"The vicissitude of Cyber Crime Threat Landscape: The past, present and the future".

What is a cyber crime? Cyber crime encompasses any criminal act dealing with computers and networks (called hacking). Additionally, cyber crime also includes traditional crimes conducted through the Internet. For example; hate crimes, telemarketing and Internet fraud, identity theft, and credit card account thefts are considered to be cyber crimes when the illegal activities are committed through the use of a computer and the Internet.
A computer has become the object of the crime or it is used as a tool to commit an offense. A cybercriminal may use a device to access a user's personal information, confidential business information, government information, or disable a device. It is also a cybercrime to sell or elicit the above information online.

Cybercrime is vastly growing in the world of tech today. Criminals of the World Wide Web exploit internet users' personal information for their own gain. They dive deep into the dark web to buy and sell illegal products and services. They even gain access to classified government information.

Cybercrimes are at an all time high, costing companies and individuals billions of dollars annually. What's even more frightening is that this figure only represents the last 5 years with no end in sight. The evolution of technology and increasing accessibility of smart tech means there are multiple access points within users' homes for hackers to exploit. While law enforcement attempts to tackle the growing issue, criminal numbers continue to grow, taking advantage of the anonymity of the internet.

There are many types of cybercrimes. Hacking ,Theft, Cyber Stalking, Identity Theft, Malicious Software, Child soliciting and Abuse are some of them.

Earlier, cybercrime was committed mainly by individuals or small groups. Presently, it is observed that there is highly complex cybercriminal networks bring together individuals at global level in real time to commit crimes.

Today, criminals that indulge in cybercrimes are not motivated by ego or expertise. Instead, they want to use their knowledge to gain profits promptly. They are using their capability to snip, deceive and exploit people as they find it easy to generate money without having to do an honest work. Cybercrimes have become major threat today.

The malicious tie to hacking was first documented in the 1970s when early computerized phones were becoming a target. Tech-savvy people known as "phreakers" found a way around paying for long distance calls through a series of codes. They were the first hackers, learning how to exploit the system by modifying hardware and software to steal long distance phone time. This made people realize that computer systems were vulnerable to criminal activity and the more complex systems became, the more susceptible they were to cybercrime.

Fast Forward to 1990, where a large project named Operation Sundevil was exposed. FBI agents confiscated 42 computers and over 20,000 floppy disks that were used by criminals for illegal credit card use and telephone services. This operation involved over 100 FBI agents and took two years to track down only a few of the suspects. However, it was seen as a great public relations effort, because it was a way to show hackers that they will be watched and prosecuted.

The Electronic Frontier Foundation was formed as a response to threats on public liberties that take place when law enforcement makes a mistake or participates in unnecessary activities to investigate a cybercrime. Their mission was to protect and defend consumers from unlawful prosecution. While

helpful, it also opened the door for hacker loopholes and anonymous browsing where many criminals practice their illegal services.

When talking about the present situation of cybercrimes, according to whitepaper 'Current State of Cybercrime-2019', released by RSA Security (is an American computer and network security company of parent organization Dell Technologies), social media fraud has increased by 43% in 2018. It says the trend will continue in 2019 because of ease of using, absence of fees and multiple other benefits of these platforms.

With Social media platforms like Facebook, Instagram, WhatsApp, Twitter and other legitimate messaging platforms emerging as new ground for criminal deception, cybercriminals are increasingly relying on them to communicate with each other, sell stolen identities, credit card numbers and other ill-gotten gains.

Artifice (fraud) from mobile apps has increased by 680% between 2015 and 2018, with frauds originating in mobile channels growing by 70% in 2018. fraudsters are also undergoing their own form of digital transformation to make cybercrime activity more efficient.

Cybercrime is on the rise-there is no doubt about it. Unfortunately, it doesn't look like things are going to get better anytime in the near future. There will surely be an increase in the number of people around the world that are engaging in cybercrime full-time and an acceleration in sophistication of attack tool and methods.

For example, if we take mobile devices, Laptop encryption will be made mandatory at many government agencies and other organizations that store customer / patient data and will be pre-installed on new equipment. Senior executives, concerned about potential public ridicule, will demand that sensitive mobile data be protected. This development provides a reasonable safety blanket to protect against an epidemic of laptop and PDA theft. Whether the data on the stolen (or lost) laptops is ever read, the mere theft makes the company and its executives subject to security breach disclosure laws and public ridicule. If the data is encrypted, in most cases, the loss does not have to be disclosed.

Other example is that Theft of PDA smart phones will grow significantly. Both the value of the devices for resale and their content will draw large numbers of thieves.

If we take Attack targets, targeted attacks will be more prevalent, in particular against government agencies. Targeted cyber attacks by nation states against US government systems over the past three years have been enormously successful, demonstrating the failure of federal cyber security activities. Other antagonistic nations and terrorist groups, aware of the vulnerabilities, will radically expand the number of attacks. Targeted attacks on commercial organizations will focus on military contractors and businesses with valuable customer information. The most common technique used in targeted attacks against military sites is spear phishing. Spear phishing uses fake emails sent to the employees of a target organization. The email seems to come from a key manager of the target and orders each recipient to load a piece of spyware or to provide log-in information that the attackers use to break in and steal important data.

