Assignment 1

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

Before discussed more details about the past, present and future of cyber-crimes, let's see what is meant by cyber-crime.
Cybercrime is any criminal activity that involves a computer, networked device or a network. While most cybercrimes are carried out in order to generate profit for the cybercriminals, some cybercrimes are carried out against computers or devices directly to damage or disable them, while others use computers or networks to spread malware, illegal information, images or other materials. Some cybercrimes do both i.e., target computers to infect them with viruses, which are then spread to other machines and, sometimes, entire networks.

A primary impact from cybercrime is financial, and cybercrime can include many different types of profit-driven criminal activity, including ransomware attacks, email and internet fraud and identity fraud, as well as attempts to steal financial account, credit card or other payment card information. Cybercriminals may target private personal information, as well as corporate data for theft and resale.

Now let's see some definition for the cyber-crime which are given by research driven parties.
The U.S. Department of Justice divides cybercrime into three categories: crimes in which the computing device is the target, for example, to gain network access; crimes in which the computer is used as a weapon, for example, to launch a denial-of-service (DoS) attack; and crimes in which the computer is used as an accessory to a crime, for example, using a computer to store illegally obtained data.
The Council of Europe Convention on Cybercrime, to which the United States is a signatory, defines cybercrime as a wide range of malicious activities, including the illegal interception of data, system interferences that compromise network integrity and availability, and copyright infringements. Other forms of cybercrime include illegal gambling, the sale of illegal items, like weapons, drugs or counterfeit goods, as well as the solicitation, production, possession or distribution of child pornography.
The ubiquity of internet connectivity has enabled an increase in the volume and pace of cybercrime activities because the criminal no longer needs to be physically present when committing a crime. The internet's speed, convenience, anonymity and lack of borders make computer-based variations of financial crimes, such as ransomware, fraud and money laundering, as well as hate crimes, such as stalking and bullying, easier to carry out.

Cybercriminal activity may be carried out by individuals or small groups with relatively little technical skill or by highly organized global criminal groups that may include skilled developers and others with relevant expertise. To further reduce the chances of detection and prosecution, cybercriminals often choose to operate in countries with weak or nonexistent cybercrime laws.
Cyber-crime is a term used to describe the activity of modifying a product or procedure to alter its normal function, or to fix a problem. The term purportedly originated in the 1960s, when it was used to describe the activities of certain MIT model train enthusiasts who modified the operation of their model trains. They discovered ways to change certain functions without re-engineering the entire device. These curious individuals went on to work with early computer systems where they applied their curiosity and resourcefulness to learning and changing the computer code that was used in early programs. Some of their hacks became so successful they outlived the original product, such as the UNIX operating system, developed as a hack by Dennis Ritchie and Keith Thompson of Bell Labs. To the general public a "hack" became known as a clever way to fix a problem with a product, or an easy way to improve its function.

The malicious association with hacking became evident in the 1970s when early computerized phone systems became a target. Technologically savvy individuals, called “phreakers” discovered the correct codes and tones that would result in free long distance service. They impersonated operators, dug through Bell Telephone company garbage to find secret information, and performed countless experiments on early telephone hardware in order to learn how to exploit the system. They were hackers in every sense of the word, using their resourcefulness to modify hardware and software to steal long distance telephone time.

This innovative type of crime was a difficult issue for law enforcement, due in part to lack of legislation to aid in criminal prosecution, and a shortage of investigators skilled in the technology that was being hacked. It was clear that computer systems were open to criminal activity, and as more complex communications became available to the consumer, more opportunities for cyber-crime developed. In 1986 the systems administrator at the Lawrence Berkeley National Laboratory, Clifford Stoll, noted certain irregularities in accounting data. Inventing the first digital forensic techniques, he determined that an unauthorized user was hacking into his computer network. Stoll used what is called a “honey pot tactic,” which lures a hacker back into a network until enough data can be collected to track the intrusion to its source. Stoll’s effort paid off with the eventual arrest of Markus Hess and a number of others located in West Germany, who were stealing and selling military information, passwords and other data to the KGB. The Berkeley lab intrusion was soon followed by the discovery of the Morris worm virus, created by Robert Morris, a Cornell University student. This worm damaged more than 6,000 computers and resulted in estimated damages of $98 million. More incidents began to follow in a continuous, steady stream. Congress responded by passing its first hacking-related legislation, the Federal Computer Fraud and Abuse Act, in 1986. The act made computer tampering a felony crime punishable by significant jail time and monetary fines. In 1990, during a project dubbed Operation Sundevil, FBI agents confiscated 42 computers and over 20,000 floppy disks that were allegedly being used by criminals for illegal credit card use and telephone services. This two-year effort involved 150 agents. Despite the low number of indictments, the operation was seen as a successful public relations effort by law enforcement officials. Garry M. Jenkins, the Assistant Director of the U.S. Secret Service, explained at a press conference that this activity sent a message to criminals that, “they were on the watch everywhere, even in those sleazy and secretive dens of cybernetic vice, the underground boards.”

