Volume II ISSUE IV **ISSN NO : 2582-6034**

LEGALFOXES LAW TIMES

CYBER SECURITY- A COMPARITIVE STUDY

By Harsh Vats and Dhruv Dahiya

ABSTRACT

Cyber Security plays an important role in the field of information technology. Securing the information has become one of the biggest challenges in the present day. Cyber-attacks represent a potential threat to information security. As rates of data usage and internet consumpti9on continue to increase, cyber awareness turned to be increasingly urgent. Whenever we think about the cyber security the first thing that comes to our mind is 'cyber crimes' which are increasing immensely day by day. Various governments and companies are taking many measures in order to prevent thesecyber-crimes. Besides various measures cyber security is still a very big concern to many. This paper mainly focuses on challenges faced by cyber security on the latest technologies. It also focuses on latest about the cyber security techniques, ethics and the trends changing the face of cyber security. This study focuses on the relationships between cyber security awareness, knowledge and behaviour with protection tools.

INTRODUCTION

Today is man able to send and receive any form of data maybe an email or an audio or video just by the click of a button but did he ever think how security his data is being transmitted or sent the other person safely without ant leakage of information?? The answer lies in cyber security. Today Internet is the fastest growing infrastructure in everyday life. In today's technical environment many latest technologies we are unable to safeguard our private information in a very effective way and hence these days cyber-crimes are increasing day by day. Today more

than 60 percent of total commercial transaction are done online, so this field required a high quality of security for transparent and best transaction. Hence cyber security has become a latest issue. The scope of cyber security is not just limited to securing the information in IT industry but also to various other fields like cyber space etc.

Even the latest technologies like cloud computing, mobile computing, ecommerce, net banking etc also needs high level of security. Since these technologies hold some important information regarding a person their security has become a must thing. Enhancing cyber security and protecting critical information infrastructure are essential to each nation's security and economic wellbeing. Making the internet safer and protecting internet users has become integral to the development of new services as well as government policy. The fight against cyber-crime needs a comprehensive and a safer approach. Given that technical measures approach alone cannot prevent any crime, it is critical that law enforcement agencies are allowed to investigate and prosecute cyber-crime effectively. Today many nations and government are imposing strict laws on cyber securities in order to prevent the loss of some important information. Every individual must also be trained on this cyber security and save themselves from increasing cyber-crimes.

CYBER SECURITY

Privacy and security of the data will always be top security measures that any organization takes care. We are presently living in a world where all the information is maintained in a digital or a cyber form. Social networking sites provide a space where users feel safe as they interact with friends and family. In the case of him users, cyber criminals would continue to target social media sites to steal personal data. Not only social networking but also during bank transaction a person must take all the required security measures.

As crime is increasing even the security measures are also increasing. According to the survey of US technology and healthcare executives nationwide, Silicon Valley bank found that companies believe cyber-attacks are serious threat to both their data and their business continuity

a. 98% of companies are maintain or increasing their cyber security resources and of those, half are increasing devoted to online attacks this year.

b. The majority of companies are preparing for when not if cyber-attacks occur.
c. Only one-third are completely confident in the security of their information and even less confident about the security measures of their business partners.

There will be new attacks on Android operating system-based devices, but it will not on massive scale. The facts tablets share the same OS as smart phones means they will be soon targeted by the same malware as those platforms. The number of malware specimens for Macs would continue to grow though much less than in the case of PCs. Windows 8 will allow users to develop applications for virtually device running Windows 8 so it will be possible to develop malicious applications like Android, hence there are some of the predict trends in cyber security.

TRENDS CHANGING CYBER SECURITY

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

1. Web servers:

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 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 these crimes.

2. Cloud computing and its services:

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 control for web applications and cloud service 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 issue are being brought up about their security. Cloud may provide immerse opportunities, but it should always be noted that as the cloud evolves so as its security concerns increase.