Cell phone worms will infect at least 100,000 phones, jumping from phone to phone over wireless data networks. Cell phones are becoming more powerful with full-featured operating systems and readily available software development environments. That makes them fertile territory for attackers fuelled by cell phone adware profitability.

Voice over IP (VoIP) systems will be the target of cyber attacks. VoIP is an immature technology that is often deployed hastily in organizations that do not understand the security challenges they will face. A new type of phishing attack is also using VoIP technology to get bank credentials to steal money. The attacker sends an email to a potential victim saying that a bank doesn't want the victim to use the internet but needs some data verified and gives a phone number to call that seems to be in the correct (local) area code (VoIP technology allows people anywhere in the world to appear to have a local phone number in any location they choose). The victim calls the number and is asked to key in or say their account number and password. The criminals use the data to empty the victim's bank account.

In the future the attack techniques may become advanced. Spyware will continue to be a huge and growing issue. The spyware developers can make money so many ways that development and distribution centers will be established throughout the world. One of the more lucrative (for the criminals) types of spyware is keystroke loggers that wait for the victim to sign on to a bank and capture the keystrokes for the user name and password. Banks tried to fight this with graphical point and click password entry, but sophisticated keystroke loggers now also capture the images on which the victim clicks.

Zero-day vulnerabilities will result in major outbreaks resulting in many thousands of PCs being infected worldwide. Security vulnerability researchers often exploit the holes they discover before they sell them to vendors or vulnerability buyers like 'Tipping Point'. The ranks of security researchers is growing rapidly, in part because they can sell what they find to VeriSign’s iDefense or 3Com's Tipping Point. Sadly by the time the researchers sell their discoveries, most have already been used by someone as zero-day attacks breaking into high-value sites.

The majority of bots will be bundled with rootkits. The rootkits will change the operating system to hide the attack's presence and make uninstalling the malware almost impossible without reinstalling a clean operating system. Rootkit sophistication is soaring. Ed Skoudis, SANS Hacker Exploits course director, tells of a tool called the Blue Pill that uses new virtualization features of recent AMD processors to create a practically undetectable rootkit as a virtual machine hypervisor, subverting a system at an extremely deep level, far below the operating system itself.

For now government has taken actions to a certain extent. Government has undertaken number of legislative, technical and institutional measures for addressing cyber security issues and strengthening cyber security system in country. National Cyber Coordination Centre (NCCC) is an operational cyber security and e-surveillance agency in India which is intended to screen communication metadata and co-ordinate intelligence gathering activities of other agencies It generates situational awareness about potential and existing cyber security threats and enables timely sharing of information for proactive, preventive and protective actions by individual entities. National Cyber Security Coordinator (NCSC) under National Security Council Secretariat (NSCS) coordinates with different agencies at the national level for cyber security matters. These are some action taken by now by the government.

To overcome from these attacks in the future also, government will take actions. Congress and state governments will pass more legislation governing the protection of customer information. If Congress, as expected, reduces the state-imposed data breach notification requirements significantly, state attorney generals and state legislatures will find ways to enact harsh penalties for organizations that lose sensitive personal information. Data breach notification laws do make a difference. Executives become very focused on computer security when they fear being shamed on

the front page of the local paper. Sadly the business lobbyists have used their political clout to persuade congressional leaders that state disclosure laws are overly burdensome.

NAC will be used as a defensive strategy mostly in the future. Network access control (NAC) will become common and will grow in sophistication. As defending laptops becomes increasingly difficult, large organizations will try to protect their internal networks and users by testing each computer's attempts to connect to the internal network. Tests will grow from today's simple configuration checks and virus signature validation to deeper analysis searching for traces of malicious code. NAC controls introduce their own security problems. For example they set up quarantine zones where all systems must wait until they are brought up to the current standard. Sophisticated attackers will penetrate the quarantine zones and infect other systems with hard-to-detect rootkits. When the infected systems get their patches updated and are allowed into the sensitive network, the rootkit will still be present, ready to inflict damage or steal information.

By all these things, it can be seen that attacker sophistication seems to be ahead of defensive tools. That is the nature of the war between hackers and defenders: the attackers are always a step ahead. But by making the attackers' job harder and harder and by increasing the length of goal sentences for cybercrime and improving international police co-operation and skill levels, we can continue to keep up with the attackers and, over time, begin to turn the tide.

https://www.avast.com/c-cybercrime

https://www.webopedia.com/TERM/C/cyber_crime.html

https://www.urbanpro.com/class-ix-x-tuition/essay-on-cyber-crime

https://www.pandasecurity.com/mediacenter/panda-security/types-of-cybercrime/

https://www.betternet.co/blog/the-current-state-of-cybercrime/