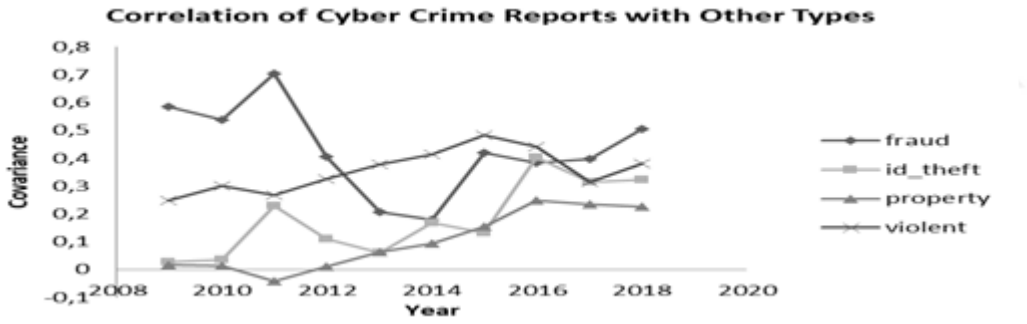
Table 4.2 Covariance of cybercrime reports with other crime types

	Entire Sample				
	CYBERCRIME_PER_POP	FRAUD_PER_POP	IDTHEFT_PER_POP	PROPCRIME_PER_POP	VIOLCRIME_PER_POP
CYBERCRIME_PER_POP	1	0.179675613	0.084173648	0.080180511	0.315893326
FRAUD_PER_POP	0.179675613	1	0.499153455	-0.078152115	0.199200718
IDTHEFT_PER_POP	0.084173648	0.499153455	1	0.029419882	0.282195189
PROPCRIME_PER_POP	0.080180511	-0.078152115	0.029419882	1	0.541699129
VIOLCRIME_PER_POP	0.315893326	0.199200718	0.282195189	0.541699129	1

Covariance of cyber crime reports with other types				
Year	Fraud	Identity Theft	Property Crime	Violent Crime
2009	0,58476976	0,026397367	0,016273348	0,246798601
2010	0,53873665	0,034464127	0,012510734	0,30097964
2011	0,70419228	0,228753467	-0,042692819	0,268236668

2012	0,40624621	0,109148909	0,010538975	0,32630865
2013	0,20749594	0,060076521	0,061550336	0,376819726
2014	0,17989845	0,168929953	0,092736397	0,413715195
2015	0,41855828	0,132191323	0,153243503	0,481319771
2016	0,38223361	0,40164393	0,248328714	0,441097254
2017	0,39567651	0,314927844	0,234439412	0,314612307
2018	0,50347915	0,321637614	0,22663548	0,381503284

Figure 4.16 Correlation of cybercrime reports with other types of crime



According to correlation test which is for covariance of cybercrime loss per GDP with fraud loss per GDP, we see that the relationship is not constant over years, and has been decreasing over time.

Covariance of cyber crime loss per GDP with fraud loss per GDP		
Year	Fraud Loss	
2009	0,391739	
2010	0,695133	
2011	0,773391	

2012	0,773245	
2013	0,598145	
2014	0,774039	
2015	0,342199	
2016	0,526992	
2017	0,366267	
2018	0,079246	

