# TITLE: CYBER SECURITY ATTACKS AND COUNTER MEASURES IN DIGITAL SECTOR


## NAME: NAFINUR LEO

## ID: 20-42195-1

## SECTION: C


### MOTIVATION:

Cyber Security represents unlimited carrier growth options. Cyber security is a matter of concern by the quick and continuous growth of security nature of threat. A good cyber security professional works to understand as much as possible about how technologies and organizations work. Cyber security protects the data and integrity of computing assets belonging to or connecting to an organization's network. Its purpose is to defend those assets against all threat actors throughout the entire life cycle of a cyber attack. Every day there are new threats emerging and various technologies being released. I am very much interested in this domain because it is the application of technologies, processes and controls to protect systems, networks, programs, devices and data from cyber-attacks. It has the power to secure system. I have a very general idea about these things but I want to know more about it. Also, I got to know that, in virtual world there is a war on the Internet and information flow. State-backed cyberattacks are being used as a means of suppressing government critics and internal opposition, as well as undermining important financial, health and infrastructure services in enemy countries. These attacks are backed by nation-states, which means they are well-funded and well-planned activities performed by tech-savvy professionals. I've interest to prevent it. And also, it has more job opportunities than any other sector. So, these are all the reasons that motivated me to select this domain.

### INTRODUCTION:

Almost everything is now carried on internet with shopping of daily items, education related searching to banking transactions and booking reservations. Every aspect of daily life of a human is now a day connected to Internet and hence the sensitive information needs to be secured against Cyber-attacks. Any type of unethical task done by individuals or whole organizations pertaining to computer IS, computer networks, and/or personal computer devices by use of different and malignant acts usually starting from a source which is unknown is called a Cyber-attack. It either steals, changes, or ends a target by hacking into a system. Also known as Cyber campaign, cyber warfare or cyber terrorism, they can start from installing spyware on a PC and trying and destroying the entire base. Cyber security has become a situation for precise organizational states as define of hacking, records stealing, trickery and hate propaganda create worry and nervousness about the new era "so known as cybercrime". To save from this, cyber safety technology, approach and canon are developed. The biggest mistake for the cybercrime is the human blunders. The protection of IS from theft or vandalization to the information, hardware and software containing it, and also from interference or goof of the services they render. It controls the physical access to the hardware, and protect them against any harm that passes through network, data injection, any malpractice by user whether accidental or -intentional, or being bluffed into and distracting deviating from safe and secure procedures. Cyber security is a shared responsibility and is of everyone who uses internet for any cause. Internet companies can contribute by strengthening the security of their networks and payment processes. Government should pave to aware and educate public. It should also impose anti-cyber-crime laws. Businesses, on the other hand, should inculcate strong security processes including awareness among employees to use unique and strong passwords.

## LITERATURE REVIEW:

Phishing: It is a constant threat when it comes to social networking. Exact duplicate of a website can be created and personal information could be asked, which is then emailed to them. This is more prone to organization, individual homes, even public to get personal and security information affecting the user or company. Phishing is done in the presence of a belief of the user that the website being seen is the one carrying integrity. Hacker can access to each and every information user enters.

Root Kit: A set of computer software, to facilitate gaining computer or its software which normally is not allowed hiding its presence and its software's existence. The term rootkit is an integration of "root" (from Unix OS) and the word "kit" (components that implements tool). This term holds bad connotations as it is connected with malware Rootkit can be installed or automated or once the user gets the root or administrator access. Once installed, it hides the invasion and even maintains privileged access. To detect Rootkit is difficult as it destroys the software designed to find it. However, detection methods use an alternative operating system which are trustworthy, methods which are behavioral-based, scanning of signature, scanning of difference, and analysis of memory dump.

Kido: Also referred as Conficker, Downup and Downadup, it is a kind of computer worm which points the Microsoft Windows OS. Using loopholes in Windows operating system software and using dictionary attacks on passwords of the administrator, it is carried out by forming a botnet, it combines use of many advanced malware techniques and hence difficult to counter. This worm focuses on networking websites like Facebook, Skype, Yahoo Messenger, and Gmail, Yahoo Mail, and AOL Mail. It also points to other networking websites, such as Myspace and Twitter, and it can affect other devices on the same local network.

Code Injection: It is the unfair use of a bug (error) when invalid data is processed. A vulnerable computer program is injected (introduced) of a code and the course of execution is changed. The result could be disastrous. It could also lead to data loss or delinquency, lack of answerability, or refusal of access. It can also result in complete host takeover.

Hacker, attacker or intruder: These are the people who try to utilize weaknesses in systems for their own gain. They enter into others place without permission. Although they are not always harm that place, sometimes they are initiated only as a means of fulfilling curiosity, their actions are typically unethical to the systems they are exploiting. The results can vary from less vulnerable to most vulnerable.

SQL Injection: Here, Data-driven applications are attacked by an injection of a code. Malicious SQL statements are put into an entrance for execution. Also known as attack vector for websites, it is able to attack any SQL database. It allows to spoof identity, modify data, create repudiation issues, allows complete access of all data on the system, destroys it or make it unavailable.

