CYBER SECURITY:REDUCE THE RISK OF CYBER ATTACK AND OPPORTUNITY TO PREVENT CYBER CRIME

Ms. Disha Saini

Assistant professor

Institute of Technology and Management, Meerut

ABSTRACT

Cyber Security plays an necessary positionwithin the fieldaboutinformationtechnology .Securing the informationhaveemerge as oneover the largest challenges between the existing day. Whenever we thinkas regards the cyber security the advanceelementup to expectation comes according to our thinking is 'cyber crimes' who are increasingimmenselydayby day. Various Governments orcorporations are receivingmany measures withinorderin imitation of preventthese cybercrimes. Besides a number of measures **c**yber security is nevertheless a verygreatconcernin imitation of many. This paperfrequently focuses over challenges confronted via cyber securityconcerning the modern daytechnologies .It additionally focuses concerningmodernabout the cyber security techniques, ethicsand the traits altering the faceconcerning cyber security.

Keywords: Cyber Security, Information Technology, Government, Ethics

1. INTRODUCTION

The management of risk to information systems is considered fundamental to effective cybersecurity. The risks associated with any attack depend on three factors: threats (who is attacking), vulnerabilities (the weaknesses they are attacking), and impacts (what the attack does). Most cyberattacks have limited impacts, but a successful attack on some components of critical infrastructure (CI)—most of which is held by the private sector—and the livelihood and safety of individual citizens. Reducing such risks usually involves removing threat sources, addressing vulnerabilities, and lessening impacts.

The federal role in cybersecurity involves both securing federal systems and assisting in protecting nonfederal systems. Under current law, all federal agencies have cybersecurity responsibilities relating to their own systems, and many have sector-specific responsibilities for CI. On average, federal agencies spend more than 10% of their annual ICT budgets on

cybersecurity.

We come across different cases of cyber crimes being committed almost on a daily basis in the newspaper or on the television or through any other person. There they usually narrate the whole procedure through which the crime was committed, these crimes are usually what we technically call as phishing where the fraudsters earn huge amount of money by misleading the victim by acting as a bank manager where they ask for sensitive bank details. But this is not it, cybercrimes are way more advanced than this. Criminals also commit non cybercrimes with the help of cyber stuffs. Now a days, every third person has a social account and they tend to regularly update about their daily life, their personal information like their address, etc. These personal information that a social media account holder gives on his account works as a tracer to the criminals and it becomes easier for them to harm that person, maybe by kidnapping them as they now know about the whereabouts of that person. The other very popular cybercrime is hacking.

Fig -1: The above graphical representation shows about the top ten types of online fraud.

1.1 CyberSecurity

Cybersecurity is often used synonymously with the term ‘information security’. It refers to the protection of information stored on devices, systems, and servers connected to the

internet from being accessed or exploited by unauthorized individuals or organizations. As already explained, sensitive data may be stored on such devices and systems. A data breach might result in unimaginable levels of damage to the reputation of the company or organization that stores such information and more importantly, might lead to the misuse of that information at the expense of innocent people who trusted said entities with their personal data.

Data breaches may be caused by cyber-attacks designed to steal, modify or delete large quantities of data either as a means to attain illegal access to secure information, to gain personal benefit from the misuse of such information or to wreak havoc as a means to send a message (cyberterrorism, for example). The prevention of such data breaches with the help of certain established best practices and security protocols is called cybersecurity. To better understand what cybersecurity is, and what the cyber-attack meaning really is, read on.

1.2 Cyber Security Skills

Apart from the various skills that have already been explained in brief earlier, to learn how to start a career in cybersecurity, one must also understand the detailed technical skills that a cybersecurity analyst must possess.

1.2.1 **Crisis handling and response**: One of the most important cybersecurity skills that one must possess is that of crisis management. Of all cybersecurity objectives, addressing and avoiding an imminent threat to an organization's data or information security is the most crucial.

1.2.2 **SIEM Management**: Security information and event management (SIEM) tools are used to constantly monitor the functioning of networks and systems in real-time, and they also provide cybersecurity updates if a threat is detected or perceived. A cybersecurity professional must be well-versed with SIEM automation and must be able to understand SIEM reporting and analysis to ensure an adequate response to reported threats.

1.2.3 **Compliance with law**: There are several data protection laws, guidelines and regulations that every organization in the jurisdiction must abide by, depending on the nature of business carried out by it. One of the most important of all cybersecurity qualifications is the ability to conduct a detailed review of the organization's

compliance with these regulations and guidelines since failure to do so would attract massive fines and penalties. HIPAA, SOX, PC, GDPR, ISO 27001 and so on are some examples of such regulations.

