U.S. Consulate General Kolkata

AMERICANCENTER

CUTS International

Cyber Safety Best Practices for MSMEs

18 February 2021 | Thursday | 17:00-18:30 hrs (IST)

Webinar Report

(Screenshot of the speakers at the webinar including team members from U.S. Consulate-Kolkata and CUTS International)

Background and Context

The growth in digital technology has transformed businesses in India and across the globe, benefiting businesses with better connectivity. The adoption of digital technologies also accelerated due to the COVID-19 pandemic, wherein many micro, small and medium enterprises (MSMEs) went online.

On the other side, on account of increasing digital adoption, cyber threats have also increased proportionally. MSMEs are most vulnerable to the growing cyber threats and attacks because of several factors, such as lack of cyber safety prioritisation, capital allocation to cybersecurity, understanding of cybersecurity risks, etc. Eminent experts discussed discrete opportunities, challenges, and cyber safety best practices for the MSMEs with this objective.

Speakers

Key speakers in the webinar were:

- Monica Shie, Public Affairs Officer, U.S. Consulate-Kolkata and Director, The American Center-Kolkata (Opening Remarks)
- Bipul Chatterjee, Executive Director, CUTS International (Welcome Note)
- Deepak Maheshwari, Distinguished Fellow, CUTS International (Moderator)
- Anil Bhardwaj, Secretary General, Federation of Indian Micro and Small & Medium Enterprises (FISME)
- Karnika Seth, Managing Partner, Seth Associates
- Rahul Sharma, Founder, The Perspective
- Ranjit Rane, Manager, Technology and Policy Research, Reserve Bank Information Technology Pvt Ltd (ReBIT)
- Tulika Pandey, Cyber Security Group, Ministry of Electronics & Information Technology (MeitY), Government of India

The webinar was attended by about 35 participants from diverse stakeholder groups. More details on the webinar can be accessed here: https://cuts-ccier.org/cuts-webinar-cyber-safety-best-practices-for-msmes/

Highlights of the Session

Welcoming panellists and participants, **Bipul Chatterjee** emphasised that:

- As businesses are increasingly getting digitised to adopt digital technologies further, it is vital to assess and build cybersecurity awareness of Indian MSMEs.
- It is equally essential for MSMEs to understand the cybersecurity threats that can jeopardise their business, and as a consequence, can be subjected to various laws and challenges.
- Although few businesses can be cyber aware, however, cybersecurity adoption can still be a constraint for them. Thus, it is necessary to appropriately link the businesses with a network of cybersecurity experts to provide the businesses with relevant cybersecurity solutions and expertise.

Monica Shie, opening the session, highlighted the significance of the U.S.-India relationship, its strength, and expanding cooperation on multiple issues, including cybercrimes. Monica discussed that:

- U.S. State Department works with partners worldwide to respond to shared threats in cyberspace, including advocating for multistakeholder governance,

promoting and protecting internet freedom, and preserving the openness and functioning of the internet against control by repressive states.

- Through the U.S.–India Cyber Dialogues, both the countries have strengthened the Computer Emergency Response Team (CERT) operations and exchanged best practices on malware, forensics, critical infrastructure protection, and combating disinformation.
- Cyber threats and threat actors are diverse than ever and no country is cyber-ready. It is imperative to secure the underlying cyberinfrastructure to reap the benefits of increasing internet connectivity.
- New technologies involve risks, and thus, businesses must understand and mitigate e-business risks.

Kapil Gupta, Assistant Policy Analyst, CUTS International, made a brief presentation on CUTS Briefing Paper entitled, 'Cybersecurity Challenges for MSMEs' (Briefing Paper available here). Gupta highlighted that the study's goal is to build the cyber capacity of Indian MSMEs to navigate cyberspace safely. Furthermore, he discussed the increasing adoption of digital technologies by MSMEs, common types of cyberattacks, vulnerabilities and challenges of Indian MSMEs, and the best practices of cybersecurity.

Moderating the session, **Deepak Maheshwari** remarked that India has a huge informal sector, including small shops and vendors, that first started accepting digital payments after demonetisation in November 2016. This adoption of digital tools was further accelerated after the COVID-19 pandemic. Maheshwari also highlighted that:

- MSMEs are increasingly transacting on online marketplaces. Inevitably, with the increased use of ICT tools, the cyber threats have concurrently increased.
- India needs to improve its cyber protection capabilities going ahead. While a cyberattack on big enterprises may be widely covered in the media, however, the aggregate economic impact of cyberattacks on small business enterprise are significant.
- While many businesses are unaware of post-cyberattack actions, they are also unaware if their commercial activities have already been breached.
- The comprehensive cybersecurity framework signed between the U.S. and India in 2016 also identified the importance of capacity buildings for MSMEs.