BotNet: A number of computers connected online and communicating with other similar devices so as to complete same tasks is a botnet. It is used to send spam email and to take active part in transmitted denial-of-service attacks. Word robot and network combines to form this word. But the term holds a negative connotation.

Virus: A malware program put into the memory without intervening into the user's program and its execution to harm system resources by creating, moving and erasing files against user's commands is called a virus. It may consume memory. It replicates by making copies of itself and propagate via network-based software. It may mislead execution of the program.

Worms: Worm is a standalone type of virus capable of replicating itself to spread to the computers to mislead execution of the program.

Trojan horse: A Trojan horse is a malicious code that behaves to be one thing but is executed differently. They create a secret path for attackers to access confidential and secured information.

Man-in-the-middle-attack: Man-in-the middle attack, also acknowledged as eavesdrop attacks, happen when attacker introduce himself or herself into a two-party operation. Formerly the attackers break off the transfer, they can sieve and pinch data.

Ddos attack: A denial-of-service assault floods systems, servers, or networks with transfer to fatigue property and bandwidth. As a consequence, the system is not capable to accomplish legitimate desires. Attackers can also use abundant compromised strategies to commence this attack. This is known as a distributed-denial-of-service (DDOS) attack.

For any corporation several policies should be prepared for mails so that the mails are not puzzled with any additional spam mails or phishing. High-quality of antivirus should be used equally by the individual user or corporation so that it can sort out and block the malicious website. Authentication should be complete at each level of the websites to avoid attacker from stealing your confidential information or gaining access of the user's individual information. Cryptography based techniques should be used to make sure the security of the user's information provided on communal networking websites. Group key replace, data mining, encryption is some of the examples which can be used to improve the security on social media. Training and learning programs should be finished by government to increase the alertness about the cyber security. The government should perform publicity campaigns and programs which include webinars, contest, and exhibitions about cyber security. As rising reputation of social networking sites these have become a major objective for cybercrime and attacks. Cybercrime is becoming a common and posing a major threat to the national and financial security. Both personal and universal institutions in sector of public health, information, and telecommunication, defense, banking, and economics are at menace.

The notion of username and password has been underlying way of protecting our information from stealers. This may be the one of the first step regarding information security. The document, which we receive, must always be authenticated before downloading it should be checked that if it is a reliable source or if not, then the company will get notify about the threat. Software update is very important because they usually include critical patches to security holes. They can also upgrade the stability of your software and remove outmoded features. If anyhow menaces can happen company should get intimation or alarm about the violation. It is a process through which we can intimate or educate people about the security so they that will not trap in any cyber-crime. Firewall is a software program or a piece of hardware that helps remove out hackers, protects the computer from any unknown access, and provides a safeguard to our confidential information.

Main objective: The objective of this research is to discuss about cyber attacks and how to prevent cyber attacks.
Sub objective 1: The sub objective of this research is to discuss about the classification of cyber security attacks.
Sub objective 2: The sub objective of this research is to discuss about how to be secured from the attacks in internet.
Sub objective 3: The sub objective of this research is to discuss about man of the middle attacks and ddos attacks.

Main research question: Does this research discuss about cyber attacks and how to prevent cyber attacks?
Sub research question 1: Does this research discuss about the classification of cyber security attacks?
Sub research question 2: Does this research discuss about how to be secured from the attacks in internet?
Sub research question 3: Does this research discuss about man of the middle attacks and ddos attacks?

## PROPOSED METHODOLOGY:

In this paper, I analyze that digital sector faces unique cyber risk. The enormous amount of data interactions, incorporation between dissimilar IOT campaign, and energetically altering processes creates new cyber threats, compounded by complexities in the other apparatus of the ecology that drape around the technology infrastructure. For example, data authority can be a prickly subject for cities as they need to consider about whether the data is internal or external; whether it is transactional or modified; whether the transactional data is composed via IOT devices; and how the information is stored, archived,

duplicated, and shattered. In addition, due to a lack of universal principles and policies, many cities are experimenting with new vendors and goods, which generate interoperability and combination problems on the position and aggravate cyber risks. Everyone wants to be secure and safe while using internet but times have come to make this sure of oneself due to emerging cyber attacks. With day to day rise of online shopping and services, the need of these countermeasures has become a mandatory requirement and is growing as the scams and attacks increase. Mobile devices too are becoming prone to cyber attacks. Their open-source software or say easy to develop software are easy to access and modify or quite easy to breach. Pirated software and fake websites too are advertising about their apps which are not up to the mark as far as security is concerned. The above stated measures help to some extent but cyber security is still an area to explore more and apply.

The proposed work observes that, the folks who can work in the cyber area or in cooperative world require a grouping of technical abilities, domain unique information, and social intellect to achieve success, but in different way, the operating network has to be dependable and sincere so that no person will be able to leak the facts. This research work examines the principal definition equipment for the term 'cyber fortification' by trustworthy sources. In this era, if the safety is considered somewhere, the word crime will be caught in our thoughts.