1.2.4 **Analytical strength**: A cybersecurity specialist must be in a position to use computer intelligence and analytical information available to him to quickly identify any potential cybersecurity threats or problems and ensure that they do not recur in the future.

1.2.5 **Firewall operation**: The denial of access to networks and data to those who are not authorized to access them is a massive part of the cybersecurity process. Therefore, anyone wishing to be successful in the field must be able to use firewalls or Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) and successfully filter out unauthorized or potentially harmful network traffic.

1.2.6 **Application security**: Any application requires constant improvements to its security features to keep it safe and eliminate vulnerabilities. An expert, therefore, must be able to identify such vulnerabilities and fix them at all stages of the software development lifecycle (SDLC) starting from pre-launch debugging to post-launch security updates.

1.2.7 **Advanced malware prevention**: The use of advanced threat protection programmes and software must be mastered in order to prevent and nullify Advanced Persistent Threats (APTs) that may be able to bypass the usual security protocols such as anti-virus programmes and firewalls.

1.2.8 **Data handling**: The **cybersecurity job description** extends far beyond just merely protecting large amounts of data. It also requires efficient and secure handling, storing, and continuous data analysis to ensure that it is safe and protected at all times.

1.2.9 **Digital forensics**: An extension of analytical qualities, a cybersecurity practitioner should be able to efficiently put to use digital forensic tools to investigate and detect any form of the data leak, anomalies or cyber-attacks against the organization and also to thwart such attempts before they are successful.

1.2.10 **Identity and Access Management (IAM)**: A good cybersecurity specialist is one who has an excellent understanding of the current best practices in the field of Identity and Access Management (IAM) in order to be able to draft an effective

security protocol to be put in place at an organization that can prevent unauthorized access and maintain data security.

2. WHERE IS CYBERSECURITY APPLIED?

The implications of having a world that is so reliant and dependent on technology are that there is almost no field where cybersecurity does not need to be employed. There are numerous applications of cybersecurity in the real world, and the following are just some examples of situations and organizations where cybersecurity plays an important role.

2.1 **Online money transactions**: One of the major cybersecurity benefits is that individuals can freely send or receive any amount of money through the internet without having to undergo any hassle. Cybersecurity becomes important for any activity that involves online payments such as e-commerce, cloud services, online banking and so on.

2.2 **Personal systems and devices**: While a lot of attention is paid to enterprises, individuals on their personal systems too could lose valuable data and information if they are not careful. Appropriate measures must be taken to ensure that individuals are safe while browsing and are cybersecurity aware to prevent untoward incidents.

2.3 **Financial institutions**: Financial institutions such as stock markets and banks arguably face the highest levels of risk in terms of cybersecurity and the efficient application of cybersecurity in such institutions is often a legal necessity, not an option.

2.4 **Businesses**: As discussed extensively, businesses need to protect the data they collect and their systems and networks. This can be done with the help of strong cybersecurity policies.

2.5 **Government and deface**: Governments and their deface departments often are subject to cyber-attack attempts, and due to the level of sensitivity of the information, cybersecurity is paramount.

These are just a few examples of the applications of cybersecurity and today, cybersecurity is used in some form or another in almost every field and industry, from the transportation and automobile industries to IT devices that make our everyday lives easier

3. IMPACT OF TRENDS ON CYBER SECURITY

Here mentioned below are some of the trends that are having a huge impact on cyber security.

3.1 Webservers:

The threat of attacks on web applications to extract data or to distribute malicious code persists. Cyber criminals distribute their malicious code via legitimate web servers they've compromised. But data-stealing attacks, many of which get the attention of media, are also a big threat. Now, we need a greater emphasis on protecting web servers and web applications. Web servers are especially the best platform for these cyber criminals to steal the data. Hence one must always use a safer browser especially during important transactions in order not to fall as a prey for thesecrimes.

3.2 Cloud computing and itsservices

These days all small, medium and large companies are slowly adopting cloud services. In other words the world is slowly moving towards the clouds. This latest trend presents a big challenge for cyber security, as traffic can go around traditional points of inspection. Additionally, as the number of applications available in the cloud grows, policy controls for web applications and cloud services will also need to evolve in order to prevent the loss of valuable information. Though cloud services are developing their own models still a lot of issues are being brought up about their security. Cloud may provide immense opportunities but it should always be noted that as the cloud evolves so as its security concernsincrease.