3. Advanced Persistent Threat (APT'S) and targeted attacks:

APT (Advanced persistent threat) is a whole new level of cyber-crime ware. For years network security capabilities such as web filtering or IPS have played 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.

4. Mobile Networks:

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 thing about the security issue of these mobile networks. Further mobile networks are highly prone to these cyber-crimes a lot of care must be taken in case of their security issues.

5. IPv6-New internet protocol:

IPv6 is the new internet protocol which is replacing IPv6(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 IPv6 capabilities. While IPv6 is a wholesale replacement n making more IP addresses available, there are some very fundamental changes to the protocol which need to be considered in security polity. Hence it is always better to switch to IPv6 as soon as possible in order to reduce the risks regarding cyber-crime.

6.Encryption of the code:

Encryption is the process of ending 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, ecommerce). Mobile telephones, wireless microphones, wireless intercoms etc. hence by encrypting the code one can know if there is any leakage of information.

CYBER SECURITY TECHNIQUES

1. Access control and password security:

The concept of username and password has been fundamental way of protecting our information. This may be one of the first measures regarding cyber security.

2. Authentication of data:

The documents that we receive must always be authenticated be before downloading that is it should be checked if it has originated from a reliable source and that they are not altered. Authenticating od these documents is a usually done by the antivirus software present is the devices. Thus, a good antivirus software is also essential to protest the devices from viruses.

3. Malware scanners:

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

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 the malware.

5. Anti-virus software:

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 as auto-updated 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. Antivirus software is a must and basic necessity for every system.

CYBER-SECURITY IN USA

America's prosperity and security depends upon how we respond to the opportunities and challenges in cyberspace. Censorious infrastructure, national defence and the daily lives of the Americans all rely on computer-driven and interconnected technologies. As all the facets of American life have become more dependent on a secure cyberspace, new vulnerabilities have been revealed and new threats continue to emerge. Building on the National Security Strategy and the Administration's progress over its first 18 months, the National Cyber Strategy outlines how the United States will ensure the Americans continue to reap the benefits of a secure cyberspace that reflects our principles, protects our security and promotes our prosperity.

Most cyber security risks to critical infrastructure stem from the exploitation of know vulnerabilities.

The United States Government will work with private and public sector entities to promote understanding of cyber security risk, so they make more informed risk-management decisions, invest in appropriate security measures and realize benefits from those investments. The united states consider unfettered access to and freedom to operate in space vital to the advancing the security, economic prosperity and the scientific knowledge of the nation. The administration is concerned about growing cyber related threats to space assets and supporting infrastructure because these assets are critical to functions such as Positioning,Navigation and Timing (PNT); Intelligence, Surveillance and Reconnaissance (ISR); satellite communications; and weather monitoring.

The administration will enhance efforts to protect our space assets and support infrastructure from evolving cyber threats and we will work with industry and international partners to strengthen the cyber resilience of existing and future space systems.

Federal departments and agencies, in cooperation with the state, local, tribal and territorial government entities, play a critical role in detecting, preventing, disrupting and investigating cyber threats to our nation. The United States is regularly the victim of malicious cyber activities

perpetrated by criminal actors, including state and non-state actors and their proxies and terrorists using network infrastructure in the United States and abroad.

Federal law enforcement works to apprehend and prosecute offenders, disable criminal infrastructure, limit the spread and use of nefarious cyber capabilities, prevent cyber criminals and their state sponsors from profiting from their illicit activity and seize their assets. The administration will push to ensure that our Federal departments and agencies have the necessary legal authorities and resources to combat transitional cybercriminal activity, including identifying and dismantling bonnets, dark markets and other infrastructure used to enable cyber-crime and combating economic espionage.

To effectively deter, disrupt and prevent cyber threats, law enforcement will work with private industry to confront challenges presented by technological barriers, such as anonymization and encryption technologies, to obtain time-sensitive evidence pursuant to appropriate legal process. Law enforcement actions to combat criminal cyber activity serve as an instrument of national power by, among other things, deterring those activities.