Anil Bhardwaj emphasised the challenges of MSMEs towards cybersecurity, including:

- The use of digital tools increased in the past few years than the MSMEs' preparedness to digital change. COVID-19 further accelerated the sudden adoption of digital tools.

- First and foremost, MSMEs lack awareness about cyber risks and systemic risk evaluation. This is further exacerbated by reliance on third-party service providers. Thus, making MSMEs vulnerable, unaware and unprepared for cybersecurity risks.
- The financial constraints include lack of capital availability and cost of up-gradation. This is worsened by the lack of schemes to support the need for MSMEs to upgrade digital infrastructure. Similarly, human resources is another significant challenge for MSMEs.
- All of these challenges are compounded by a lack of adequate legal remedies and a weak judicial system.

Karnika Seth discussed the following significance of legal compliances for MSMEs:

- Lack of internal policies, including IT, social media and IPR, may address many issues for preventing cyber risks. Similarly, documents such as non-disclosure agreements, appointment letters and standing orders internally created are very relevant to safeguard against data theft and other issues.
- As companies deploy technologies such as DLP softwares to counter cyber attacks, it is important to include employees' guidelines to regulate personal email use for work purposes to safeguard confidential information leakage.
- Certifications, such as ISO 27001, are essential to keep reasonable security practices to safeguard data. The Chief Technology Officer's role is vital to administer IT rules and assess legal softwares and licenses.
- Hesitation to report cyberattacks to safeguard reputation may expose the businesses to judicial injunctions and compensations, including criminal and civil cases.

Rahul Sharma pointed out the following issues for MSMEs on data privacy and cybersecurity strategy:

- The compliance burden of the organisations is growing. Thus, compliance costs could also become a challenge for the MSMEs. Besides, compliance cost should not compromise data protection.
- MSMEs should be allowed to earn back a substantial portion of penalities, provided if they have an accidental data breach, but showcases responsible reporting and commitment towards compliance.
- MSMEs also need to focus on managing the entire spectrum of data governance management from creation to deleting data.

- The valuation of MSMEs also depends on their Cyber Hygiene, thus reducing the cyber insurance premium. Need a change in mindset towards a uniform approach towards cybersecurity and privacy and understand risks to businesses.

Ranjeet Rane discussed the following issues to ensure cloud security for MSMEs:

- Although there is a demand for cybersecurity products and awareness in the market, the open and free market failed to provide it as per the expectation.
- While the costs for MSMEs may be higher, the byte-size products are still missing in the market. This is why cybersecurity adoption is low and adoption costs are higher.
- In the financial sector, cooperative banks are comparable to MSMEs. RBI's five-pillared strategy known as GUARD - Governance Oversight, Utile Technology Investment, Appropriate Regulation and Supervision, Robust Collaboration and Developing IT and Cybersecurity Skills Set, can be replicated for the MSME sector to reduce costs without encouraging free-rider problem.
- A cloud-based platform offering specialised byte-sized functionalities may address some of the key challenges towards adopting cybersecurity at a large scale.

Tulika Pandey highlighted the nuances of cyber threats and the government's perspective:

- India is called the bot capital because it failed to understand the nuances of cybersecurity processes that need to be addressed. MSMEs are the assets to build country's cybersecurity ecosystem.
- MeitY has a start-up hub with more than 2000 start-ups, mentors, and VCs. They have been synergised on a single platform to synchronise the industry and facilitate procedures and processes that may be daunting for smaller teams.
- MeitY is also facilitating a soft landing programme to help build security processes in the entire business design and development, bringing security aspects and business development.
- Compliances are necessary for cyber ethics and cyber hygiene as a practice.

Way Forward

Concluding the session, **Arnab Ganguly,** Policy Analyst, CUTS International, emphasised the importance of cybersecurity for east India and Indian MSMEs.

As the next steps, CUTS will organise capacity-building workshops on cybersecurity for MSMEs in Guwahati, Ranchi and Patna in March and May 2021.

After the workshops, a Compendium of Best Practices will be developed and released to help MSMEs safely navigate cyberspace and mitigate cyber risks.

Press Release links: https://bit.ly/3qI3JDJ; https://bit.ly/2P0VZi5; https://bit.ly/3aHoFoz

YouTube link: https://bit.ly/3kBS3jk

Twitter Thread link: https://bit.ly/3kBS3jk