Cybercrime ranges across a spectrum of activities. At one end are crimes that involve fundamental breaches of personal or corporate privacy, such as assaults on the integrity of information held in digital depositories and the use of illegally obtained digital information to blackmail a firm or individual. Also at this end of the spectrum is the growing crime of identity theft. Midway along the spectrum lie transaction-based crimes such as fraud, trafficking in child pornography, digital piracy, money laundering, and counterfeiting. These are specific crimes with specific victims, but the criminal hides in the relative anonymity provided by the Internet. Another part of this type of crime involves individuals within corporations or governments deliberately altering data for either profit or political objectives. At the other end of the spectrum are those crimes that involve attempts to disrupt the actual workings of the Internet. These range from spam, hacking, and denial of service attacks against specific sites to acts of cyberterrorism. That is, the use of the Internet to cause public disturbances and even death. Cyberterrorism focuses upon the use of the Internet by non-state actors to affect a nation’s economic and technological infrastructure. Since the September 11 attacks of 2001, public awareness of the threat of cyberterrorism has grown dramatically. Cybercrime affects both a virtual and a real body, but the effects upon each are different. This phenomenon is clearest in the case of identity theft. In the United States, for example, individuals do not have an official identity card but a Social Security number that has long served as a de facto identification number. Taxes are collected on the basis of each citizen’s Social Security number, and many private institutions use the number to keep track of their employees, students, and patients. Access to an individual’s Social Security number affords the opportunity to gather all the documents related to that person’s citizenship (i.e., to steal his identity. Even stolen credit card information can be used to reconstruct an individual’s identity) Although identity theft takes places in many countries, researchers and lawenforcement officials are plagued by a lack of information and statistics about the crime worldwide. Cybercrime is clearly, however, an international problem.

In 2015 the U.S. Bureau of Justice Statistics (BJS) released a report on identity theft. The BJS report showed that while the total number of identity theft victims in the United States had grown by about 1 million since 2012, the total loss incurred by individuals had declined since 2012 by about $10 billion to $15.4 billion. Most of that decline was from a sharp drop in the number of people losing more than $2,000. Most identity theft involved small sums, with losses less than $300 accounting for 54 percent of the total. Internet related frauds are another growing threat which schemes to defraud consumers abound on the Internet. Among the most famous is the Nigerian, or “419,” scam. The number is a reference to the section of Nigerian law that the scam violates. Although this con has been used with both fax and traditional mail, it has been given new life by the Internet. In the scheme, an individual receives an e-mail asserting that the sender requires help in transferring a large sum of money out of Nigeria or another distant country. Usually, this money is in the form of an asset that is going to be sold, such as oil, or a large amount of cash that requires “laundering” to conceal its source; the variations are endless, and new specifics are constantly being developed. The message asks the recipient to cover some cost of moving the funds out of the country in return for receiving a much larger sum of money in the near future. Should the recipient respond with a check or money order, he is told that complications have developed; more money is required. Over time, victims can lose thousands of dollars that are utterly unrecoverable.