Cyberspace and its underlying infrastructure are vulnerable to a wide range of risks stemming from both physical and cyber threats and hazards. Sophisticated cyber actors and nation-states exploit vulnerabilities to steal information and money and are developing capabilities to disrupt, destroy, or threaten the delivery of essential services. Cyberspace is particularly difficult to secure due to a number of factors: the ability of malicious actors to operate from anywhere in the world, the linkages between cyberspace and physical systems, and the difficulty of reducing vulnerabilities and consequences in complex cyber networks. Of growing concern is the cyber threat to critical infrastructure, which is increasingly subject to sophisticated cyber intrusions that pose new risks. As information technology becomes increasingly integrated with physical infrastructure operations, there is increased risk for wide scale or high-consequence events that could cause harm or disrupt services upon which our economy and the daily lives of millions of Americans depend.

In light of the risk and potential consequences of cyber events, strengthening the security and resilience of cyberspace has become an important homeland security mission.

The United States Government will continue to encourage reporting of intrusions and theft of data by all victims, especially critical infra-structure partners. The prompt reporting of cyber incidents to the Federal Government is essential to an effective response, linking of related incidents, identification of the perpetrators, and prevention of future incidents.

Computer hacking conducted by transnational criminal groups poses a significant threat to our national security. Equipped with sizeable funds, organized criminal groups operating abroad employ sophisticated malicious software, spear-phishing campaigns, and other hacking tools some of which rival those of nation states in sophistication to hack into sensitive financial systems, conduct massive data breaches, spread ransom ware, attack critical infrastructure, and steal intellectual property. The Administration will advocate for law enforcement to have effective legal tools to investigate and prosecute such groups and modernized organized crime statutes for use against this threat.

Deterring cybercrime requires a credible threat that perpetrators will be identified, apprehended, and brought to justice. However, some foreign nations choose not to cooperate with extradition requests, impose unreasonable limitations, or actively interfere in these efforts. The United States will continue to identify gaps and potential mechanisms for bringing foreign-based cyber criminals to justice. The United States Government will also increase diplomatic and other efforts with countries to promote cooperation with legitimate extradition requests. We will push other nations to expedite their assistance in investigations and to comply with any bilateral or multilateral agreements or obligations.

The United States should also aid willing partner nations to build their capacity to address criminal cyber activity. The borderless nature of cybercrime, including state-sponsored and terrorist activities, requires strong inter-national law enforcement partnerships. This cooperation

requires foreign law enforcement agencies to have the technical capability to assist United States law enforcement effectively when requested. It is therefore in the interest of United States national security to continue building cybercrime-fighting capacity that facilitates stronger international law enforcement cooperation. The United States will strive to improve international cooperation in investigating malicious cyber activity, including developing solutions to potential barriers to gathering and sharing evidence. The United States will also lead in developing interoperable and mutually beneficial systems to encourage efficient cross-border information exchange for law enforcement purposes and reduce barriers to coordination. The Administration will urge effective use of existing international tools like the United Nations Convention Against Trans-National Organized Crime and the G7 24/7 Network Points of Contact. Finally, we will work to expand the international consensus favouring the Convention on Cybercrime of the Council of Europe (Budapest Convention), including by supporting greater adoption of the convention.

The United States of America is one of the countries that are experiencing a huge number of cyber-attacks each year. That's why around 58% of the cyber security companies are located there and try to find new ways to fight with the latest attacks.

CHALLENGES

Cybercrime is the fastest growing type of criminal activity in the United States – and it's affecting more and more of us each year.

The United States is highly dependent on the Internet and therefore greatly exposed to cyber-attacks.

It's a measure of the growth of cyber and America's vulnerability to it that the cyber threat was at the top of the list of worldwide threats the director of national intelligence chose to highlight at a Senate Select Committee on Intelligence hearing today.