3.3 APT's and targetedattacks

APT (Advanced Persistent Threat) is a whole new level of cybercrime ware. For years network security capabilities such as web filtering or IPS have played a key part in identifying such targeted attacks (mostly after the initial compromise). As attackers grow bolder and employ more vague techniques, network security must integrate with other security services in order to detect attacks. Hence one must improve our security techniques in order to prevent more threats coming in the future.

3.4 MobileNetworks

Today we are able to connect to anyone in any part of the world. But for these mobile networks security is a very big concern. These days' firewalls and other security measures are becoming porous as people are using devices such as tablets, phones, PC's etc. all of which again require

extra securities apart from those present in the applications used. We must always think about the security issues of these mobile networks. Further mobile networks are highly prone to these cybercrimes a lot of care must be taken in case of their securityissues.

3.5 IPv6: New Internetprotocol

IPv6 is the new Internet protocol which is replacing IPv4 (the older version), which has been a backbone of our networks in general and the Internet at large. Protecting IPv6 is not just a question of porting IPv4 capabilities. While IPv6 is a wholesale replacement in making more IP addresses available, there are some very fundamental changes to the protocol whichneed to be considered in security policy. Hence it is always better to switch to IPv6 as soon as possible in order to reduce the risks regarding cybercrime.

3.6Encryption of thecode

Encryption is the process of encoding messages (or information) in such a way that eavesdroppers or hackers cannot read it.. In an encryption scheme, the message or information is encrypted using an encryption algorithm, turning it into an unreadable cipher text. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Encryption at a very beginning level protects data privacy and its integrity. But more use of encryption brings more challenges in cyber security. Encryption is also used to protect data in transit, for example data being transferred via networks (e.g. the Internet,e-commerce),mobile telephones, wirelessmicrophones, wireless intercoms etc. Hence by encrypting the code one can know if there is any leakage ofinformation.

Hence the above are some of the trends changing the face of cyber security in the world. The top network threats are mentioned in below Fig.

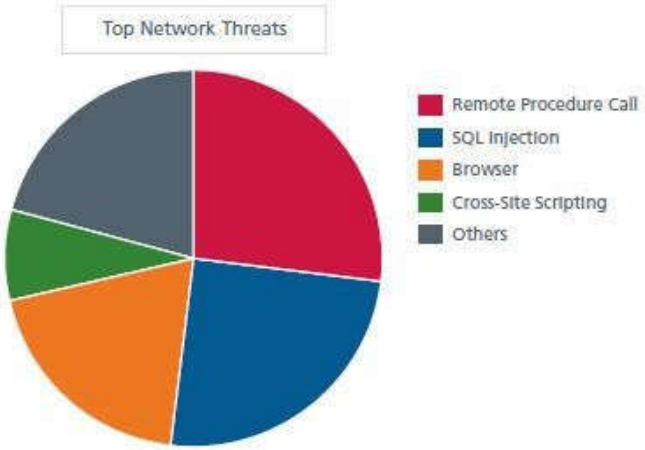

Fig -2: The above pie chart shows about the major threats for networks and cyber security.

4. CYBER SECURITYTECHNIQUES

4.1 Access control and passwordsecurity

The concept of user name and password has been fundamental way of protecting our information. This may be one of the first measures regarding cybersecurity.

4.2 Authentication ofdata

The documents that we receive must always be authenticated be before downloading that is it should be checked if it has originated from a trusted and a reliable source and that they are not altered. Authenticating of these documents is usually done by the anti-virus software present in the devices. Thus a good anti-virus software is also essential to protect the devices fromviruses.

4.3 Malwarescanners

This is software that usually scans all the files and documents present in the system for malicious code or harmful viruses. Viruses, worms, and Trojan horses are examples of malicious software that are often grouped together and referred to as malware.

4.4 Firewalls

A firewall is a software program or piece of hardware that helps screen out hackers, viruses, and worms that try to reach your computer over the Internet. All messages entering or leaving the internet pass through the firewall present, which examines each message and blocks those that do not meet the specified security criteria. Hence firewalls play an important role in detecting themalware.

4.5 Anti-virussoftware

Antivirus software is a computer program that detects, prevents, and takes action to disarm or remove malicious software programs, such as viruses and worms. Most antivirus programs include an auto-update feature that enables the program to download profiles of new viruses so that it can check for the new viruses as soon as they are discovered. An anti virus software is a must and basic necessity for every system.

