Combating computer crime:

It is difficult to find and combat cyber crime's perpetrators due to their use of the internet in support of cross-border attacks. Not only does the internet allow people to be targeted from various locations, but the scale of the harm done can be magnified. Cyber criminals can target more than one person at a time. The availability of virtual spaces to public and private sectors has allowed cybercrime to become an everyday occurrence.In 2018, The Internet Crime Complaint Center received 351,937 complaints of cybercrime, which lead to $2.7 billion lost.

Common examples of cybercrime Some of the more commonly seen cybercrime attacks include **distributed DoS (DDoS)** attacks, which are often used to shut down systems and networks. This type of attack uses a network's own communications protocol against it by overwhelming its ability to respond to connection requests. DDoS attacks are sometimes carried out simply for malicious reasons or as part of a cyberextortion scheme, but they may also be used to distract the victim organization from some other attack or exploit carried out at the same time.

Infecting systems and networks with malware is an example of an attack used to damage the system or harm users. This can be done by damaging the system, software or data stored on the system. Ransomware attacks are similar, but the malware acts by encrypting or shutting down victim systems until a ransom is paid.

Phishing campaigns are used to infiltrate corporate networks by sending fraudulent emails to users in an organization, enticing them to download attachments or click on links that then spread viruses or malware to their systems and through their systems to their company's networks.

A credentials attacks is when a cybercriminal aims to steal or guess user IDs and passwords for the victim's systems or personal accounts. They can be carried out through the use of brute-force attacks by installing keylogger software or by

exploiting vulnerabilities in software or hardware that can expose the victim's credentials.

Cybercriminals may also attempt to **hijack a website** to change or delete content or to access or modify databases without authorization. For example, an attacker may use an Structured Query Language (SQL) injection exploit to insert malicious code into a website, which can then be used to exploit vulnerabilities in the website's database, enabling a hacker to access and tamper with records or gain unauthorized access to sensitive information and data, such as customer passwords, credit card numbers, personally identifiable information (PII), trade secrets and IP.

Other common examples of **cybercrime include illegal gambling, the sale of illegal items -- like weapons, drugs or counterfeit goods -- and the solicitation, production, possession or distribution of child pornography.**

Effects of cybercrime on businesses

The true cost of cybercrime is difficult to assess accurately. In 2018, McAfee released a report on the economic impact of cybercrime that estimated the likely annual cost to the global economy was nearly $600 billion, up from $45 billion in 2014.

While the financial losses due to cybercrime can be significant, businesses can also suffer other disastrous consequences as a result of criminal cyberattacks, including the following:

- Damage to investor perception after a security breach can cause a drop in the value of a company.

- In addition to potential share price drops, businesses may also face increased costs for borrowing and greater difficulty in raising more capital as a result of a cyberattack.
- Loss of sensitive customer data can result in fines and penalties for companies that have failed to protect their customers' data. Businesses may also be sued over the data breach.
- Damaged brand identity and loss of reputation after a cyberattack undermine customers' trust in a company and that company's ability to keep their financial data safe. Following a cyberattack, firms not only lose current customers, but they also lose the ability to gain new customers.
- Businesses may also incur direct costs from a criminal cyberattack, including increased insurance premium costs and the cost of hiring cybersecurity companies to do incident response and remediation, as well as public relations (PR) and other services related to an attack.

Effects of cybercrime on national defense

Cybercrimes may have public health and national security implications, making computer crime one of DOJ's top priorities. In the United States, at the federal level, the Federal Bureau of Investigation's (FBI) Cyber Division is the agency within DOJ that is charged with combating cybercrime. The Department of Homeland Security (DHS) sees strengthening the security and resilience of cyberspace as an important homeland security mission, and agencies such as the U.S. Secret Service (USSS) and U.S. Immigration and Customs Enforcement (ICE) have special divisions dedicated to combating cybercrime.

USSS' Electronic Crimes Task Force (ECTF) investigates cases that involve electronic crimes, particularly attacks on the nation's financial and critical infrastructures. USSS also runs the National Computer Forensics Institute (NCFI),

which provides state and local law enforcement, judges and prosecutors with training in computer forensics. The Internet Crime Complaint Center (IC3), a partnership among the FBI, the National White Collar Crime Center (NW3C) and the Bureau of Justice Assistance (BJA), accepts online complaints from victims of internet crimes or interested third parties.

How to prevent cybercrime

Some steps for resisting cybercrime include the following:

- develop clear policies and procedures for the business and employees;
- create cybersecurity incident response management plans to support these policies and procedures;
- outline the security measures that are in place about how to protect systems and corporate data;
- use two-factor authentication (2FA) apps or physical security keys;
- activate 2FA on every online account when possible;
- verbally verify the authenticity of requests to send money by talking to a financial manager;
- create intrusion detection system (IDS) rules that flag emails with extensions similar to company emails;
- carefully scrutinize all email requests for transfer of funds to determine if the requests are out of the ordinary;
- continually train employees on cybersecurity policies and procedures and what to do in the event of security breaches;

- keep websites, endpoint devices and systems current with all software release updates or patches; and
- back up data and information regularly to reduce the damage in case of a ransomware attack or data breach.