I suggest as much as data is possible to collect for this research. I suggest to read mainstream news articles, surf underground forums, academic papers, manuals and take a plethora of notes. Notes taken during research have proved most beneficial when discovering a previously undisclosed threat. An example would be while working with a device or operating system I suggest to get it to perform a action or manipulate its behavior that is not documented and record the method and the behavior no matter how benign it may seem at the time. Manipulation can be performed in various ways including sending the device commands, attaching soldering wires to communications pads or interacting with it as a normal user would. Working with so many different devices mean you have to possess basic knowledge about many different operating systems, programming languages, and core communications protocols. When one couples research and development with knowledge feeds that have been ingested there is good chance that a vulnerability can be exposed.

The next action is to determine the criticality of the threat. Is this vulnerability something that has to be executed locally with physical access to the device or is this one that can be triggered remotely via an already established communications channel such as the Internet. The latter of the two is what I consider the most important to protect against because this means someone from anywhere in the world could have the potential to trigger the vulnerability.

## REFERENCES:


Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *computers & security*, *38*, 97-102.

Cavelty, M. D. (2010). Cyber-security. In *The routledge handbook of new security studies* (pp. 166-174). Routledge.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity: What everyone needs to know*. oup usa.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, *4*(10).

Kemmerer, R. A. (2003, May). Cybersecurity. In *25th International Conference on Software Engineering, 2003. Proceedings.* (pp. 705-715). IEEE.

Wang, W., & Lu, Z. (2013). Cyber security in the smart grid: Survey and challenges. *Computer networks*, *57*(5), 1344-1371.

Sun, C. C., Hahn, A., & Liu, C. C. (2018). Cyber security of a power grid: State-of-the-art. *International Journal of Electrical Power & Energy Systems*, *99*, 45-56.

Thakur, K., Qiu, M., Gai, K., & Ali, M. L. (2015, November). An investigation on cyber security threats and security models. In *2015 IEEE 2nd international conference on cyber security and cloud computing* (pp. 307-311). IEEE.

O'Connell, M. E. (2012). Cyber security without cyber war. *Journal of Conflict and Security Law*, *17*(2), 187-209.

Mirkovic, J., & Benzel, T. (2012). Teaching cybersecurity with DeterLab. *IEEE Security & Privacy*, *10*(1), 73-76.

Lezzi, M., Lazoi, M., & Corallo, A. (2018). Cybersecurity for Industry 4.0 in the current literature: A reference framework. *Computers in Industry*, *103*, 97-110.

Nye, J. S. (2011). Nuclear lessons for cyber security?. *Strategic Studies Quarterly*, *5*(4), 18-38.

Luiijf, E., Besseling, K., & De Graaf, P. (2013). Nineteen national cyber security strategies. *International Journal of Critical Infrastructures 6*, *9*(1-2), 3-31.

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, *80*(5), 973-993.

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, *45*, 13-24.

Mulligan, D. K., & Schneider, F. B. (2011). Doctrine for cybersecurity. *Daedalus*, *140*(4), 70-92.

Warner, M. (2012). Cybersecurity: A pre-history. *Intelligence and National Security*, *27*(5), 781-799.

Sales, N. A. (2012). Regulating cyber-security. *Nw. UL Rev.*, *107*, 1503.

Carley, K. M., Cervone, G., Agarwal, N., & Liu, H. (2018, July). Social cyber-security. In *International conference on social computing, behavioral-cultural modeling and prediction and behavior representation in modeling and simulation* (pp. 389-394). Springer, Cham.

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International studies quarterly*, *53*(4), 1155-1175.

Martin, G., Martin, P., Hankin, C., Darzi, A., & Kinross, J. (2017). Cybersecurity and healthcare: how safe are we?. *Bmj*, *358*.

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a more representative definition of cyber security. *Journal of Digital Forensics, Security and Law*, *12*(2), 8.

Kott, A. (2014). Towards fundamental science of cyber security. In *Network science and cybersecurity* (pp. 1-13). Springer, New York, NY.

Xu, S. (2019). Cybersecurity dynamics: A foundation for the science of cybersecurity. In *Proactive and dynamic network defense* (pp. 1-31). Springer, Cham.

Stevens, T. (2018). Global cybersecurity: new directions in theory and methods. *Politics and Governance*, *6*(2), 1-4.

Finnemore, M., & Hollis, D. B. (2016). Constructing norms for global cybersecurity. *American Journal of International Law*, *110*(3), 425-479.

Galinec, D., Možnik, D., & Guberina, B. (2017). Cybersecurity and cyber defence: national level strategic approach. *Automatika: časopis za automatiku, mjerenje, elektroniku, računarstvo i komunikacije*, *58*(3), 273-286.

Garfinkel, S. L. (2012). The cybersecurity risk. *Communications of the ACM*, *55*(6), 29-32.

Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: an overview from machine learning perspective. *Journal of Big data*, *7*(1), 1-29.

Atoum, I., Otoom, A., & Ali, A. A. (2014). A holistic cyber security implementation framework. *Information Management & Computer Security*.