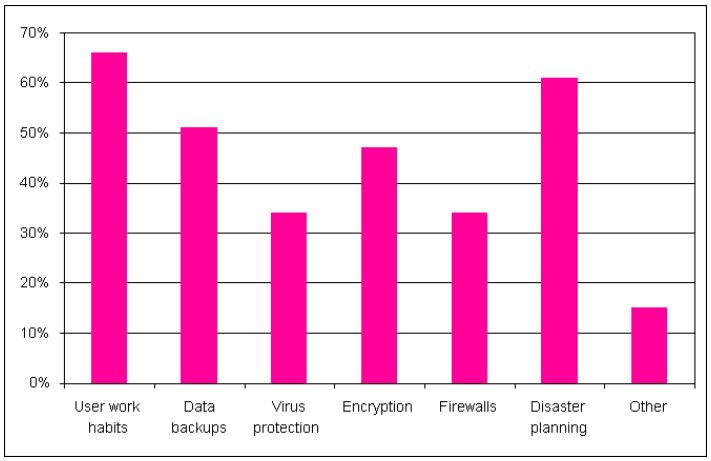

Figure 3: Techniques on cyber security

5. CYBERCRIME

Cybercrime is a term for any illegal activity that uses a computer as its primary means of commission and theft. The U.S. Department of Justice expands the definition of cybercrime to include any illegal activity that uses a computer for the storage of evidence. The growing list of cybercrimes includes crimes that have been made possible by computers, such as network intrusions and the dissemination of computer viruses, as well as computer-based variations of

existing crimes, such as identitytheft, stalking, bullying and terrorism which have become as major problem to people and nations. Usually in common man's language cybercrime may be defined as crime committed using a computer and the internet to steel a person's identity or sell contraband or stalk victims or disrupt operations withmalevolent programs. As day by day technology is playing in major role in a person's life the cybercrimes also will increase along with the technological advances.

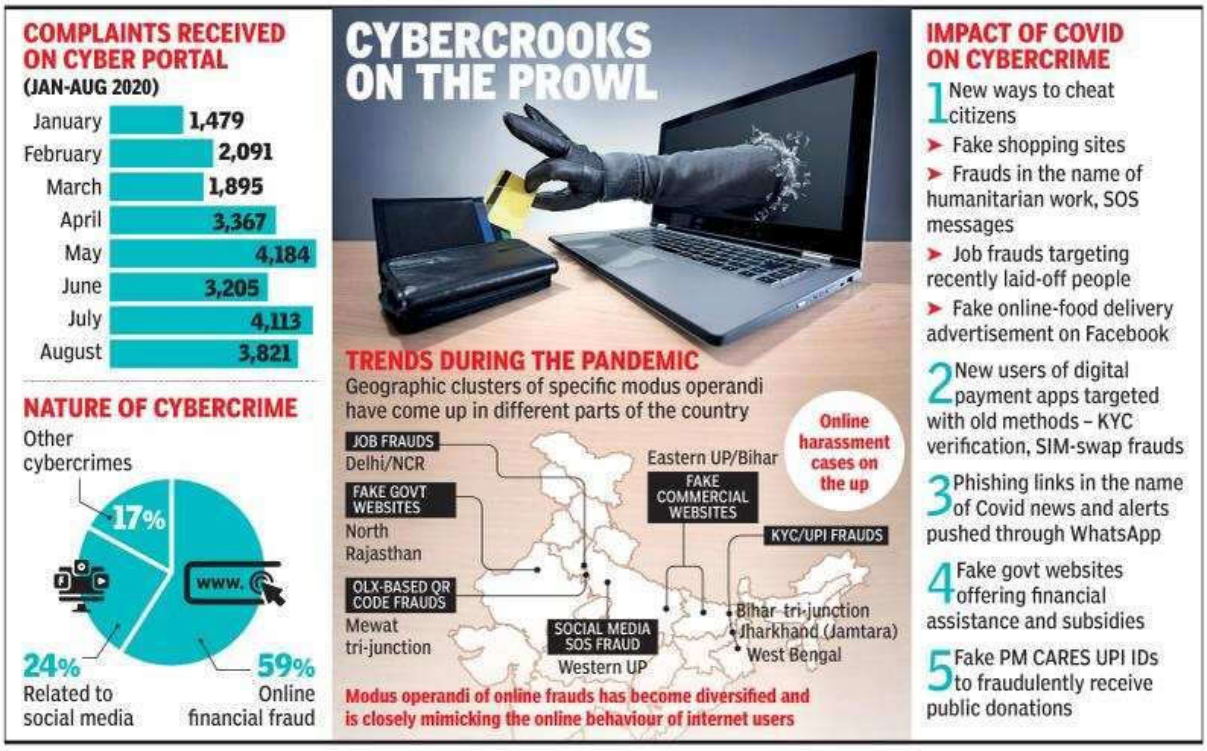

Figure 4: The above picture shows the impact of COVID on cybercrime

5.1 EVOLUTION OF CYBERCRIME

When cybercrime start, Cybercrime's history and the evolution of cybercrime did are easy to trace and coincide with the evolution of the Internet itself. The first offenses were, of course, essential hacks from local networks to steak records, but when the Internet became more developed, so did the attacks.

