Information Security governance of modern Cybernetic systems

Dr.Manmohan Chaturvedi.

Information Security Consultant, Gurgaon, India

The design of cyber-physical systems rests on the foundation of the theory of cybernetics developed by Norbert Weiner at MIT in the 1950s.Cyber-physical systems are the product of a trans-disciplinary engineering design process–mechatronics–that integrates electronic, software, computer, and motor control. Cyber-physical systems and trans-disciplinary design are, therefore, important to the security of these increasingly integrated and pervasive systems. Stafford Beer introduced the Viable System Model as a blueprint for designing the communication and control aspects of viable systems. It is a model for organizational structure that is based on the structure of the human nervous system. A System is considered to be viable if it is able to survive in a particular environment. The viable system maintains itself in a homeostatic manner and exhibits survival, self-production, and identity through 'coherence' between its component sub-systems. This is essentially a systems approach to address organizational complexity. The Viable System Approach has at its heart the recognition of 'Management Control' structures and processes best suited to cope with the environmental changes.

Information Systems support and help develop business management at all levels by providing support for policy and decision making as well as control & coordination of the operations. The disruption or destruction of these information systems can cause serious disruption to, or loss of, businesses. As systems increasingly come under threat from both internal and external agents, there is a need to establish vigorous and dynamic responses to protect information assets. If an organisation is viewed, metaphorically, as an entity that seeks to continue to live and grow in a world full of potential threats it must have a mechanism that is capable of dealing with and recognising threat and communicating particularly dangerous threats to a point that is capable of taking immediate remedial action. Information Security governance could thus immensely benefit by incorporating the underpinnings of a viable system.