Cyber Security

Research · December 2018

CITATIONS
0

READS
2,432

1 author:

Moinul Hoque Robin
North South University
5 PUBLICATIONS **0** CITATIONS

SEE PROFILE

Cyber Security

Table of Contents

Topic	*Pages*
Introduction	3-4
Cyber Security Definitions	4-7
Issues/Consideration	7-11
Potential Impacts	11-16
Conclusion	16-17
References	18-19

Introduction: Cyber security becomes a very important issues now a days. We are staying now in a very good world civilization. We are so lucky that we are now using the best inventions of science and technology. Lots of inventions computer is the most powerful invention of science and technology. Computer becomes very update and our life becomes faster by means of internet. We use internet to make easier our life. We use different types of social sites for better communications.Facebook,Whatsapp,Imo,Viber,Tango,Line,Instagram,Twitter,Skype,Mig33, Youtube are more popular to this generation. Peoples share their own Photos, Videos, Recent locations, feelings, entertainment and different sort of news also. Some people share their some very personal photos by their own privacy to keep as a memory like cloud computing. Some dishonest person plunders our photos or videos and blackmailing us by representing these wrong ways. Actually, they are known in our society as hacker. They hack our very personal and important information and makes our life hyper. It is one kind of crime. Yes. Its a **Cyber crime**. At first we should know what is **Cyber Crime?**

Cyber crime, or **computer related crime**, is crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target.

Sometimes hacker attacks very very important person or the government also for being success to their own self-interest. Mainly those dishonest people do that for harassing someone or they claim a big amount of money from the victims. Some hackers hack for playing victim as their will or they did very bad things to the victims.

In Bangladesh, we have Law, Rules and regulation, ICT act to protect our country and mango people. But we are not aware about that. Thats why, we easily fall into any problem in IT sector. Dishonest people can easily abuse us as a trump card and in a complicated situation we have to obey them. But this is not fair. Why we are being abused by them by living in an independent country? We are educated people, we have knowledge, we have common sense. So why we are not concerned about this big term **Cyber Security?**

Computer security, also known as **Cyber Security** or IT security, is the protection of computer systems from the theft and damage to their hardware, software or information, as well as from disruption or misdirection of the services they provide.

Now we have to conscious about this term Cyber Crime. We should know how and why it occurs?

Cyber Crime may occur for many reasons. Among them-

- **Personal Hostility**
- **Hackers Self-Interest**
- **Users Lack of knowledge about Social Media.**
- **Users poor password**
- **Get entered any sites randomly**
- **Using untrusted link.**
- **Using unauthorized application.**
- **Lack of knowledge about using email**.

- **Backdated Operating Systems.**
- **Hackers Use Religious Values.**

These are the most common reason. We have to handle those hacker in Cold blood. Because these hackers are too much clever and much more updated in this social media. For protecting ourselves we have to gain knowledge few topics and understand the whole cyber security systems. Generally, hackers use different types of malware for hacking. Now we are going to know about some malware.

- **Adware**
- **Ransomware**
- **Backdoor**
- **Virus**
- **Key Logger**
- **Root Kit**
- **Spyware**
- **Trojan horse**
- **Identity Thieves/Fishing**
- **Worm**

We have to keep knowledge all of this. Awareness can be the strongest weapon to prevent these types of cyber-crimes. To keep our life safe, we have to keep an eye on this issue. It will save our internet and our personal life.

Cyber Security Definitions:

1. Cyber security or information technology security are the techniques of protecting computers, networks, programs and data from unauthorized access or attacks that are aimed for exploitation.

2. Cybersecurity refers to a set of techniques used to protect the integrity of networks, programs and data from attack, damage or unauthorized access.

3. Measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack.

4. Our daily life, economic vitality, and national security depend on a stable, safe, and resilient cyberspace.

5. Computer security, also known as cyber security or IT security, is the protection of computer systems from the theft and damage to their hardware, software or information, as well as from disruption or misdirection of the services they provide

6. The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.

7. Cyber security refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access. Cyber security may also be referred to as information technology security.

8. Cybersecurity refers to preventative methods used to protect information from being stolen, compromised or attacked. It requires an understanding of potential information threats, such as viruses and other malicious code. Cybersecurity strategies include identity management, risk management and incident management.

9. Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following:
    - Availability
    - Integrity, which may include authenticity and non-repudiation
    - Confidentiality

10. Use of the term 'cybersecurity' as a synonym for information security or IT security confuses customers and security practitioners, and obscures critical differences between these disciplines.

11. Cybersecurity encompasses a broad range of practices, tools and concepts related closely to those of information and operational technology security. Cybersecurity is distinctive in its inclusion of the offensive use of information technology to attack adversaries.

12. The term cybersecurity encompasses all the tools, policies, security concepts, security mechanisms, guidelines, risk management methods, actions, training, good practices, guarantees and technologies that can be used to protect the cyber environment and assets of organizations and users.

13. Cybersecurity refers to a set of techniques used to protect the integrity of networks, programs and data from attack, damage or unauthorized access.