The United States is under attack -- under attack by entities that are using cyber to penetrate virtually every major action that takes place in the United States. "From U.S. businesses, to the federal government, to state and local governments, the United States is threatened by cyber-attacks every day." Russia, China, Iran and North Korea pose the greatest cyber threats, but others use cyber operations to achieve strategic and malign objectives.

Some of these actors, including Russia, are likely to pursue even more aggressive cyber-attacks with the intent of degrading our democratic values and weakening our alliances. Persistent and disruptive cyber operations will continue against the United States and our European allies, using elections as opportunities to undermine democracy, sow discord and undermine our values.

China also uses cyber to enable espionage and attack capabilities to support its national security and economic priorities. "Iran will try to penetrate U.S. and allied networks for espionage and lay the groundwork for future cyber-attacks. North Korea will continue to use cyber operations to raise funds, launch attacks and gather intelligence against the United States.

CASES

1. **Former AWS engineer arrested for Capital One data breach:**

   Capital One has revealed a data breach affecting 100 million US customers and a further six million in Canada as Federal Bureau of Investigation (FBI) officers arrested a suspect. The US Justice Department said Paige Thompson, 33, a former Seattle technology company software engineer, was arrested on 29 July and charged with computer fraud and abuse for allegedly hacking into the financial firm's data. Thompson appeared briefly

in the Seattle District Court and was ordered to be detained pending a hearing on 1 August, according to Reuters.

2. Twitter Hack:

Twitter took the whole internet by storm when it was hit by one of the most brazen online attacks in history! The social media platform suffered a breach where the hackers verified Twitter accounts of high-profile US personalities like Barack Obama, Elon Musk, Joseph R. Biden Jr., Bill Gates, and many more. Out of 130 targeted accounts, hackers were able to reset 45 user accounts' passwords. Hackers posted fake tweets from these accounts, offering to send $2000 for $1000 sent to an unknown Bit coin address. Reportedly, the **Twitter breach** well-coordinated scam made attackers swindle $121,000 in Bit coin through nearly 300 transactions.

3.Marriott Data Breach:

On March 31st, 2020, the hotel chain Marriott disclosed a security breach that impacted the data of more than 5.2millionhotel guests who used their company's loyalty application.

Hackers obtained login credentials of two accounts of Marriott employees who had access to customer information regarding the loyalty scheme of the hotel chain. They used the information to siphon off the data approximately a month before the breach was discovered.

The data accessed in the breach involved personal details such as names, birthdates, and telephone numbers, travel information, and loyalty program information.

According to the Marriot, hackers might have obtained credentials of their employees either by credential stuffing or phishing. Previously, the hotel giant announced a data breach in late 2018 in which up to 500 millionguests were impacted.

4. MGM Data Dump:

Last year in 2019, MGM Resorts suffered a massive data breach. The news of the breach incident started to circulate in February 2020 when hackers leaked the personal details of 10.6millionhotel guests for free download. But in the later findings, the number increased by 14 times (nearly 142 million) than the number recorded in February 2020. The personal information published on the hacking forum included name, home address, phone numbers, email address, and DOB of guests. The leaked files of guests included Justin Bieber, Twitter CEO Jack Dorsey, and many major government agency officials.

5. Zoom Credentials Up for Sale:

Due to the COVID-19 pandemic, various organizations across the globe adopted work from home policy. In view of the situation, the Zoom video conferencing app became the most used application for the virtual meeting and got popular among cybercriminals too.

Within a short span of time, the application became vulnerable to various security threats and eventually became a victim of the data breach. In the first week of April 2020, the news of 500,000 stolen Zoom passwords available for sale in dark web crime forums shook the application users.

It was reported that more than half a million Zoom account login credentials were up for sale and some of the accounts' credentials were given away for free. In fact, some of the login credentials were sold for less than a US cent each!