- Although there was cyber-crime before that, during the late '80s, the first big surge of cyber-crime came with email proliferation. It has made it easy to send a host of scams and/or viruses to your inbox.

- With advancements in web browsers, the next wave of the cybercrime history continuum came in the 90s. There were many users to pick from at the time, many more than now, and most were vulnerable to viruses. Any time dubious websites were accessed, viruses were distributed via Internet connections.
- In the early 2000s, as social media came to life, cybercrime finally started to take off. An influx of personal information and the emergence of ID fraud was generated by the influx of people throwing all the information they could into a profile folder. Thieves used the information to enter bank accounts, set up credit cards, or other financial fraud in various ways.
- The new wave is the emergence of an annual multinational crime enterprise totaling almost half a trillion dollars. Such criminals run in groups, use well-established tactics and target anyone and anybody with a web presence.

5.1.1 From landline hacking to Cryptojacking

We look back to understand how cybercrime will develop in the future to understand how it originated in the past. Cybercrime roots are rooted in telecommunications, with the culture of "hackers" as we know it today arising from "phone phreaking," which peaked in the 1970s. Phreaking, mostly to receive free or subsidized telecommunications rates, was leveraging hardware and frequency flaws in a telephone network.

5.1.2 Phishing makes a splash

Phishing is the method of tricking a user into offering account logins or other confidential data willingly. With downloadable files via email, such as the ILOVEYOU worm, this common attack style started but quickly became more sophisticated. Phishing emails frequently resemble a trustworthy source, such as a provider of internet or telephone services, and often include official images, email addresses, and dummy websites to trick the recipient.

5.1.3 The rise of ransomware

Ransomware threats have been on the rise and getting increasingly extreme in recent years, with cybercriminals seeking to encrypt as much of a business network as possible to extort a bitcoin ransom in return for returning it. A single attack can lead to hundreds of thousands or even millions of dollars being earned by cybercriminals.

In some cases, hackers are pursuing threats to reveal information they have gained in the run-up to implement the ransomware attack if the victim does not pay, something that might intimidate potential victims and allow them to react more quickly to the demands of extortion.

6. CRYPTOJACKING: THE CUTTING EDGE?

Cryptojacking is malicious crypto-mining that happens on corporate and personal machines, printers, and handheld devices as cybercriminals compromise software installation. This app utilizes the power and energy of the machine to mine for cryptocurrency or steals wallets owned by unsuspected victims. The code is simple to deploy, runs in the background, and can be hard to detect.

Tools are used by hackers both to steal cryptocurrencies from other digital wallets and to allow hijacked computers to do the job so that valuable coins can be mined.

The main concept behind Cryptojacking is that to do their mining work for them, and hackers use business and personal computer and system tools. Through using these stolen machines, cybercriminals siphon the currency that they either receive or steal into their own digital wallet. The slowing down of the CPU function and the use of more power for processing affects these hijacked machines.