14. The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this.

15. Computing the state of being safe from electronic crime and the measures taken to achiev e this.

16. A comprehensive cybersecurity program leverages industry standards and best practices to protect systems and detect potential problems, along with processes to be informed of current, threats and enable timely response and recovery.

17. The protection of data and systems in networks that are connected to the Internet.

18. Cybersecurity is system of computer technology that protects and integrates global interconnected information technology infrastructure.

19. Cybersecurity are measures of adopt of technologies, processes and practices aim to protect computers, networks and digital data from attack.

20. Cyber security is the protection of computers, data, networks and programs against unauthorized access or attack by individuals, groups, companies, and governments. Threats range from cyber espionage to cyber-crime and, at a national level, cyberwarfare. Cyber security is a growing concern for companies, for whom threats are now akey boardroom issue. Companies' efforts to protect against cyber-attacks are however being undermined by their staff's non-compliance with policies designed to prevent data breaches.

21. Precautions taken to guard against crime that involves the Internet,
especially unauthorized access to computer systems and data connected to the Internet.

22. Cybersecurity refers to preventative methods used to protect information from being stolen, compromised or attacked. It requires an understanding of potential information threats, such as viruses and other malicious code. Cybersecurity strategies include identity management, risk management and incident management.

23. Cyber security or information technology security are the techniques of protecting computers, networks, programs and data from unauthorized access or attacks that are aimed for exploitation.

Issues and consideration:

The past of Cyber Security:

Cyber security is invented since 1988, when Robert Tappan Morris tried to measure how big the Internet was by releasing one of the first recognized worms to infect the world emerging cyber infrastructure. The worm relied upon weaknesses in the UNIX system to replicate itself. Once transited, computers slowed down to the point of being unusable. Tappan became the first person convicted under the United States Computer Fraud and Abuse Act. Since then, we have seen an increase in cyber hacking and subsequent scams taking us beyond individual "Geeks" gaining access and criminals looking for easy money, to a new cyber underworld of transnational networks and state-sponsored cyber spies. In the process, sophisticated hackers continue to gain access to personal, banking and government information as well as military and industrial secrets. A major shift in cyber-attacks occurred in October 2010 with the release and detection of the Stuxnet worm. Stuxnet was introduced into the government computers by individuals using a personal USB drive. With Stuxnet, hacking had gone from an accessible phishing enterprise to an all-out clearness struggle. Security experts agree that the single method most effective in minimizing intrusion and compromise of information is you, the user. Policies and procedures are not effective if computer users are not trained and educated on the proper methods of implementing security policies and using security procedures. More than 32 lakh debit cards issued to various Indian banks were compromised earlier last year, which resulted in the loss of R$ 1.3 crore in fraudulent transactions as reported by the National Payments Corporation of India (NPCI). These hacks went undetected for months, allowing the hackers to continuously extract money off these user accounts as well as infect other bank operations with malicious software. Twitter accounts around the world were hacked. The most noteworthy for India was the attack by an infamous hacker group known as Legion. Banking in Bangladesh was also not spared as one of the largest financial crimes online took place early last year, resulting in $81 million "liberated" from the banks and "reinvested" in places such as the Philippines, Sri Lanka, and other parts of Asia. State-sponsored Russian hackers made a big splash across the US by hacking into the Democratic and Republican National Committees' email archives through repeated phishing attacks.

The present of cyber security:

we become increasingly dependent on technology in our daily lives we open ourselves up to an entirely new kind of threat, cyberattacks. The cyber security must stop looking back and now

transform to keep up with the rate of innovation happening in the wider technology. On October 21, 2016 the largest cyber-attacks on record as websites such as Twitter, Netflix, Airbnb, Reddit, SoundCloud, and others were temporarily shut down. This threefold attack interrupted websites and caused outages across the United States and Europe. The newly emerging Internet of Things (IoT) and its associated devices were also slammed by attacks on the servers of DYN, the company controlling the largest portion of the Internet's domain name servers (DNS), and thereby highlighting future vulnerabilities across the IoT. The cyber security industry must stop looking back and now transform to keep up with the rate of innovation happening in the wider technology industry.

The Rise of IoT :

IoT, or "Internet of Things," is the idea that certain things can be made more functional and efficient by being connected to a network. Examples range from the large-scale, such as RFID chips that connect to a shipping company's tracking system, to the more small-scale, such as printers that provide the option to order new ink when it runs out. There's little doubt that life and work can be made considerably easier by the IoT, but there are caveats — particularly in the form of morally questionable data collection. IoT-ready devices are particularly adept at providing information ranging from a consumer's product usage. Some even use hidden microphone tech designed to "improve consumer experience." When sensitive data is collected en masse, there's the potential for hackers to obtain that information and use it to their advantage. Never before has such large chunks of data regarding people's browsing history or behaviors been available, which in and of itself is a cybersecurity concern.

