

Cyber Safe East India – Workshops on Cyber Security for MSMEs

Background and Rationale

Technology advancement has helped businesses, specifically micro, small and medium enterprises (MSMEs) with better access to market and opportunities, it also compromises them to threats of cyber-attack while participating in the digital economy.

The advancement in technologies has transformed businesses and processes across the globe. As in the offline world, the internet ecosystem also has its own vulnerabilities and threats called as cyber threats. To this end, cybersecurity strives to protect systems including networks, applications, and resources from cyber threats and cyberattacks. Importantly, the incidences of cyberattacks have grown exponentially over the years, and particularly in India, the reported cybercrime increased by 121 percent between 2016 and 2018 and was also the second most cybercrime-affected country in the world. This growth in cybercrime is evident that the need for cybersecurity is more prominent than ever, even more for vulnerable businesses with weak system protection and low awareness.

Given this background, CUTS is going to organise three capacity-building workshops in Ranchi, Patna, and Guwahati on cybersecurity and protection for MSMEs. The project will be instrumental in identifying cybersecurity needs of MSMEs based on the understanding of their usage of digital technology, assessing challenges faced by them ineffective use of cybersecurity tools, designing appropriate strategies to help them benefit from such tools, and collate and disseminate best practices to safely navigate the space.

Goal

- Empower and capacitate MSMEs to safely navigate the digital space and mitigate cybersecurity risks.

Objectives

- Create a network and platform for cross-learning between experts in US and India
- Generate awareness about cybersecurity risks and available tools to mitigate cyber risks
- Facilitate interaction among stakeholders within the knowledge network, on a sustainable basis to interact on the use of cybersecurity tools, even beyond the project's timeline

Methodology

In order to achieve the objectives, the project will be implemented in three phases, i.e. Preparatory, Capacity Building and Review and Reporting. In depth literature review would be undertaken to identify existing literature and gaps in cybersecurity *vis-à-vis* MSMEs. The team would undertake scoping visits in Guwahati, Ranchi and Patna to assess the need and challenges of MSMEs in cybersecurity. The need assessment report would form the basis to design the capacity building workshops and will be organised in the mentioned three cities, with local partners.

Supported by



US Consulate General, Kolkata

The project has engaged Cyber Security Experts from India and the US and together form a Key Resource Group (KRG). The KRG members would provide expert opinion and technical support to ensure successful implementation of project related activities. As part of the project design, media would also be engaged for wider dissemination of best practices for MSMEs on cyber security issues.

Envisaged Outputs

- Three capacity building workshops in Ranchi, Guwahati, and Patna.
- Best practices compendium illustrating the strategies and tools of cybersecurity for MSMEs.

Expected Outcomes

- Improved capacity of MSMEs on cybersecurity and equip enterprises to adopt internet and digital tools for their businesses.
- Contribute to the Digital India Campaign platform to address key issues of e-commerce, entrepreneurship, cyber risks, challenges and opportunities
- Encourage and inform MSMEs to adopt best practices of cybersecurity.

Project Duration

The project commences from July 2019 and will be concluded in July 2020.