Information security and resistance to cybercrime attacks can also be built by encrypting all computers' local hard disks and email platforms, using a virtual private network (VPN) and by using a private, secured domain name system (DNS) server.

Cybercrime legislation and agencies

As mentioned above, various U.S. government agencies have been established to deal specifically with the monitoring and management of cybercrime attacks. The FBI's Cyber Division is the lead federal agency for dealing with attacks by cybercriminals, terrorists or overseas adversaries. Within DHS is the Cybersecurity and Infrastructure Security Agency (CISA). This group coordinates between private sector and government organizations to protect critical infrastructure.

Furthermore, the Cyber Crimes Center (C3) provides computer-based technical services that support domestic and international investigations included in the Homeland Security Investigations (HSI) portfolio of immigration and customs authorities. C3 focuses on cybercrimes that involve transborder illegal activities; it is responsible for finding and targeting all cybercrimes within HSI jurisdiction. C3 includes the Cyber Crimes Unit (CCU), the Child Exploitation Investigations Unit (CEIU) and the Computer Forensics Unit (CFU).

Various laws and legislation have been enacted in addition to the agencies that have been established to deal with cybercrime. In 2015, the United Nations Office on Drugs and Crime (UNODC) released the cybercrime repository, which is a central database that includes legislation, previous findings, and case law on

cybercrime and electronic evidence. The intention of the cybercrime repository is to assist countries and governments in their attempts to prosecute and stop cybercriminals.

Legislation dealing with cybercrime can be applicable to the general public, or it can be sector-specific, extending only to certain types of companies. For example, the Gramm-Leach-Bliley Act (GLBA) focuses on financial institutions and regulates the implementation of written policies and procedures that should improve the security and confidentiality of customer records, while also protecting private information from threats and unauthorized access and use.

Other legislation has been established to deal with specific cybercrimes, such as cyberbullying and online harassment. A little over half of U.S. states have implemented laws dealing directly with these crimes.

Investigation:

- A computer can be a source of evidence (see digital forensics). Even where a computer is not directly used for criminal purposes, it may contain records of value to criminal investigators in the form of a logfile.
- In most countries Internet Service Providers are required, by law, to keep their logfiles for a predetermined amount of time. For example; a European wide Data Retention Directive (applicable to all EU member states) states that all e-mail traffic should be retained for a minimum of 12 months.
- There are many ways for cybercrime to take place, and investigations tend to start with an IP Address trace, however, that is not necessarily a factual basis upon which detectives can solve a case.
- Different types of high-tech crime may also include elements of low-tech crime, and vice versa, making cybercrime investigators an indispensable part of modern law enforcement. Methods of cybercrime detective work are dynamic and constantly improving, whether in closed police units or in international cooperation framework.
- In the United States, the Federal Bureau of Investigation (FBI) and the Department of Homeland Security (DHS) are government agencies that combat cybercrime. The FBI has trained agents and analysts in cybercrime placed in their field offices and headquarters.Under the DHS, the Secret

Service has a Cyber Intelligence Section that works to target financial cyber crimes. They use their intelligence to protect against international cybercrime. Their efforts work to protect institutions, such as banks, from intrusions and information breaches. Based in Alabama, the Secret Service and the Alabama Office of Prosecution Services work together to train professionals in law enforcement through the creation of The National Computer Forensic Institute.This institute works to provide "state and local members of the law enforcement community with training in cyber incident response, investigation, and forensic examination in cyber incident response, investigation, and forensic examination.

- Due to the common use of encryption and other techniques to hide their identity and location by cybercriminals, it can be difficult to trace a perpetrator after the crime is committed, so prevention measures are crucial.

Legislation

- Agencies, such as the FBI, have used deception and subterfuge to catch criminals.
- Then-President Barack Obama released in an executive order in April 2015 to combat cybercrime. The executive order allows the United States to freeze assets of convicted cybercriminals and block their economic activity within the United States. This is some of the first solid legislation that combats cybercrime in this way.

Penalties:

Some hackers have been hired as information security experts by private companies due to their inside knowledge of computer crime, a phenomenon which theoretically could create perverse incentives..These approaches involve restricting individuals to specific devices which are subject to computer monitoring or computer searches by probation or parole officers.

Awareness:

As technology advances and more people rely on the internet to store sensitive information such as banking or credit card information, criminals increasingly attempt to steal that information. Cybercrime is becoming more of a threat to people across the world. Raising awareness about how information is being

protected and the tactics criminals use to steal that information continues to grow in importance. Anybody who uses the internet for any reason can be a victim, which is why it is important to be aware of how one is being protected while online. Users of internet should use unique passwords, run anti-virus software, watch suspicious emails and do not open such type of programs coming from unknown sources.

Agencies:

- Cyber Crime Investigation Cell, a wing of Mumbai Police, India