Mobile Malware:

We often associate the terms "virus" and "malware" with desktops. They are, after all, designed to take over desktops — or at least they were. This was before the age of smartphones. With smartphones becoming the device of choice for many consumers, it makes sense that hackers are busy crafting malware that can infiltrate your phone and gobble up all sorts of personal data, from personal photos to your contact book. With a projected over 215 million online shoppers in the US alone in 2018, it makes sense that hackers have already begun devoting resources to crafting mobile malware. Although a complete mobile device meltdown has yet to take place across the industry, several weaker mobile operating systems could be at risk in the coming year.

Digital Banking and Financial Transactions:

New tech like Apple Pay, Google Wallet and chip-based credit cards make the possibilities of card-not-present fraud a lot less viable, though it also raises the risk of digital theft if a particular device is exploited or a database is hacked containing sensitive information. As one credit card fraud potential window closes another one seems to open with the digital transition, something that all CEOs should be aware of for future transactions, especially if their data is stored within the cloud. When your local identity information is being sent to a shared cloud environment, the

risky synchronization requirements can lead to holes in SaaS or IDaaS cloud providers that could put your data at risk.

Weaponized Data:

Our browsing habits should be private and secure, but that doesn't stop certain hackers from accessing undesirable information — like you accessing an inappropriate website — and blackmailing you over that information. Even worse would be a personal photo that could harm your reputation. If you have any data on your computer or mobile device that could potentially incriminate you or put your company's reputation at risk, it's fully possible that a hacker will obtain it and financially blackmail you over it. Welcome to the new age of exploitative cybercrime.

Prevalent Social Engineering:

Social engineers target human nature and emotion to generate a lead, sale, or click-through. Masqueraded email messages and fake social media profiles to advance an agenda are two common examples of social engineering in full form, something that is unfortunately becoming very predominant. As CEO, you should be wary of all social media content or general internet content unless it comes from a trusted source. In this age it's hard to tell the genuineness of content or a profile in general.

One Dimensional View:

First, many organizations, and even vendors, are still focusing on the network layer, while barely acknowledging other areas of the attack surface; for example, the application layer. What's needed instead is a holistic view of the attack surface, to match the strategies and capabilities of adversaries. The Verizon 2016 Data Breach Report confirms this. The network layer and end points are only one piece of the puzzle. The attack surface has grown dramatically and therefore security practices should align accordingly.

CVE-Focus:

Second, most vulnerability management tools rely on Common Vulnerabilities and Exposures (CVE), which can lead to a misalignment of resources and efforts. The POODLE vulnerability is a good example, which occurred in 2014. At the time it was published, it received a 5.5 rating by the National Vulnerability Database (NVD). It's a common practice to filter vulnerabilities and only take action on those with a CVE value of 7 or higher. Using this model, the POODLE vulnerability would have been ignored. Finding out early that it was spawning hundreds of thousands of attacks, would have enabled organizations to adjust their remediation priorities to

address the POODLE threat. This incident illustrates the importance of contextualizing internal security intelligence with external threat data.

To improve the odds of defeating cyber-attacks, organizations can implement the following three best practices:

1. Given the shortage of qualified security professionals, leverage technology to automate as many security operations tasks as possible.

2. Increase the frequency of security posture assessments as propagated by the National Institute of Standards and Technology's "continuous monitoring and diagnostic" guidelines.

3. Lastly, extend protection measures to address today's growing attack surface. This includes moving beyond the network layer and endpoints, to include applications, databases, cloud environments, the Internet of Things, etc.

It's no longer feasible to manage threats individually, given the sheer volume of security gaps that exist. A holistic, risk-based approach that considers both security posture and business impact can reduce attack surfaces and reduce the dwell time during which vulnerabilities can be exploited. In recent years, there has been an increase in the frequency and severity of individuals and groups attempting to expose flaws in security systems and compromise organizational infrastructures for a number of reasons so we would know the present 10 most likely threats may be open to in 2017...

1. Phishing
2. Hacking (DDOS,key logging,cookie Theft)
3. Bots
4. Compliance with cyber securities policies
5. Misuse of employee privileges
6. BYOD (Bring Your Own Device)
7. Cyber Security muni quiz
8. Insufficient Recovery Planning
9. Password cracking
10. Ransomware

The Future of Cyber Security

We can expect the unexpected. We never would have predicted last year that we would be talking about the DNC and hacking of elections. Expect new trends to come out of left field. Ransomware