Along with account login credentials, victims' personal meeting URLs and Host Keys were available too. The leaked accounts' details belonged to financial institutions, banks, colleges, and various organizations.

6. Magellan Health:

One of Fortune 500 companies, Magellan Health was struck by a ransom ware attack and data breach in April 2020. The healthcare giant confirmed by stating that about 365,000 patientswere affected in the sophisticated cyber-attack.

According to the investigation, the attack was launched with a fully planned process where hackers first installed malware to steal employee login credentials. Then they leveraged a phishing scheme to gain access to systems of Magellan after sending out a phishing email and impersonating as their client before deploying ransom ware attack.

The data thieves were able to steal login credentials of employees, personal information, employee ID numbers, sensitive patient details such as W-2 information, Social Security numbers, or Taxpayer ID numbers.

CYBER SECURITY IN INDIA

The Ministry of Home Affairs released a press statement outlining the current measures the Government has taken to strengthen the country's cyber security. The Government approved a framework to enhance security in Indian cyberspace for cyber security with the National Security Council Secretariat functioning as the nodal agency.

The National Cyber Security Policy, 2013 was developed to build a secure and resilient cyberspace for India's citizens and businesses. The Ministry of Electronics and Information Technology said that the policy aims to protect information and the information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology and cooperation.

India has one of the highest numbers of internet users in the world and is also among the top-10 countries facing cyber-attacks. Today, cyber security issues are not only limited to hacking and money related frauds but also have become critical from a national security point of view. The announcement by the prime minister on Independence Day, that India will soon have a new cyber security policy is timely, as its dependence on cyberspace has increased manifold.

The new policy is expected to address the current gaps and provide a strong framework to handle issues related to cyber security. The policy will focus on major governance reforms. Today, there are many agencies at the national and state levels, looking into cyber security-related issues. However, there is no centralized command to have oversight and coordinate efforts to handle larger cyber security issues.

It is expected that the new cyber security policy would address the issue of protecting critical information infrastructure in cyberspace, build integrated capabilities to prevent and respond to cyber threats, reduce vulnerabilities and minimize damage from cyber incidents through a

combination of institutional structures, people, processes and technology through well-defined governance framework as there is an urgent need of having a comprehensive and unified government institution for creating a cyber defence network.

A holistic cyber security strategy with a possible amendment in the IT Act, as some of its provisions have become redundant and can't address issues arising from the evolving threats.

Government needs to consider creating a Cyber Defence Agency, which is to be entrusted with the responsibility to implement the cyber defence strategy for national security. India is at number 23 of the UN Global Cyber security Index (GCI) 2017. The National Cyber Security Coordinator, it is not a desirable number but is much better than many of the countries on the list. He said that India's target this year is to make it among the top 10.

CHALLENGES

1. Lack of uniformity in devices used for internet access:

With varying income groups in India, not everyone can afford expensive phones. In the US, Apple has over 44% market share. However, in India the iPhones with their higher security norms are used by less than 1% of mobile users. The widening gap between the security offered by the high-end iPhone and lower cost mobiles make it almost impossible for legal and technical standards to be set for data protection by the regulators.

2. Lack of national level architecture for Cyber security:

Critical infrastructure is owned by private sector, and the armed forces have their own firefighting agencies. However, there is no national security architecture that unifies the efforts of all these agencies to be able to assess the nature of any threat and tackle them effectively. The Prime Minister's Office has created a position towards this cause but there is a long way to go before India has the necessary structure in place.

3.Lack of separation:

Unlike countries or states, in cyberspace there are no boundaries, thus making the armed forces, digital assets of ONGC, banking functions, etc. vulnerable to cyber-attacks from anywhere. This could result in security breaches at a national level, causing loss of money, property or lives. To respond to possible threats on the country's most precious resources, there is a need for a technically equipped multi-agency organization that can base its decisions on policy inputs and a sound strategy.