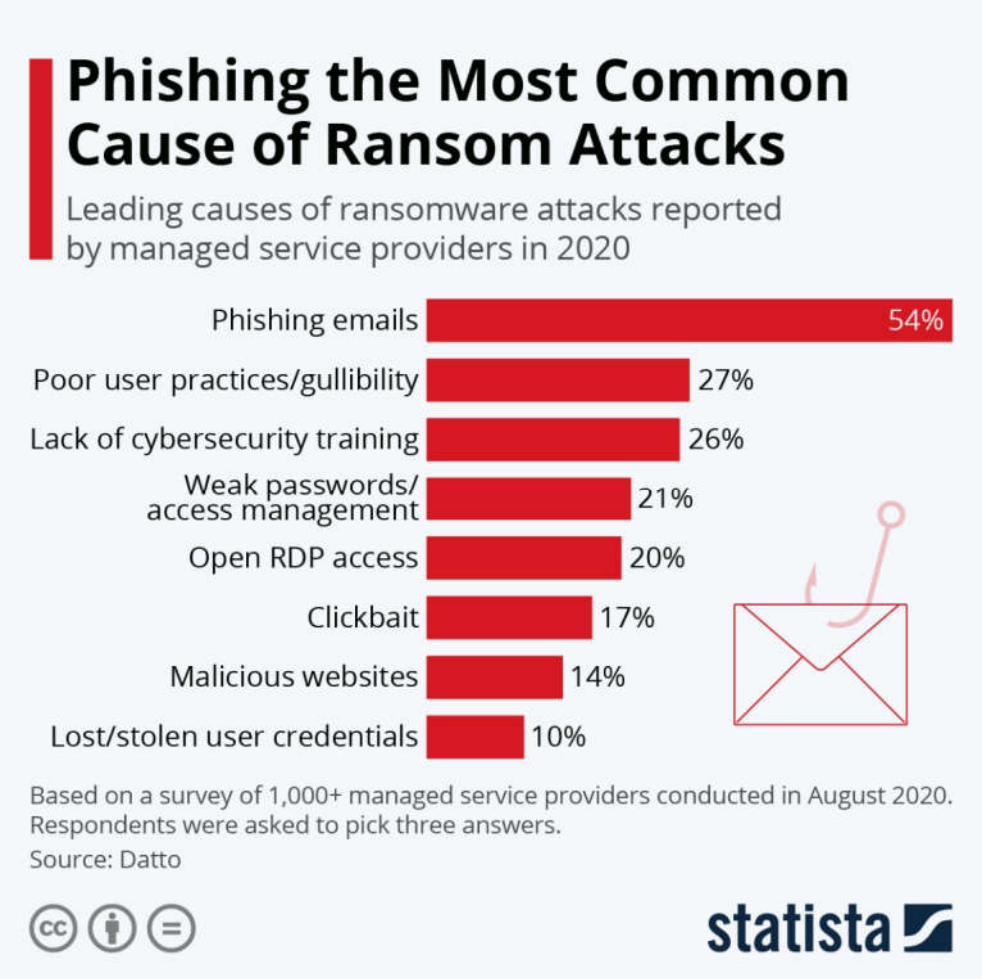

Figure 5: The above picture shows phishing the most common cause of ransom attacks

6.1 VARIOUS TYPES OF CYBER CRIMESINCLUDE:

6.1.1 Unauthorized access of hosts-

More commonly known as hacking. Hacking can take various forms, some of which might not always involve deep technicalknowledge.

- Social engineering involves "talking" your way into being given access to a computer by an authorizeduser.
- A divide exists between individuals who illegally break into computers with malicious intent, or to sell information garnered from the compromised computer, known as "crackers" or black hats", and those who do it out of curiosity or to enhance their technical prowess- known as "hackers" or "whitehats".

6.1.2 Spamming –

Involves mass amounts of email being sent in order to promote and advertise products and websites.

- Email spam is becoming a serious issue amongst businesses, due to the cost overhead it causes not only in regards to bandwidth consumption but also to the amount of time spent downloading/ eliminating spammail.
- Spammers are also devising increasingly advanced techniques to avoid spam filters, such as permutation of the emails contents and use of imagery that cannot be detected by spamfilters.

6.1.3 Computer Fraud/ "Phishing" scams-

South Africa has recently been afflicted by an onset of intricate scams that attempt to divulge credit and banking information from online banking subscribers.

- These are commonly called "Phishing' scams, and involve a level of social engineering as they require the perpetrators to pose as a trustworthy representative of an organization, commonly the victim'sbank.

6.1.4 Denial of Service Attacks-

Not to be confused with unauthorized computer access and hacking.

- Denial of Service or Do's attacks involve large volumes of traffic being sent to a host or network, rendering it inaccessible to normal users due to sheer consumption of resources.
- Distributed Denial of Service attacks involve multiple computers being used in an attack, in many cases through the use of "zombie" servers, which are trojanised programs that attackers install on variouscomputers.
- Often legitimate computer users have no idea they are involved in denial of service attacks due to the stealthy nature of the zombiesoftware.

6.1.5Viruses, Trojans and Worms-

These three all fall into a similar category as they are software designed to "infect" computers- or install themselves onto a computer without the users permission, however they each operate verydifferently.

- Many computer users have experienced the frustration of having a malicious virus wreak havoc upon their computers and data, but not all viruses have a malicious payload.
- Trojan is a program that allows for the remote access of the computer it's installed on. Trojans exist for multiple performs and have varying degrees incomplexity.
- Worms make use of known vulnerabilities in commonly used software, and are designed to traverse through networks- not always with destructive ends, historically however worms have had devastating effects such as the infamous Code Red and Melissaworms.
- Intellectual Property Theft- Intellectual property theft in relation to cyber-crime deals mainly with the bypassing of measures taken to ensure copyright- usually but not restricted tosoftware.