will be on the upswing and evolve in new unforeseen ways. It will be more targeted and focus on more valuable targets as we saw with healthcare. And it will continue to attack new, more damaging industries like we recently witnessed with San Francisco BART and Muni. Like the attacks with Krebs and Dyn, DDoS is coming back in a big way. Thanks to the proliferation of insecure things on the Internet, the risk of crippling cyberattacks will only increase." "Blockchains are moving from the realm of just fueling Bitcoin to providing smart contracts, identity management, and multiple ways of proving integrity of data. They may also hold the key to defending against IoT attack. Quantum computing will have possibly the biggest impact within 10 years. Most over-the-wire encrypted transmissions collected over the next decade will be readable, and even private keys will be reversible from public blockchains (for example, you can spend someone else's Bitcoin). Post-quantum safe crypto will be a must. Al will be used to identify hacking flaws and patch them to stay ahead of malicious attackers." The top challenge for cybersecurity isn't preventing data breaches, stamping out ransomware, or preventing ever-more-massive DDoS attacks, it is securing our digital privacy. 2017 and the years to come will dictate the future of cybersecurity, and most importantly human privacy. Digital threats have evolved quickly and can wreak havoc on our lives, endangering our personal privacy and the privacy of those around us. To tackle this important issue, we need the national government to take a stance on what our digital privacy is. It is more innovative, in examining today and tomorrow's needs and not looking backwards, it will be in a better place to plot a course for comprehensive, cogent security protocols which will still be relevant in the next ten, even 20 years.

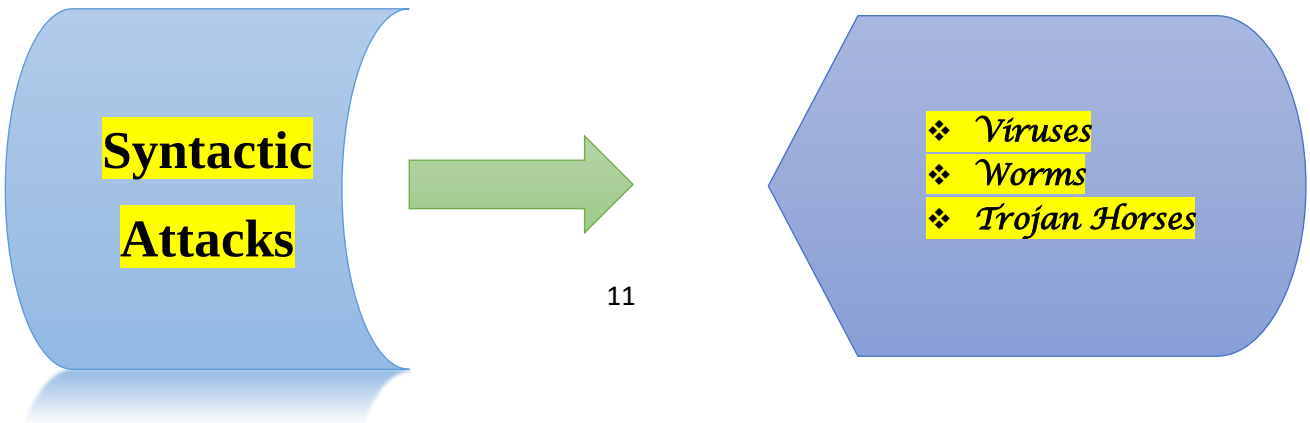
Potential Impacts: Types of Cyber-attacks can be two types. They are-

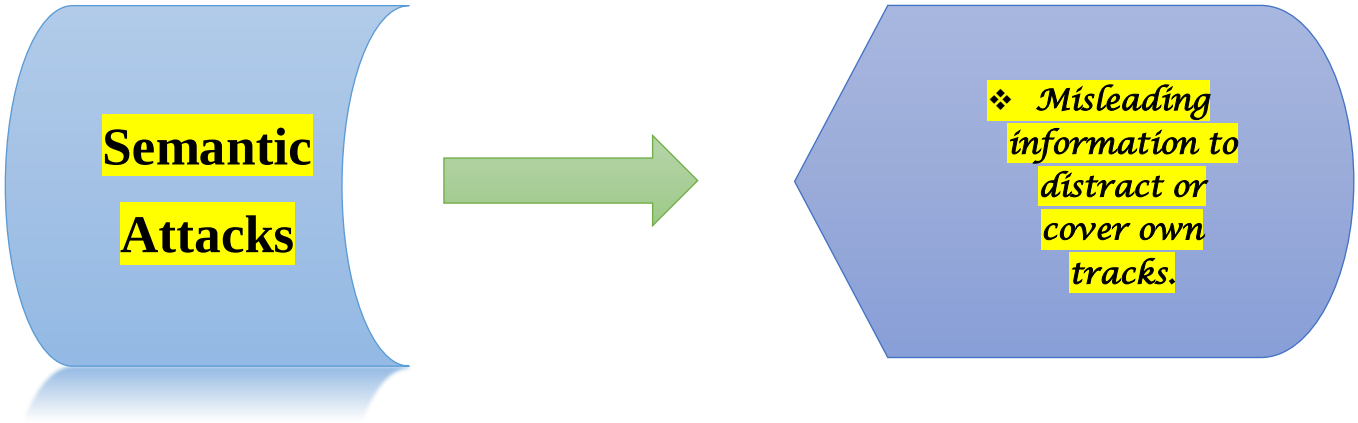
- **Syntactic Attacks**
- **Semantic Attacks**

Syntactic systems attacks by Viruses, Worms and Trojan Horses.

Semantic systems attacks by Misleading or Information to distract or cover own tracks.