Table 4.3 Covariance of cybercrime loss per GDP with fraud loss per GDP

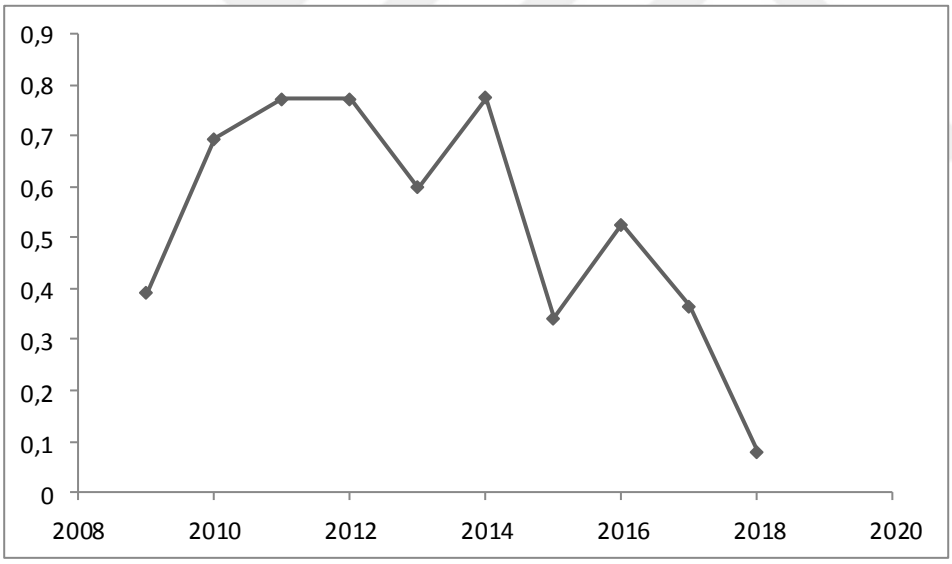


Figure 4.17 Correlation of cybercrime loss per GDP with fraud loss per GDP

As long as the database has 50 states' data for a 10 period of time, in order to find the statistically significant determinants for each crime type, I did panel least squres tests. At the table 4.4, we can see the results of cybercrime per population's relation with the other variables. We see that

GDP per capita, internet usage, and poverty, all have a statistically significant effect on cybercrime reports as a percentage of the state's population. The coefficients for these variables are all positive.

Table 4.4 Panel Least Squares Test #1

Dependent Variable: CYBERCRIME_PER_POP
Method: Panel Least Squares
Date: 01/21/20 Time: 23:23
Sample: 2009 2018
Periods included: 10
Cross-sections included: 50
Total panel (balanced) observations: 500
Period weights (PCSE) standard errors & covariance (d.f. corrected)

Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	-0,481330	1,299599	-0,370368	0,7113
GDP_PER_CAP	2,135284	0,570088	3,745533	0,0002
GRADUATE_RATE_25_	0,001225	0,004645	0,263805	0,7921
INCOME_INEQUALITY	-0,019403	0,224784	-0,086320	0,9313
INTERNET_USAGE	0,131861	0,046006	2,866196	0,0044
LN_POP	0,015461	0,083324	0,185558	0,8529
POP_PERC_40_50	0,612589	0,495877	1,235365	0,2174
POP_PERC_50_60	0,634107	0,489196	1,296222	0,1956
POP_PERC_60_	-0,573287	0,459191	-1,248471	0,2125
POVERTY	0,004363	0,002145	2,033552	0,0426
UNEMPLOYMENT_RATE	-0,002842	0,001726	-1,646878	0,1003

Effects Specification

Cross-section fixed (dummy variables)
Period fixed (dummy variables)

R-squared	0,790347	Mean dependent var	0,080503
Adjusted R-squared	0,757269	S.D. dependent var	0,041467
S.E. of regression	0,02043	Akaike info criterion	-4,81615
Sum squared resid	0,179889	Schwarz criterion	-4,23453
Log likelihood	1273,037	Hannan-Quinn criter.	-4,58792
F-statistic	23,89375	Durbin-Watson stat	1,400741
Prob(F-statistic)	0		

At the table of 4.5, we can see the results of fraud per population relation with other variables, only the population, used here as a natural logarithm has a significant negative effect on fraud reports. The percentage of the population between 40-50 as well as betwen 50-60 also have a significant positive effect.

Table 4.5 Panel Least Squares Test #2

Dependent Variable: FRAUD_PER_POP
Method: Panel Least Squares
Date: 01/22/20 Time: 15:29
Sample: 2009 2018
Periods included: 10
Cross-sections included: 50
Total panel (balanced) observations: 500
Period weights (PCSE) standard errors & covariance (d.f. corrected)

Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	4,939051	1,585706	3,114733	0,0020
GDP_PER_CAP	-0,672168	0,774408	-0,867977	0,3859
GRADUATE_RATE_25_	-0,003048	0,005873	-0,518902	0,6041
INCOME_INEQUALITY	0,075014	0,326106	0,230030	0,8182
INTERNET_USAGE	0,079934	0,065042	1,228961	0,2198
LN_POP	-0,343461	0,101861	-3,371862	0,0008
POP_PERC_40_50	2,574222	0,611968	4,206462	0,0000
POP_PERC_50_60	1,128527	0,564998	1,997400	0,0464
POP_PERC_60_	0,327883	0,556540	0,589146	0,5561
POVERTY	0,001714	0,002274	0,753577	0,4515
UNEMPLOYMENT_RATE	-0,000128	0,002084	-0,061624	0,9509