6.1.6 Other types of Cyber Crime could be categorized under thefollowing:

- Unlawful access to computer information - 8002crimes.
- Creation, use and distribution of malware or machine carriers with such programs- 1079.
- Violation of operation rules of computers, computer system or networks-11.
- Copyright and adjacent rights violation-528.

6.2 WHO AREINVOLVED?

Those involved in committing cyber-crimes are in three categories and they are:

6.2.1 The idealists (teenager) -

They are usually not highly trained or skillful, but youngsters between the ages of 13 – 26 who seek social recognition. They want to be in the spotlight of the media. Their actions are globally damageable but individually negligible. “Like denying a lot of important e-commerce servers in February, 2000 is said to have caused high damages to these companies”. Most often they attack systems with virusestheycreated;theiractualharmtoeachindividualisrelativelynegligible.Bytheage of 26 to 26 when they have matured and understood the weight of their actions, they lose interest and stop.

6.2.2 The greed – motivated (career criminals) -

This type of cyber-criminals is dangerous because they are usually unscrupulous and are ready to commit any type of crime, as long as it brings money to them. “They started the child pornography often called cyber-pornography which englobes legal and illegal pornography on the internet”. They are usually very smart and organized and they know how to escape the law enforcement agencies. These cyber-criminals are committing grievous crimes and damages and their unscrupulousness, particularly in child-pornography and cyber-gambling is a serious threat to the society. Example to show how serious a threat they pose to the society is “the victim of the European bank of Antigua are said to have lost more than $10million” “…theft of valuable trade secrets: the source code of the popular micro-soft windows exploration system by a Russian based hacker could be extremely dangerous… the hackers could use the code to break all firewalls and penetrated remotely every computer equipped with windows were confirmed. Another usage could be the selling of the code tocompetitors”.

6.2.3 The cyber – terrorists –

They are the newest and most dangerous group. Their primary motive is not just money but also a specific cause they defend. They usually engage in sending threat mails, destroying data stored in mainly government information systems just to score their point. The threat of cyber-terrorism can be compared to those of nuclear, bacteriological or chemical weapon threats. This disheartening issue is that they have no state frontiers; can operate from anywhere in the world, and this makes it difficult for them to get caught. The most wanted cyber-terrorist is Osama Bin Laden who is said to “use steganography to hide secret messages within pictures, example, a

picture of Aishwarya Rai hosted on the website could contain a hidden message to blow up a building". A surprising fact is that these hidden messages do not alter the shape, size or look of the original pictures in any way[17].

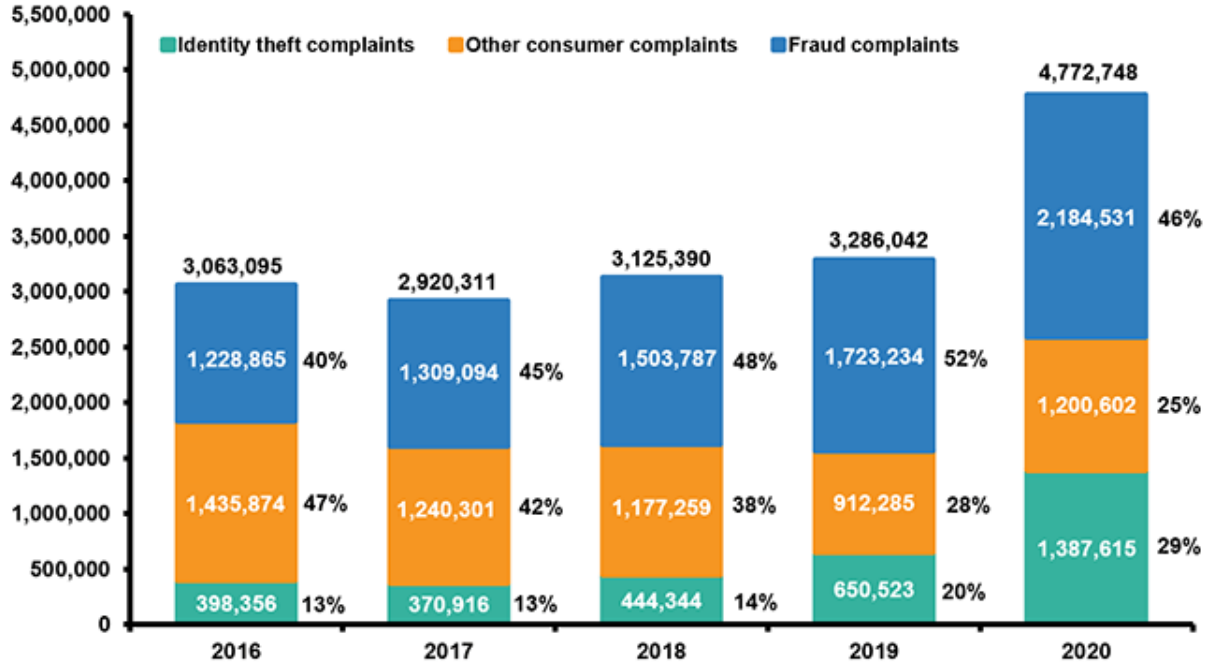

Figure 6: The above graph shows identify theft complaints, other consumer complaints and fraud complaints.