Most of the cyber-crimes caused by these sorts of elements. We are not aware about Viruses, Malware, Worms and Trojan Horses. These types of viruses are so dangerous that can damage any programme very quickly. Sometimes hackers attack the whole systems and they take control the whole system and then real users have nothing to do. Than hackers claimed huge amount of money or hacker tell to do same whatever s/he want. This makes a user lives hyper.

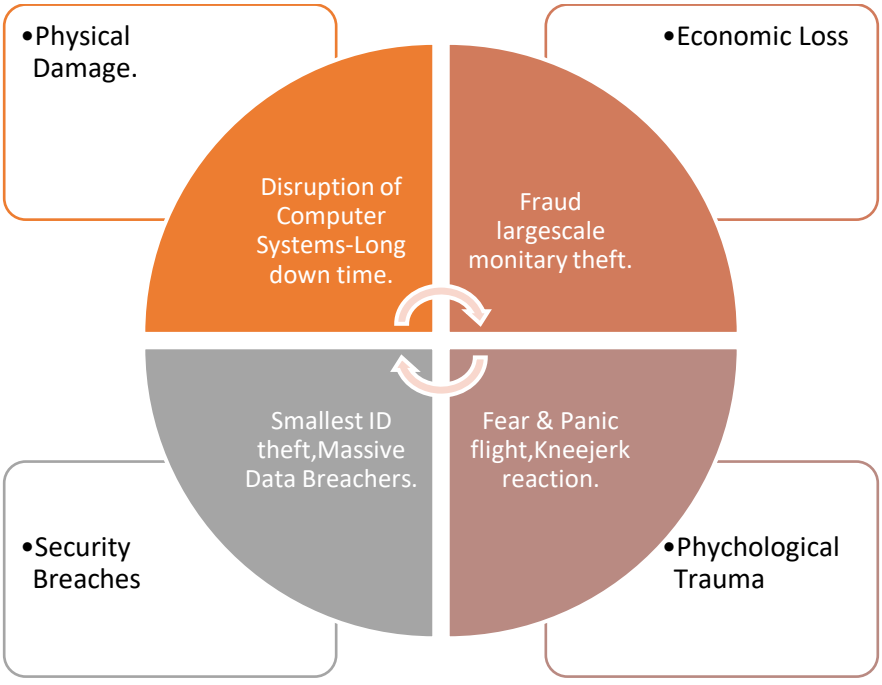




Manifestation Attack:

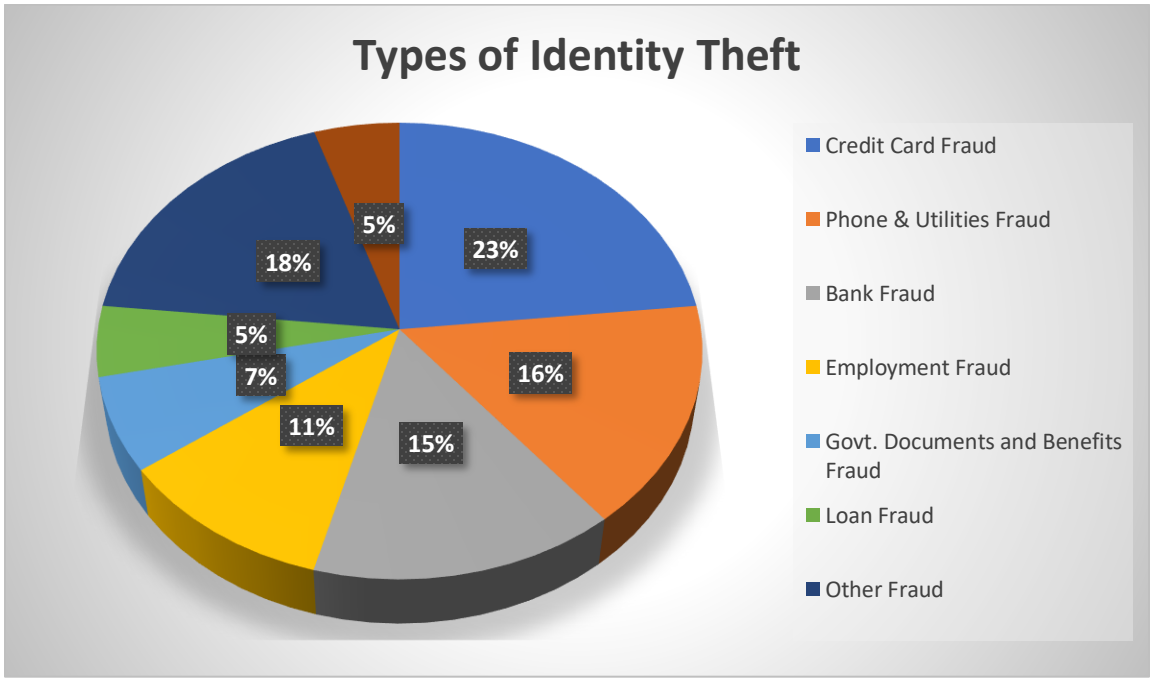
Manifestation of cyber-attacks can damage a system by Hardware damage, Economic Loses, Security Breaches and Psychological Trauma. In physical damage a system can damaged by Disruption of computer system long down time. If it occurs than it kills users valuable times and makes him impatient. Than we have to look another stage and that is Economical Losses. In these types of fraud users becomes hampered of large scale monetary theft.