Effects Specification

Cross-section fixed (dummy variables)
Period fixed (dummy variables)

R-squared	0,836299	Mean dependent var	0,279875
Adjusted R-squared	0,810471	S.D. dependent var	0,068945
S.E. of regression	0,030015	Akaike info criterion	-4,046723
Sum squared resid	0,388294	Schwarz criterion	-3,465107

Log likelihood	1080,681	Hannan-Quinn criter.	-3,818498
F-statistic	32,38007	Durbin-Watson stat	0,961914
Prob(F-statistic)	0		

At the table of 4.6, we can see the results of identity theft relation with other variables. The significant factors here are the percentage of population between 40 and 50 years, as well as the unemployment rate. Coefficients for both these factors are negative.

Table 4.6 Panel Least Square Test #3

Dependent Variable: IDTHEFT_PER_POP
Method: Panel Least Squares
Date: 01/22/20 Time: 16:10
Sample: 2009 2018
Periods included: 10
Cross-sections included: 50
Total panel (balanced) observations: 500
Period weights (PCSE) standard errors & covariance (d.f. corrected)

Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	-1,337724	0,930156	-1,438172	0,1511
GDP_PER_CAP	-0,055822	0,469663	-0,118855	0,9054
GRADUATE_RATE_25_	0,001289	0,003651	0,353156	0,7241
INCOME_INEQUALITY	0,017331	0,206442	0,083951	0,9331
INTERNET_USAGE	-0,013724	0,044861	-0,305915	0,7598
LN_POP	0,093187	0,060325	1,544734	0,1231
POP_PERC_40_50	-0,926914	0,371564	-2,494625	0,0130
POP_PERC_50_60	0,491620	0,325821	1,508864	0,1321
POP_PERC_60_	0,170847	0,342209	0,499248	0,6179
POVERTY	0,000847	0,001368	0,619060	0,5362
UNEMPLOYMENT_RATE	-0,003076	0,001242	-2,477587	0,0136

Effects Specification

Cross-section fixed (dummy variables)
Period fixed (dummy variables)

R-squared	0,757631	Mean dependent var	0,084342
Adjusted R-squared	0,719392	S.D. dependent var	0,037502
S.E. of regression	0,019866	Akaike info criterion	-4,87212
Sum squared resid	0,170097	Schwarz criterion	-4,2905
Log likelihood	1287,03	Hannan-Quinn criter.	-4,64389
F-statistic	19,81298	Durbin-Watson stat	1,620982
Prob(F-statistic)	0		

At the table of 4.7, we can see the results of property per crime's relation with other variables. The relevant factors here include the percentage of people with a college degree, internet usage, the percentage of population between 50 and 60, and the unemployment rate. Except for the last factor, all other coefficients are negative.

Table 4.7 Panel Least Square Test #4

Dependent Variable: PROPCRIME_PER_POP
Method: Panel Least Squares
Date: 02/02/20 Time: 05:33
Sample: 2009 2018
Periods included: 10
Cross-sections included: 50
Total panel (balanced) observations: 500
Period weights (PCSE) standard errors & covariance (d.f. corrected)

Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	17,24328	9,822646	1,755462	0,0799
GDP_PER_CAP	5,253574	4,135419	1,270385	0,2046
GRADUATE_RATE_25_	-0,222405	0,035162	-6,325103	0
INCOME_INEQUALITY	-2,160121	1,626675	-1,327936	0,1849
INTERNET_USAGE	-0,746039	0,348349	-2,141646	0,0328
LN_POP	-0,171089	0,629697	-0,2717	0,786
POP_PERC_40_50	1,739804	3,683676	0,472301	0,637
POP_PERC_50_60	-27,09968	3,430208	-7,900302	0
POP_PERC_60_	-5,51415	3,371328	-1,635602	0,1027
POVERTY	0,009659	0,012532	0,77074	0,4413
UNEMPLOYMENT_RATE	0,021615	0,011775	1,835641	0,0671

R-squared	0.950575
Adjusted R-squared	0.942777
S.E. of regression	0.150556

Sum squared resid	9,769494
Log likelihood	274,3666
F-statistic 121.9002	121,9002
Prob(F-statistic) 0	0

At the table of 4.8, we can see the results of violent crime per populations relation with other variables. Similar factors are significant here as for property crime, except that in addition income inequality has a marginally significant negative effect; there is no statistically significant impact of internet usage; a positive impact of the percentage of population between 40 and 50; and poverty rate has a marginally significant negative effect.

