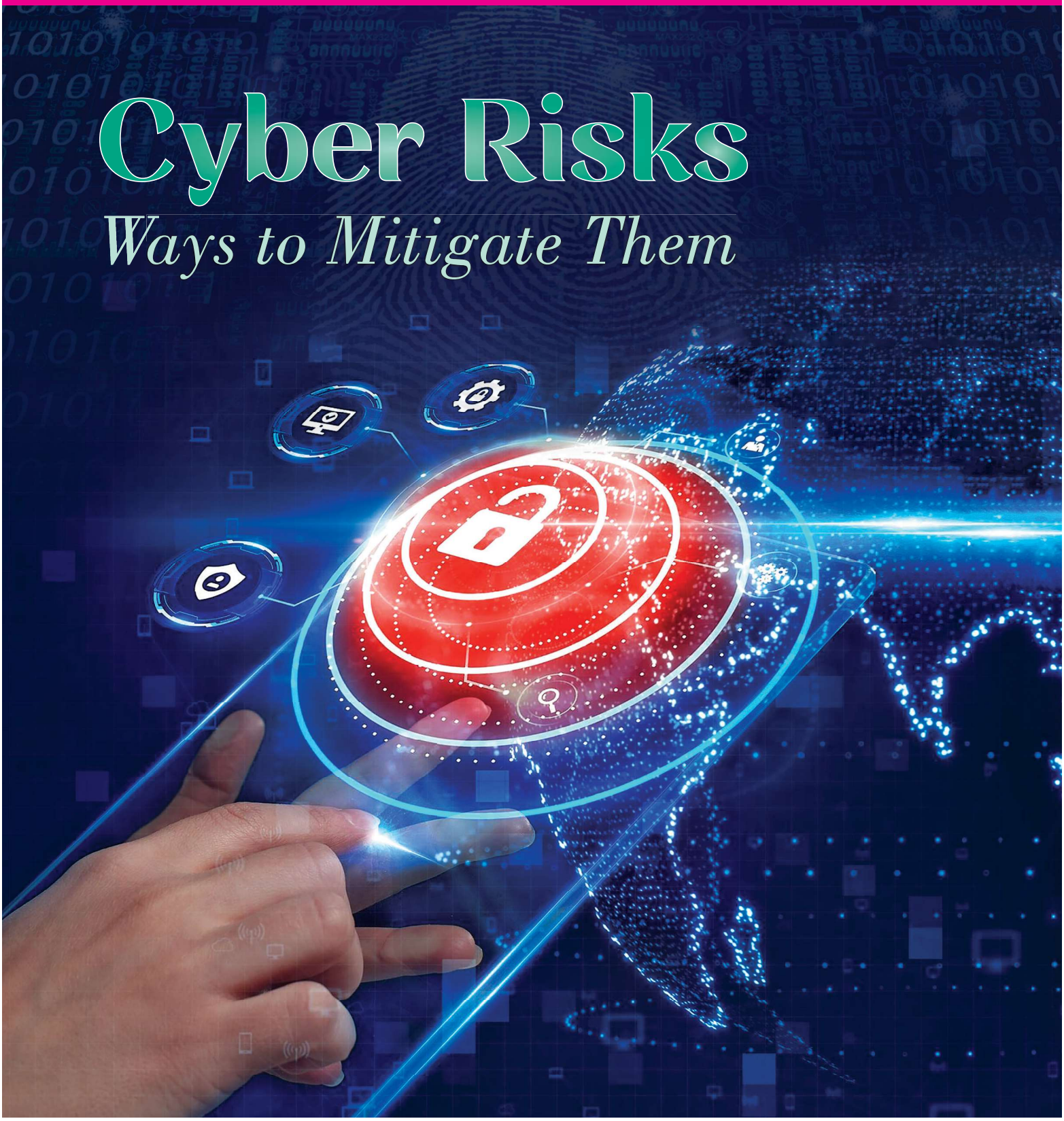
The Kolkata
PROTECTOR
Vol 11 Issue 3 2022 Rs. 50/-
NEW MEDIA
Adding A Cutting Edge To The Digital Age
www.theprotector.in
A Magazine for the Kolkata Police
PROMOTING PEACE

Cyber Risks

Ways to Mitigate Them




KOLKATA POLICE FORCE
सत्यमेव जयते

Changing Face of Cybercrime and Preparedness of Police to Crack Such Cases

In this dazzling world, hardly any work can be done without the help of technology and the internet. In the present era, people are going for modernization and digitalization at such a fast pace so that its ill effects are drastically being felt in modern society. But for some point of time we can ignore its ill effects, as certain serious issues need to be addressed immediately. For example, the investigation and control of crimes such as cyber fraud, stalking, harassment, pornography, sexting, espionage and ransomware are the pressing concerns.