A Cycle matrix view of Manifestation of Cyber Attack



Security Breaches works by hack Smallest ID but achieve Massive Data Breachers. Sometimes Government becomes the target of hackers. After affected by cyber-crimes real users fall in to psychological disease or psychological trauma. Fear, Panic and Kneejerk reaction are the symptoms of psychological trauma.

Now we have to know, how many types of fraud can be or Which sort of elements hackers choose to hack ourselves. And in no time, we are going to know these types of fraud percentage also. We have a nice and authentic information about the types of identity theft.



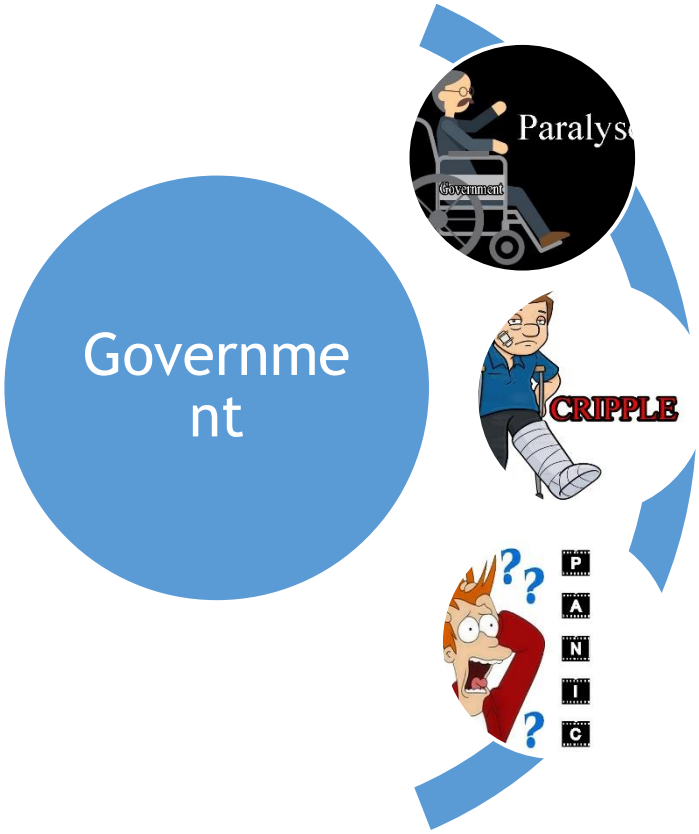
The leading fraud is Credit card fraud. About 23% of credit card fraud found in cyber-crimes. Which is very contemplative matter and then Phone and Utilities fraud takes places. Its take in 2nd position in the types of identity theft. In the meantime, Bank fraud is the most horrible issue for us. Employment fraud, Government documents and benefits fraud, Loan fraud and other fraud also increasing.

Cyber Crimes has lots of bad impacts on our personal, Social life and the whole world. Now we are going to know, What is the effects of cyber-attack on National lives.

Firstly, it has a great impact on government and by means of its effect the government becomes paralyzed.

Cyber Attacks !

Its cripples a nations critical infrastructure. It can break the unity of the people. Cyberattacks cause great damage to our national security, but as the recent ransomware cyberattack sadly reminded us, they also inflict major harm on the world economy. In fact, last week's international ransomware cyber-attack, which encrypted files, folders and hard drives, affected over 200,000 computers in over 150 countries worldwide.



Paralyses the government's Decesion making system.