In 2002 the newly formed U.S. Internet Crime Complaint Center (IC3) reported that more than $54 million dollars had been lost through a variety of fraud schemes. This represented a threefold increase over estimated losses of $17 million in 2001. The annual losses grew in subsequent years, reaching $125 million in 2003, about $200 million in 2006, close to $250 million in 2008, and over $1 billion in 2015. In the United States the largest source of fraud is what IC3 calls “non-payment/non-delivery,” in which goods and services either are delivered but not paid for or are paid for but not delivered. Unlike identity theft, where the theft occurs without the victim’s knowledge, these more traditional forms of fraud occur in plain sight. The victim willingly provides private information that enables the crime, hence, these are transactional crimes. Few people would believe someone who walked up to them on the street and promised them easy riches, however, receiving an unsolicited e-mail or visiting a random Web page is sufficiently different that many people easily open their wallets. Despite a vast amount of consumer education, Internet fraud remains a growth industry for criminals and prosecutors. Europe and the United States are far from the only sites of cybercrime. South Korea is among the most wired countries in the world, and its cybercrime fraud statistics are growing at an alarming rate. Japan has also experienced a rapid growth in similar crimes.

Ransomware and cryptojacking were go-to moneymakers for cyber criminals. But 2018 brought diminishing returns, resulting in lower activity.For the first time since 2013, ransomware declined, down 20 percent overall, but up 12 percent for enterprises.

With a 90 percent plunge in the value of cryptocurrencies, cryptojacking fell 52 percent in 2018. Yet, cryptojacking remains popular due to a low barrier of entry and minimal overhead; Symantec blocked four times as many cryptojacking attacks in 2018 compared to the previous year.

Living off the land techniques allow attackers to hide inside legitimate processes. For example, the use of malicious PowerShell scripts increased by 1000 percent last year.

Attackers also increased their use of tried-and-true methods, like spear-phishing, to infiltrate organizations. While intelligence gathering remains their primary motive, attack groups using malware designed to destroy and disrupt business operations increased by 25 percent in 2018.

Twenty leaders in cyber security, including representatives from the SANS Institute, directors from the Internet Storm Center and US state chief information security officers (all listed at the end of the article) worked together to reach consensus on the top 10 security developments for future. They narrowed 40 probable computer security developments down to 10 that have the highest probability of happening and will, if they happen, have substantial impact on large numbers of people.

These developments are coming about in an environment of rapidly skyrocketing financial cybercrime (more than 400 per cent year over year growth in most large banks), deep penetration of government and other sensitive sites, increasing numbers of people around the world that are engaged in cybercrime full-time and accelerating sophistication of attack tool and methods. We have divided them into five groups like those involving mobile devices, attack targets, attack techniques, government action and defensive strategies.

Laptop encryption will be made mandatory at many government agencies and other organisations 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. 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.

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 organisations 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 organisation. 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 organisations 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.

Spyware will continue to be a huge and growing issue. The spyware developers can make money so many ways that development and distribution centres 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 'TippingPoint'. The ranks of security researchers is growing rapidly, in part because they can sell what they find to Verisign's iDefense or 3Com's TippingPoint. 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. 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 organisations 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. Committee chairmen in the US House of Representatives have drafted federal laws that eliminate much of the responsibility of business to disclose losses. The result will be a significant decline in management concern about security.

Cybercrime is becoming harder to stop as new technologies emerge, its impacts widespread and overwhelming financially. It effects to the confidentiality, integrity and availability of data. It’s important to act now in order to slow its progress. Through increased awareness, improved laws which target cybercrime and by utilizing biometrics which greatly enhance security, the effects of cybercrime will be mitigated. As explored before, cyber criminals will only continue to find motivation in cybercrime when they are faced with such low risks. Governments’ lack of funding and effort to take cybercrime seriously enough is only going to allow cybercrime to continue growing. The potentially shocking financial gains available will also only serve to motivate them even more. The fact that some statistics are a little out of date highlights limitations in accuracy but still serves the purpose in depicting the growth of cybercrime. Biometric technology is still developing and at the moment has certain limitations in regards to how accurately it can work or whether it’s really an efficient way to go. Great areas for future research would be the growth in biometric technology and seeing how it will develop over time, as it should be a key area in securing one’s personal information, not just for large organizations but for individuals at home as well.

Above we discussed the growth of the cyber-crimes and its future. We cannot assure that we are secure even we use all of the security precautions, because the field of cyber-crime becomes very big day by day rapidly. We have to always care about our internet security when we are dealing with modern devices because we may be the next victim.