Table 4.8 Panel Least Squares #5

Dependent Variable: VIOLCRIME_PER_POP
Method: Panel Least Squares
Date: 01/22/20 Time: 19:37
Sample: 2009 2018
Periods included: 10
Cross-sections included: 50
Total panel (balanced) observations: 500
Period weights (PCSE) standard errors & covariance (d.f. corrected)

Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	7,790224	2,151962	3,620056	0,0003
GDP_PER_CAP	-0,701755	0,890994	-0,787609	0,4314
GRADUATE_RATE_25_	-0,015183	0,007866	-1,930174	0,0542
INCOME_INEQUALITY	-0,706970	0,347818	-2,032585	0,0427
INTERNET_USAGE	0,000664	0,072338	0,009186	0,9927
LN_POP	-0,418481	0,138378	-3,024181	0,0026
POP_PERC_40_50	1,381531	0,803672	1,719024	0,0863
POP_PERC_50_60	-4,561731	0,735002	-6,206418	0,0000
POP_PERC_60_	0,933426	0,728517	1,281269	0,2008
POVERTY	-0,004952	0,002621	-1,889365	0,0595
UNEMPLOYMENT_RATE	0,007782	0,002497	3,116316	0,0020

Effects Specification			
Cross-section fixed (dummy variables)			
Period fixed (dummy variables)			
R-squared	0,955601	Mean dependent var	0,364529
Adjusted R-squared	0,948596	S.D. dependent var	0,140007
S.E. of regression	0,031743	Akaike info criterion	-3,9348
Sum squared resid	0,434281	Schwarz criterion	-3,35318
Log likelihood	1052,699	Hannan-Quinn criter.	-3,70657
F-statistic	136,4192	Durbin-Watson stat	0,691522
Prob(F-statistic)	0		

At the table of 4.9, we can see the results of cyberlosses per GDP's relation with other variables.

Table 4.9 Panel Least Squares #6

Dependent Variable: LN_CYBERLOSS_BY_GDP
Method: Panel Least Squares
Date: 01/23/20 Time: 00:36
Sample: 2009 2018
Periods included: 10
Cross-sections included: 50
Total panel (balanced) observations: 500
Period weights (PCSE) standard errors & covariance (d.f. corrected)

Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	15,89638	11,49099	1,383379	0,1673
GDP_PER_CAP	38,75551	16,49398	2,349675	0,0192
GRADUATE_RATE_25_	0,144019	0,06565	2,193727	0,0288
INCOME_INEQUALITY	0,614451	3,248019	0,189177	0,8500
INTERNET_USAGE	0,806928	0,715336	1,128041	0,2599
LN_GDP	-2,544974	0,950596	-2,677242	0,0077
POP_PERC_40_50	7,353009	7,209771	1,019867	0,3084

POP_PERC_50_60	0,666842	6,582468	0,101306	0,9194
POP_PERC_60_	-12,74155	6,444759	-1,977041	0,0487
POVERTY	-0,021123	0,024333	-0,868093	0,3858
UNEMPLOYMENT_RATE	-0,030686	0,023891	-1,28442	0,1997

Effects Specification

Cross-section fixed (dummy variables)
Period fixed (dummy variables)

R-squared	0,748953	Mean dependent var	-10,23088
Adjusted R-squared	0,709345	S.D. dependent var	0,572655
S.E. of regression	0,308732	Akaike info criterion	0,614814
Sum squared resid	41,08098	Schwarz criterion	1,19643
Log likelihood	-84,70357	Hannan-Quinn criter.	0,843039
F-statistic	18,90899	Durbin-Watson stat	1,864523
Prob(F-statistic)	0		

At the table of 4.10, we can see that none of the factors provided a significant coefficient for fraud loss.

