CONFERENCE ON SECURING THE CYBER SPACE
Cyber Resilience: Adaptive Line of Defense

17 May 2018: Bombay Exhibition Centre, Mumbai

Draft Programme

0900 – 0930 hrs.	**Welcome Tea & Registration**
0930– 1030 hrs.	**Inaugural Session**
1030 - 1145 hrs.	**SESSION I: Cyber Resilience – The Inescapable Need of the Hour** *Internet and modern ICTs are force multipliers. However, innumerability of entry points, concentration of assets, borderless nature and difficulty of attribution make cyberspace an inherently attractive target for hostile elements. Cyber security is an ecosystem where laws, organizations, skills, cooperation and technical implementation need to be in harmony to be most effective. A coordinated global approach to cyber security and resilience is the inescapable need of the hour.* The panel will focus on the following: • Cyber Threats and National Security • Cyber Preparedness & Response • Improving Incident Reporting and Response Strategies. • Legal, Economic, Financial & Political Consequences of Cyber Attacks. • Need for Comprehensive, Co-ordinated and Agile Policy Framework
1145 -1200 hrs.	**Tea Break**
1200 – 1300 hrs.	***SESSION II: Impact of Emerging Technologies in the Cyber Landscape*** *There are plentiful of emerging technologies that can help us steer the increasingly malicious cyber threat landscape The prominent question that arises is, Will these technologies benefit the attacker or the defender more? AI, IoT, Big Data, Cloud, and Mobility offer both promise and peril. These are being used for both offense and defense, like, for e.g., IoT devices are often created with little to no regard for security, yet they process and transmit a significant amount of personal data, making it a big target for hackers, whereas, AI systems can spot patterns and anomalies in ways that humans can't, helping to stem the tide of cyber-attacks that might otherwise steal personal data. In fact, as hackers employ artificial intelligence systems themselves to develop increasingly sophisticated attacks, using artificial intelligence to defeat cyber-attacks may be the only way to protect vulnerable systems and the data they contain. It's important to ensure that artificial intelligence is deployed in productive ways to enable people to continue to enjoy the benefits of IoT*

	without the data security risks. The panel will examine: • The Role of Disruptive Technologies in Cyber Landscape. • Given the vulnerabilities in IoT and other emerging technologies, how can AI benefit them for Cyber Security? • Can AI be the Future of Cyber Security?
1300 – 1400 hrs.	***Networking Lunch***
1400 - 1500 hrs.	**SESSION III: Cyber Security Challenges and Solutions in the BFSI sector** *There is a rise in the complexity of the attacks being launched against the BFSI industry. While the financial institutions are taking a number of steps to safeguard their IT infrastructure, they continue to be challenged by the pace of innovation and rising sophistication of the attacks.* The session will have case studies and representation from the BFSI sector.
1500 – 1630 hrs	**SESSION IV: Bridging the Skill Deficit Gap in the Indian Cyber Landscape** *Emerging threats have overtaken our efforts and pace to build capability and capacity. In India, the National Cyber Security Policy 2013 recognizes the need to address the burgeoning skill gaps and has called for creating a work force of half-a-million cyber security professionals. There exists a strong case for making India a global cyber security skills & innovation hub.* The Panel will focus on the following: • How to Address Ecosystem Gaps and Move from Industry-Academia Collaboration to a Holistic Eco-system • Leveraging the Demographic Dividend, IT Prowess and Indian Diaspora. • Creation of Cyber Security Universities & Security Industry Clusters.
1630- 1700 hrs	**Closing Remarks**
1700 – 1730 hrs	**Tea & Networking Session**