According to the NCRB report, cyber-crime has registered a growth of around 12% in the year 2020. During 2020, 60.2% of the total cybercrime cases registered were for fraud (30,142 out of 50,035 cases), followed by sexual abuse with 6.6% (3,293 cases) and extortion with 4.9% (2,440 cases). These figures are probably incomplete, as only one third of cybercrime cases are registered in India and many complaints never get converted into

FIRs. The reality is that cybercrime is increasing at a rate of about 200% every year and new threats are emerging. The police and the law machinery will have to make extensive preparations to control the rising cybercrime cases.

Upcoming Cyber Threats

Today, mainly cases related to financial frauds, and digital account hackings are coming to the fore. In the future, many new and serious cyber threats are going to come out. This would not only be new in methodology, but would also require a state-of-the-art cyber lab along with a skilled team to deal with it.

Data theft, hijacking and alteration would be the huge threats to every government and non-government organizations. For example, in digitisation today almost every hospital has started to put the diagnosis and consultation data of patients online. And in many high-tech hospitals, the treatment is also fully automated, where the machinery determines the oxygen level for the patient and the amount of medicine in the glucose bottle. If the hacker is able to hack the automation and smart hospital system, it can cause the hospital system to malfunction and even cause loss of life. Similarly, hacking of Internet of Things (IOT) and smart vehicles can also have dire consequences.

Guidelines

To prevent cyber crimes, the Government of India regularly issues guidelines for many social media and online service providers. In February, 2020, the Indian government had issued an official guideline for social media intermediaries and OTT platforms. India's former IT, Law and Justice Minister Ravi Shankar Prasad had said that "Social media companies should accept requests to remove illegal, misleading and violent content within 24 hours and provide full redress within 15 days".

On 28 April, 2022, the Indian Computer Emergency Response Team (CERT-In) issued new directions under Section 70B (6) of the Information Technology Act, 2000 (IT Act), that it is mandatory for service providers, intermediaries, data centres, companies and government organizations to report cyber incidents within six hours.

Preparedness of Police

Nowadays, criminals are using high-end computer devices and virtual platforms. They are quite capable of hiding their identity with the help of virtual private network (VPN), virtual number, temporary email ID and rented bank accounts. Therefore, the investigating approach and methodology of the police should fasten their belts to be able to crackdown on cyber incidents of the next level. Every police station should have a strong capability to investigate cyber-crime cases effectively.

The cyber forensic laboratory should have sufficient capacity and bandwidth to examine all digital devices, cloud and online accounts in a short time. Today, it takes many months to get the evidence test report from digital forensic labs because the number of labs are few, and on top of that many labs do not have enough equipment, and many do not have skilled manpower. To effectively handle new cyber-crime cases, police personnel should be given case study oriented training regularly. Several crucial changes need to be implemented in the police recruitment process, such as a special drive to recruit cyber experts.

Preparedness of Judiciary

The Indian judicial system, which has been running for the last 73 years, probably does not have the power to take tough decisions in cases related to cybercrime. There can be two possible reasons for this, firstly the vastness of the cases pending in the court and secondly the lawyers and judges do not have enough knowledge of the cyber world. There is a dire need to enact a strict law to make the judiciary more strong and effective. Along with the new law, there is also a need to amend the IT Act 2000 so that all avenues of escape for criminals are closed and almost every offence should be made non-bailable.

Dedicated courts and trained judges should be arranged for cyber-crime cases. Lawyers and judges should be trained regularly to make the judicial system more reliable and effective.There should be strict provision of punishment and fine in the law so that no one dares to commit such an offence.

Author:
Ummed Meel
Designation: Cyber Expert (Police and Defence Advisor)
Education: B Tech, LLB (Cyber Law), CISA, CEH, CHFI, DCL

Ummed Meel is a renowned cyber expert (Police and Defence Advisor). He has been invited as an expert in more than 100 training and workshops on cybersecurity, intelligence, and cybercrime Investigation for Ministries including State Police, India Air Force, BSF, CISF, CAG, BPRD, CDTI and other law enforcement agencies. He has 7+ years of experience in cybersecurity, VAPT, Digital Forensics and Cybercrime Investigation. His articles have been published in many world renowned magazines. He has also been interviewed by several news channels and newspapers for expert views on cybercrime. In addition, he has delivered over a hundred lectures in seminars on cyber-crime awareness in schools, colleges and universities. He has also assisted various investigative agencies in solving around 200 major cases related to cyber-crime in the country.