Scope of Cybersecurity

Physical Infrastructure Security: Control of physical and digital access to confidential information system infrastructure and resources. This covers asset management, asset classification, asset disposal, acceptable usage, environmental protection, protection from natural disasters, access control, and surveillance, etc.

Network & Internet Security: Protecting networking infrastructure against threats and mitigating such threats originating from external, and internal networks. The absence of proper access control and protection can lead to an internet-based attack that includes unauthorized access from the internet spread of the virus, worms, malware, etc. There could be unsecured transit on the network that can lead to unauthorized access leading to loss of critical & sensitive information.

Application Security: Applications are vulnerable to various kinds of attacks, which are exploited by malicious activity. Computer software owned or licensed must not be copied by users; employees and others for use at home or any other location.

To determine appropriate risk response options, identify performance gaps between current and desired risk levels. The risk associated with IT systems whether appropriate and effectively mitigated to an acceptable level by securing **Operating Systems**.

The enterprises need to define and develop adequate controls to secure its **Database**.

The enterprises must be protected against vulnerability due to viruses and attacks by Trojans and malicious codes. Hence IT assets must use enterprise-level **Anti-virus** solutions on the system.

Generally the user and customer gain access to information/data through user-ID and the **Password** provided for securing transactions. Access to systems should be strictly limited for the genuine business purposes with the complement of User ID and password.

E-mail ID and access made available to employees purely based on business needs. The enterprises will protect the system with appropriate technology and other means against the breach or unauthorized access.

Awareness & Training: At the enterprise level user awareness is the biggest protection against any kind of cyber attack. Both intentional and non-intentional misconduct amount to a security breach. The implementation of the right policies and strict adherence protects critical information assets from a majority of the threat landscape.

Business Continuity Plan: The enterprises ensure the safeguard of their information and information assets to minimize the risk, costs & duration of disruption to business operations. The enterprise will establish and maintain integration between response plans, DRP & BCP. The enterprise will have a plan for effective continuity of business & a well-rehearsed recovery process or a combination of these which will enable the resumption of critical business activities.

Incident Management: Cybersecurity or Information Security incidents could be a single or a series of unwanted or unexpected events that have a significant probability of compromising business operations and threatening IS & IT security. Incident management calls for plans and procedures to deal with the incidents so as to protect the information and or information assets.

Procurement and Outsourcing: There are a number of IT-based activities that the enterprise outsources to a third-party vendor. These include AMC for hardware and software, maintaining few services, or outrightly procuring any hardware or software. The enterprise is well aware of the risk of improper access to information and information assets from users of a third party or an outsourcing agencies which could prove detrimental to the enterprise’s interests.

Cybersecurity Framework

Identify: Understand organizational requirements and complete security risk assessments.

Protect: Implement safeguards to ensure your infrastructure can self-sustain during an attack.

Detect: Deploy solutions to monitor networks and identify security-related events.

Respond: Launch countermeasures to combat potential or active threats to business security.

Recover: Develop and activate necessary procedures to restore system capabilities and network services in the event of a disruption.