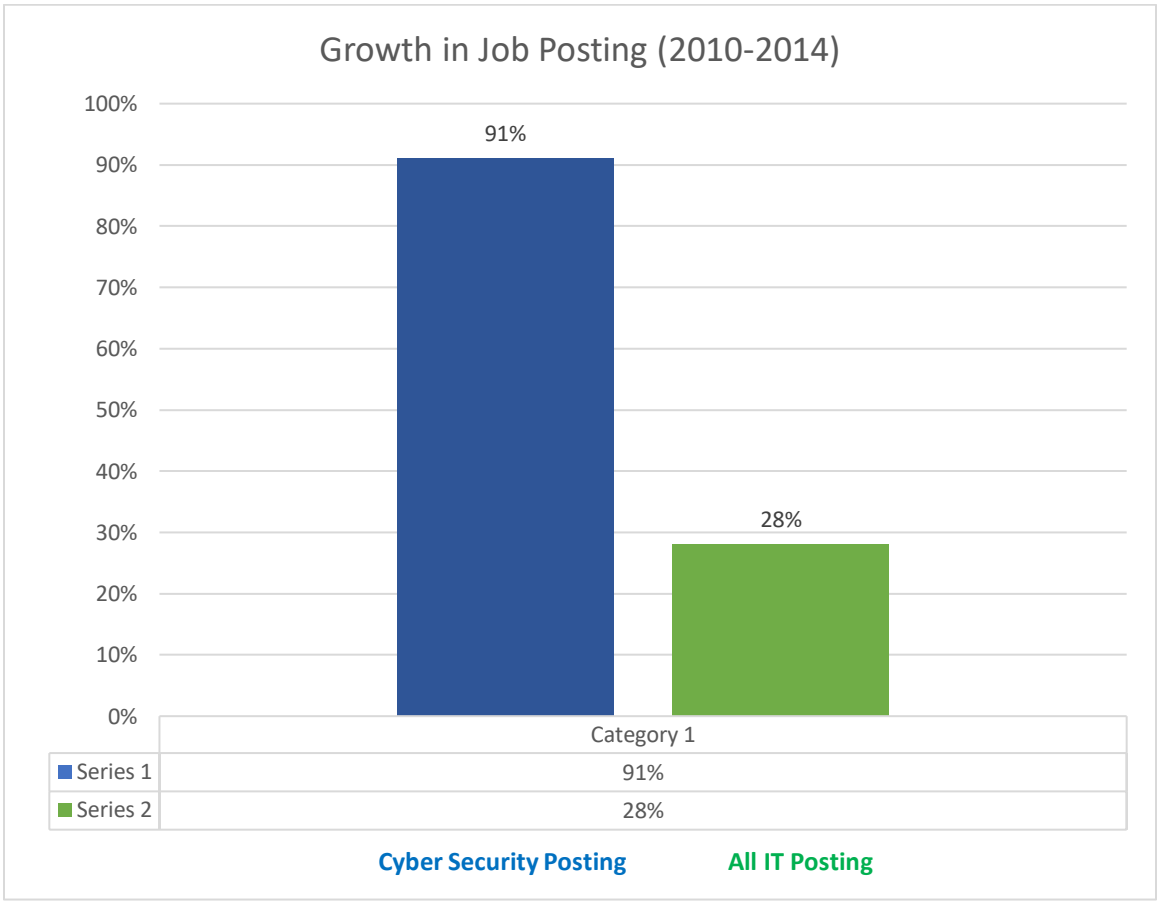
Cripples a nations critical Infrastructure.

Cause massive Panic & Trigger Inadvertant wars.

The cyber-crime of piracy has had major effects on the entertainment, music and software industries. Claims of damages are hard to estimate and even harder to verify, with estimates ranging widely from hundreds of millions to hundreds of billions of dollars per year. In response, copyright holders have lobbied for stricter laws against intellectual property theft, resulting in laws like the Digital Millennium Copyright Act. These laws allow copyright holders to target file sharers and sue them for large sums of money to counteract the financial damage of their activities online.

We can minimize the threat of cyber-attack or cyber-crime by getting a little aware and conscious while using social media platforms. It is possible to ensure the security of your personal data of those social media platforms with a very minimal effort. Do not share your password with any of your friends or colleagues or even on any online form. It is also suggested avoiding share information about your debit or credit card over these social media networks in order to avoid credit/debit card fraud, as well.

Tough we have seen lots of negative impacts with the cyber related term. But has some positive impacts too. Job market is one of them. Look a graph-



When whole IT posting are achieved 28% of Job market except Cyber Security Posting, Cyber Security can catch the job market in its way. So, we can easily say that if we study about Cyber Security properly we can get job easily 63 times more opportunity.

Conclusion: Cyber threats are a complex problem to solve, especially if they involve hidden malicious activities. The malicious actors may operate across a nation's border in performing illicit efforts. To keep the computer system safe from any harmful activities, all parties who deal in cyber space should be aware that any form of intangible threats may endanger these attempts.

We have take some necessary subject against cyber-crime. Otherwise social, economical and national life will be hampered. We have to provide or ensure more security for us and our next generation. We should use more complex password for internet based work. We may use-

%$@#5429874!aAccWqnbn@@$# instead of using "**Jones123**" kind of password. We should not use same password. We should more aware about our password. The most important thing is-

- Do not use user name as a password.
- Do not keep bank information in password.
- Do not use too small password.
- Do not share password with no one else.
- Do not use unauthorized apps.
- Do not use unauthorized link.
- Do not get entered randomly any website without checking.
- Do not use same password several kinds of social sites.

- ✓ Use Stronger Password for ensure more security.
- ✓ Use update application.
- ✓ Use update system.
- ✓ Use high security Antivirus.

The cyber-crime or cyber issues have been all time in around as well as information systems are around us. In respect of the mention case scenario or the case study, it is clear that the hacking or cyber-crime is the offence at where simple bytes are going much faster than the bullet. To prevent the cyber issue or to hack in the world, all countries are wanted to make some important and harsh laws by which the cyber-crimes are prevented. Also, want to stop all the illegal websites that are unauthorized by the governments of the countries. It is also important to every government for providing educational program regarding the cyber issue or cyber-crime. More care as more study is most import part to prevent the cyber issue or cyber-crime in the all over the world.