Table 4.10 Panel Least Squares #7

Dependent Variable: LN_FRAUDLOSS_BY_GDP
Method: Panel Least Squares
Date: 01/23/20 Time: 00:43
Sample: 2009 2018
Periods included: 10
Cross-sections included: 50
Total panel (balanced) observations: 500
Period weights (PCSE) standard errors & covariance (d.f. corrected)

Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	-0,180322	7,632708	-0,023625	0,9812
GDP_PER_CAP	0,495259	11,01555	0,04496	0,9642
GRADUATE_RATE_25_	-0,04345	0,042471	-1,023053	0,3069
INCOME_INEQUALITY	-2,08559	2,252123	-0,926055	0,3549

INTERNET_USAGE	0,51148	0,496998	1,029139	0,3040
LN_GDP	-0,619293	0,62976	-0,983379	0,3260
POP_PERC_40_50	1,443799	4,665797	0,309443	0,7571
POP_PERC_50_60	-1,074052	4,272315	-0,251398	0,8016
POP_PERC_60_	-2,695815	4,179095	-0,645071	0,5192
POVERTY	0,005022	0,015772	0,318386	0,7503
UNEMPLOYMENT_RATE	0,024443	0,015702	1,556648	0,1203

Effects Specification

Cross-section fixed (dummy variables)
Period fixed (dummy variables)

R-squared	0,847029	Mean dependent var	-9,8254
Adjusted R-squared	0,822894	S.D. dependent var	0,510962
S.E. of regression	0,215033	Akaike info criterion	-0,10855
Sum squared resid	19,92911	Schwarz criterion	0,473066
Log likelihood	96,13743	Hannan-Quinn criter.	0,119675
F-statistic	35,09586	Durbin-Watson stat	1,876015
Prob(F-statistic)	0		

5. CONCLUSION

Our data confirms that cybercrime is an increasing problem, but the issue, in terms of complaints to IC3, is rising costs of cybercrime rather than just the number of incidents. Macroeconomic and demographic factors have been studied in terms of their impact on various crime types. Our results show that cybercrime rates as well as losses are impacted by macroeconomic and demographic factors as well. However in terms of specific significant factors, cybercrime incidents are impacted by per-capita GDP and internet usage as well as poverty. In contrast, incidents of fraud are more related to demographic factors such as population and its age distribution. The only other crime type for which internet usage was relevant was property crimes. GDP per-capita was not relevant to other crime types. We also find that while macroeconomic and, to an extent demographic factors inluence the losses reported due to cybercrime, such factors were not significant for fraud in general. This suggests that response strategies for cybercrime may need to be different from those for other crime types. The case of fraud losses is interesting as the data shows irregular trends, and results show none of the factors to be significant. This could be due to the limitations of the data sample, in terms of limited time periods.

REFERENCES

Adeta, A., & Okeshola, F. (2013, September 9). The Nature, Causes and Consequences of Cyber Crime in Tertiary Institutions in. *American International Journal of Contemporary Research*, s. 98-114.

Britz, M. T. (2013). *Computer Forensics and Cyber Crime.* Pearson.

Eleanor Lockley, B. A. (2014). *Cyber Crime and Cyber Terrosim Investigator's Handbook.* Massachusetts: Elsevier.

FBI. (2017). *Internet Crime Report .* FBI.

Ghernauti, S. (2013). *Cyber Power : Crime, Conflict and Security in Cyberspace.* Lausenne: EPFL Press.

Kshetri, N. (2010). Diffusion and Effects of Cyber-Crime. *Third World Quarterly*, s. 1057-1079.

Kshetri, N. (2010). *The Global Cybercrime Industry.* Springer.

Kshetri, N. (2016). *The Quest To Cyber Superioty.* Switzerland: Springer.

Methmali, S. (2016). Perception of internet usage and its impact on cyber-crime in Sri Lanka. *International conference on Signal Processing, Communication, Power and Embedded System (SCOPES)*, (s. 674-690).

Pieszko, G. (2016, September). The influence of socio - economic factors on crime. *IOSR Journal Of Humanities And Social Science*, s. 18-21.

Wori, O. (2014, January 23). Computer Crimes: Factors of Cybercriminal Activities. *International Journal of Advanced Computer Science and Information Technology*.

https://www.iii.org/table-archive/21319

https://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml?pid=ACS_17_5YR_S1501

https://www2.census.gov/library/publications/2014/acs/acsbr13-01.pdf