4. Lack of awareness:

As there is no National regulatory policy in place for cyber security there is a lack of awareness at both company level as well as individual level. Domestic natives can protect and be protected from the cyber-attacks only if there is a guided and supervised legal framework.

CASES

1. Cosmos Bank Cyber Attack in Pune:

A recent cyber-attack in India 2018 was deployed on Cosmos Bank in Pune. This daring attack shook the whole banking sector of India when hackers siphoned off Rs. 94.42 crore from Cosmos Cooperative Bank Ltd. in Pune. Hackers hacked into the bank's ATM server and took details of many visas and rupee debit cardholders. Money was wiped off while hacker gangs from around 28 countries immediately withdrew the amount as soon as they were informed.

2. ATM System Hacked:

Around mid-2018, Canara bank ATM servers were targeted in a cyber-attack. Almost 20 lakh rupees were wiped off from various bank accounts. Count of 50 victims was estimated and according to the sources, cyber attackers held ATM details of more than 300 users. Hackers used skimming devices to steal information from debit cardholders. Transactions made from stolen details amounted from Rs. 10,000 to the maximum amount of Rs. 40,000.

UIDAI Aadhaar Software Hacked

2018 started with a massive data breach of personal records of 1.1 Billion Indian Aadhaar cardholders. UIDAI revealed that around 210 Indian Governmentwebsites had leaked Aadhar details of people online.

Data leaked included Aadhaar, PAN and mobile numbers, bank account numbers, IFSC codes and mostly every personal information of all individual cardholders. If it wasn't enough shocking, anonymous sellers were selling Aadhaar information of any person for Rs. 500 over WhatsApp. Also, one could get any person's Aadhaar car printout by paying an extra amount of Rs.300.

3. Hack Attack on Indian Healthcare Websites:

Indian-based healthcare websites became a victim of cyber-attack recently in 2019. As stated by US-based cyber security firms, hackers broke in and invaded a leading India-based healthcare website. The hacker stole 68 lakh records of patients as well as doctors.

4. SIM Swap Scam:

Two hackers from Navi Mumbai were arrested for transferring 4 crore rupees from numerous bank accounts in August 2018. The illegally transferred money from bank accounts of many individuals. By fraudulently gaining SIM card information, both attackers blocked individuals' SIM cards and by the help of fake document posts, they carried out transactions via online banking. They also tried to hack accounts of various targeted companies.

Aforesaid stats and events of the latest cyber-attacks in India are the wake-up call for all those individuals and companies who are still vulnerable to cyber threats

CONCLUSION

In conclusion, though many similarities in frequency of cyber-attacks exist between east and west there are vast differences in nature of attacks, type and intent of perpetrators, cyber-criminal profile, priority and resources for cyber risk management, adequacy of cyber risk response and the paradoxes of cyber-crime response organizations. It is interesting to understand how the nature of cyber-attack is determined by the demographic profile and motive of cyber criminals. The economic growth of any nation and its security whether internal or external and competitiveness depends on how well its cyberspace is secured and protected. The present study could provide a window of opportunity to address the spiralling menace of cybercrime.

Computer security is a vast topic that is becoming more important because the world is becoming highly interconnected, with networks being used to carry out critical transactions.

Cyber-crime continues to diverge down different paths with each New Year that passes and so does the security of the information. The latest and disruptive technologies, along with the new cyber tools and threats that come to light each day, are challenging organizations with not only how they secure their infrastructure, but how they require new platforms and intelligence to do so. There is no perfect solution for cyber-crimes, but we should try our level best to minimize them in order to have a safe and secure future in cyber space.

References

1. https://www.kratikal.com/blog/5-biggest-cyber-attacks-in-india/
2. https://www.toptal.com/finance/finance-directors/cyber-security
3. https://www.websitebuilderexpert.com/blog/us-state-cybercrime-losses/
4. https://www.computerweekly.com/news/252475441/Top-10-cyber-crime-stories-of-2019
5. https://www.fbi.gov/investigate/cyber