7. CAUSES OF CYBER –CRIME:

There are many reasons why cyber-criminals commit cyber-crime, chief among them are these three listed below:

- Cyber Crimes can be committed for the sake of recognition. This is basically committed by youngsters who want to be noticed and feel among the group of the big and tough guys in the society. They do not mean to hurt anyone in particular; they fall into the category of the Idealists; who just want to be inspotlight.
- Another cause of cyber-crime is to make quick money. This group is greed motivated and is career criminals, who tamper with data on the net or system especially, e-commerce, e-banking data information with the sole aim of committing fraud and swindling money off unsuspecting customers.
- Thirdly, cyber-crime can be committed to fight a cause one thinks he believes in; to cause threat and most often damages that affect the recipients adversely. This is the most dangerous of all the causes of cyber-

crime. Those involve believe that they are fighting a just cause and so do not mind who or what they destroy in their quest to get their goals achieved. These are the cyber-terrorists.

8. CONCLUSSION:

Cybercrime and Cyber security has become a subject of great concern to all governments of the world. Nigeria, representing the single largest concentration of people of Africa decent has an important role to play. This situation has almost reached an alarming point, according to various studies and countries which neglects and /fail to respond timely and wisely, will pay very dearly for it.

It has been deduced from this study that reliance on terrestrial laws is still an untested approach despite progress being made in many countries, they still rely on standard terrestrial laws to prosecute cybercrimes and these laws are archaic statutes that have been in existence before the coming of the cyberspace. Also weak penalties limit deterrence: countries with updated criminal statutes still have weak penalties on the criminal statutes; this cannot deter criminals from committing crimes that have large-scale economic and social effect on the society. Also a global patchwork of laws creates little certainty; little consensus exist among countries regarding which crimes need to be legislated against. Self-protection remains the first line of defense and a model approach is needed by most countries; especially those in the developing world looking for a model to follow. They recognize the importance of outlawing malicious computer-related acts in a timely manner or in order to promote a secure environment for e-commerce.

Cyber-crime with its complexities has proven difficult to combat due to its nature. Extending the rule of law into the cyberspace is a critical step towards creating a trustworthy environment for people and businesses. Since the provision of such laws to effectively deter cyber-crime is still a work in progress, it becomes necessary for individuals and corporate bodies to fashion out ways of providing security for their systems and data. To provide this self-protection, organizations should focus on implementing cyber-security plans addressing people, process and technology issues, more resources should be put in to educate employees of organizations on security practices, “develop thorough plans for handling sensitive data, records and transactions and incorporate robust security technology- -such as firewalls, anti-virus software, intrusion detection tools and authentication services”.

8. REFERENCES

1. Paulson LD. Spam hits instant messaging. Computer and Internet Security, 37 no 4:18,2004.
2. Tygar J Rachna D and Marti Hearst. Proceedings of the conference on human factors in computing systems. In Why Phishing Works,2006.
3. Jansweijer W Schreiber G, Wielinga B. IJCAI workshop on eradicating cybercrime in the world. In Towards Cybercrime Eradication, August 19-20th1995.
4. Goodman Symour E and Herbert S. Towards a Safer and More Secure Cyberspace. National academies Press,2007.
5. EugueneVolokh. Crime-facilitating speech. Stanford Law Review, 57:1095_1222, March2005.
6. http://www.asianlaws.org/press/cybercrime.htm
7. http://www.dailytrust.com,2008
8. http://news.softpedia.com/news/Nigerian-Phishers-Arrested-83024.shtml
9. http://www.crime-research.org/Golubev_interview_052004/
10. www.mcconnellinternational.com/services.cybercrime.htm
11. http://www.irs.ustreas.gov
12. http://www.antiphishing.org
13. http://netsecurity.about.com/b/2005/02/20/nigerianbank-scam-meets-phishing-attack.htm
14. http://www.cybesecurity.org/Research/2004.06.dissertation.Pdf.
15. http://www. The Menace Of Cyber Crime - Author - AnusuyaSadhu.htm)