Cyberspace and Cyber Crime Monitoring Framework, Policy and Protocols

The Internet has helped society evolve quickly & better. People, companies and organisations have already switched to the online mode and started sharing the information from one system to another to serve their customer or clients. Due to the fact that every information travels from one place to another in the cyberworld and the way of transferring the data may or may not be secure all the time. Not every system is perfectly safe. Bad actors find the vulnerable points of the system or service they want to hack and they exploit to get the hold of other's sensitive data & misuse. Cyber threats have grown exponentially. Consequently, cyberspace has become a war-fighting domain with the potential to destroy or make use-less logical, physical, and virtual infrastructure, and to damage critical national capabilities. There comes a huge requirement of the Cyberspace and Cyber Crime monitoring frameworks & security policies. Monitoring is the process of detecting cyber threats and data breaches in the IT infrastructure, systems or networks. It is a crucial part of cyber risk management to analyse the threats in their infancy and respond to them before they can cause any damage. There are different monitoring tools available. Network security monitoring tools analyse the security logs from various sources. Popular monitoring tools include SIEM (Security Incident and Event Management Systems), IDS (Intrusion Detection Systems), and Behaviour Analysis Systems. One must include Behaviour analysis & code analysis tools to the programs that are running on their servers to keep an eye on their behaviour and prevent unknown code (or malware) from stealing or controlling it. Another important type of monitoring is Endpoint Security Monitoring, its tools & technologies provide security visibility at the host level, enabling the security teams to detect the threats earlier and prevent it from happening. Its tools include Endpoint Detection and Response (EDR) and Endpoint Protection Platforms (EPP). These monitoring frameworks ensure the swift response to the cyber incidents accelerating the Incident Response (IR) and makes the process more efficient by taking necessary automated actions & elevating the security capabilities. The objective of the Security Monitoring Policy is to ensure that information security and technology security controls working as per the requirements. Security monitoring is advantageous in early identification of security issues or new security vulnerabilities. Other advantages include

compliance with a security audit, FERBA, HIPAA. FERPA and HIPAA, both intended to protect the information of individuals or organisations and prevent anyone without authority from accessing the data. One must consider the CIA Triad for their data & services. It comprises Confidentiality (preserving authorized restrictions on information access and disclosure), Integrity (guarding against unauthorized modification or destruction of the information), Availability (ensuring timely and reliable access to information and its use). Additional concepts are Authenticity (verifying the users & inputs arriving at the system came from a trusted source) and Accountability (the requirement for actions of an entity to be traced uniquely to that entity, which supports nonrepudiation, fault isolation, intrusion detection & prevention, after-action recovery and legal action). Security protocols are also a significant part of data security. They are plans, protocols, actions and measures that help to keep your data safe (which is a prominent asset in today's cyber world) from various security incidents. Popular security protocols consist of Firewalls, Encryption, Incident Response (IR) & Incident Management, and Education (making the employees aware of the types of attacks and their working). There are acts like Information Technology Act (IT Act) 2000, the Indian Penal Code (IPC), and the Indian CopyRight Act of 1957 to address copyright infringement, trademark infringement, to a wide range of cybercrimes including identity theft, credit card fraud and other computer & internet related crimes. One should be aware of them to take the right action if something like that happens to him or his organization. The concerns have been raised that using AI for offensive purposes may make cyberattacks increasingly difficult to block or defend against by enabling rapid adaptation of malware to adjust to restrictions imposed by countermeasures and security controls. We need to incorporate AI into its cyber defenses to proactively detect and mitigate threats that require a speed of response far greater than human decision-making allows. There's a need for careful control over both the training datasets that are used to build AI models and the inputs that those models are then provided with to ensure security of machine-learning-enabled decision-making processes. Many security-focused policies by the government of different countries for AI have emphasized the importance of transparency, testing, and accountability for algorithms and their developers, by defining some baseline requirements. Making yourself & your employees aware of the attacks, and applying monitoring tools & security frameworks, policies, and protocols can keep your data prevented from being stolen or systems hacked.