References:

1. *Moore, R. (2005) "Cyber crime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing.*
2. *Warren G. Kruse, Jay G. Heiser (2002). Computer forensics: incident response essentials. Addison-Wesley. p. 392. ISBN 0-201-70719-5.*
3. *Gasser, Morrie (1988). Building a Secure Computer System (PDF). Van Nostrand Reinhold. p. 3. ISBN 0-442-23022-2. Retrieved 6 September 2015.*
4. *"Cyber security or information technology", Cybercrime, viewed 4 November, 2017 from-* https://economictimes.indiatimes.com/definition/cyber-security
5. *"Cybersecurity refers to", Cybercrime.Viewed 4 November 2017, from-* https://www.paloaltonetworks.com/cyberpedia/what-is-cyber-security
6. *"Measures taken to",Cybercrime,viewed 4 November 2017 from-* https://www.dhs.gov/topic/cybersecurity
7. *"Our daily life, economic", Cybercrime,viewed 4 November 2017 from-* https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CPDP%202015%20-%20KORFF%20Handout%20-%20DK150119.pdf
8. *"Computer security", Cybercrime,viewed 4 November 2017 from-* https://digitalguardian.com/blog/what-cyber-security
9. *"The activity or process"Cybersecurity, viewed 4 November 2017 from-* https://www.techopedia.com/definition/24747/cybersecurity
10. *"Cyber security refers to the body" ,Cybersecurity, viewed 4 November 2017 from-* http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx
11. *"Cybersecurity refers to preventative" Cybersecurity, viewed 4 November 2017 from-* *Cyber Security or Cybersecurity [Internet]. [cited 2015 Oct 9]. Available from:* http://www.digitalbond.com/blog/2013/08/08/cyber-security-or-cybersecurity/
12. *"Cybersecurity is the collection", Cyber security standards [Internet]. Wikipedia, the free encyclopedia. 2015 [cited 2015 Oct 9]. Available from:* https://en.wikipedia.org/w/index.php?title=Cyber_security_standards&oldid=676890158
13. *"Use of the term 'cybersecurity'", Cybercrime,viewed 4 November 2017 from-* http://drshem.com/2015/10/12/cyberconfusion-cyber-security-cyber-security-or-cybersecurity/
14. *"Cybersecurity encompasses", Cybersecurity, viewed 4 November 2017 from-* https://www.infocrise.lu/en/web/guest/cyber-definition-cybersecurity
15. *"A comprehensive cybersecurity", Cybercrime,viewed 4 November 2017 from-* https://en.oxforddictionaries.com/definition/us/cybersecurity
16. *"The protection of data", Cybercrime,viewed 4 November 2017 from-* https://www.thefreedictionary.com/cybersecurity
17. *"Cybersecurity is system of computer", Cybersecurity, viewed 4 November 2017 from-* http://infosecisland.com/blogview/23287-Cybersecurity-vs-Cyber-Security-When-Why-and-How-to-Use-the-Term.html

18. *"Cybersecurity are measures", Cybersecurity, viewed 4 November 2017 from-* http://www.yourdictionary.com/cybersecurity
19. *"Precautions taken to", Cybersecurity, viewed 4 November 2017 from-* http://dictionary.reverso.net/english-definition/Cybersecurity
20. *"Cybersecurity refers to preventative", Cybersecurity, viewed 4 November 2017 from-* http://lexicon.ft.com/Term?term=cyber-security
21. *"Cyber security or information technology", Cybersecurity, viewed 4 November 2017 from-* https://economictimes.indiatimes.com/definition/cyber-security
22. *"Computing the state of being", Cybersecurity, viewed 4 November 2017 from-* https://economictimes.indiatimes.com/definition/cyber-security
23. *"Cyber security is invented since 1988" Cybersecurity, viewed 8 November 2017 from-* www.information-age.com
24. *"IoT, or "Internet of Things," Cybersecurity, viewed 8 November 2017 from-* www.Deccandherald.com
25. *"Quantum computing", Cybersecurity, viewed 8 November 2017 from-* http://techo.com
26. *"Manifestation of cyber-attacks", Cybersecurity, viewed 8 November 2017 from-* http://www.foxnews.com/opinion/2017/05/17/cyberattacks-threaten-our-national-security-and-economy.html
27. *"The cyber-crime of piracy", Cybersecurity, viewed 8 November 2017 from-* https://www.socialmediatoday.com/content/impact-cyber-crime-and-security-social-media
28. *"Cyberattacks cause great damage", Cybersecurity, viewed 8 November 2017 from-* https://itstillworks.com/computer-viruses-affect-economy-8739209.html
29. *"Cyber threats are a complex problem", Cybersecurity, viewed 11 November 2017 from-* http://thinkspace.csu.edu.au/suri/2016/06/01/conclusion/