Cyber Warrior Team

written by iasexam.com | 07/03/2023

Context- Visakhapatnam's "Cyber Warrior" teams and help desks are being used to combat the rising cybercrime.

Key Highlights

- As compared to 316 cases reported in 2021, Visakhapatnam had reported as many as 610 cases of cybercrime in 2022—a nearly 93% increase.
- All of the city's police stations will soon have their own "cyber warriors" teams to handle cases like these to stop the rise in cybercrime.
- In addition, within the next two months, all police stations will have cybercrime help desks.

About Cyber Warriors

- Around 70 police officers, including around 20 sub-inspectors and a few ASIs, will receive online and offline training on various aspects of cybercrime as part of the initiative.
- A Sub-Inspector and staff will be in charge of the Cyber Warriors team.
- The employees will be taught about various aspects of the reported cases of cybercrime, including how cyber fraudsters operate.
- The police plan to implement the cyber sentinel concept, in which at least one person in each colony or area will receive training in basic cybercrime prevention techniques and raise public awareness.
- After a cybercrime has been committed, employees will also receive technical skills

training to initiate immediate communication with data operators and bank authorities.
- The goal is to prevent money from being transferred to con artists by freezing accounts, stopping money transfers, and retrieving call data records.

Cybercrime in India: (NCRB Report)

- India reported nearly 52,974 incidents of cybercrime, nearly 6 percent more than in 2020.
- The state with the most cases of cybercrime was Telangana, which had more than 19% of the total.
- The number of cases involving cybercrime decreased by 24% and 20%, respectively, in Karnataka and Uttar Pradesh.
- Jurisdictional issues and difficulties obtaining electronic logs from foreign service providers are the primary obstacles to cybercrime prosecution.
- Cybercrime cases have decreased over the past three years, but Bengaluru had the highest number.
- Nearly 61% of cases involved fraud, making it the most common reason for cybercrime.
- In 2021, Karnataka had the most cases of cybercrime against women, with 2,243.
- In cases of cybercrime, the percentage of police pendency increased from 71.3% in 2020 to 56.4% in 2021.
- The charge-sheeting rate decreased from 47.5 percent in 2020 to 33.8 percent in 2021, and the conviction ratio for cases involving cybercrime remains low.
- With 81.4% of all trials remaining in 2021, the court pendency rate remained high. at the end of the year, pending.

Challenges of Cybercrime:

- **A Lack of Awareness-** In India, many people are still unaware of the dangers of cybercrime, making them more susceptible to attacks.
- **Low awareness of cybersecurity:** In India, a lot of people and businesses don't know much about cybersecurity, which makes them easy targets for hackers.
- **The Cyber Threat Landscape Is Rapidly Changing:** Cybercrime is constantly evolving, with new threats appearing on a regular basis. Law enforcement agencies find it difficult to keep up with these developments.
- **Limited infrastructure for cybersecurity**: Many organizations do not have adequate security measures in place to safeguard their networks and data because the cybersecurity infrastructure in India is still in its infancy.
- **Increasing Technology Use:** In India, the widespread adoption of technology increases the number of people who are susceptible to cybercrime, making its prevention and detection even more challenging.
- **Cybercrime laws are lacking:** India's laws on cybercrime are out of date and not up to date with current threats. To combat the ever-evolving landscape of cybercrime, updated laws must be enacted.

Need for controlling cyber crimes in India

- **Increasing Digitalization**: India's growing digitalization has increased the number of people who use online services and technology, which has raised the number of cases of cybercrime.
- **Financial Impact:** India's economy suffers greatly from cybercrime, which results in annual losses of billions of dollars. Additionally, the nation is missing out on potential investments as a result of cybersecurity concerns.
- **Security in the Nation:** Cybercrime can compromise sensitive information and infrastructure, compromising national security and potentially causing political instability.
- **Private Life:** Identity theft, financial fraud, and other forms of cyberstalking can all result from cybercrime, which can violate personal privacy.
- **Jobs in cyber security**: There are job opportunities in India as a result of the growing importance of cybersecurity and the demand for skilled professionals in the field.
- **Initiative for Digital India:** The Digital India initiative launched by the Indian government aims to make India a digitally empowered society and knowledge economy. Cybercrime, on the other hand, may impede the initiative's progress and damage public confidence in digital technologies.

Cybercrime laws in India

- **Information Technology Act, 2000:** In India, this is the primary law that regulates cybercrime. Cybercrime punishments, procedures for handling investigations and prosecutions, and legal recognition of electronic transactions are provided by the act.
- **The Indian Penal Code:** Cybercrime, such as identity theft, online stalking, hacking, and the dissemination of obscene materials, is addressed by the IPC.
- **Aadhaar Act, 2016**: Aadhaar, a biometric identification system, is governed by this law, which also provides penalties for unauthorized access to or misuse of Aadhaar data.
- **Copyright Act, 1957:** Intellectual property rights, such as trademarks, patents, and copyrights, are safeguarded by this law, as are penalties for intellectual property theft committed online.
- **Right to Information Act 2005** : Cybercrime involving unauthorized access to public information is punishable by this law, which grants citizens access to information provided by public authorities.
- **Prevention of Money Laundering Act, 2002** Cybercrime connected to money laundering is punishable under this law, which aims to stop money laundering.

Way ahead

- Cybercrime poses a significant threat to India's economy, national security, and personal privacy.
- To combat cybercrime and establish a safe and secure digital environment in the nation, proactive measures are required.
- This is why cyber warriors are important, especially since India ranks fifth globally in terms of reported incidents.