Regional Dialogue for the Asia-Pacific (ASP) - Securing Critical National Infrastructure

S. S. Sarma, Director
Ashutosh Bahuguna, Joint Director
Indian Computer Emergency Response Team
(CERT-In)

Indian Computer Emergency Response Team (CERT-In)

CERT-IN was established in January 2004. It is a functional organisation under Ministry of Electronics & Information Technology, Government of India

Section 70B, Information Technology Act 2000: Designates CERT-In as the National nodal agency to serve as the national agency to perform the following functions in the area of cyber security:

- Collection, analysis and dissemination of information on cyber incidents
- Forecast and alerts of cyber security incidents
- Emergency measures for handling cyber security incidents
- Coordination of cyber incident response activities
- Issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents
- Such other functions relating to cyber security as may be prescribed

CERT-In Key Activities

- **Proactive**
  - Cyber threat-intelligence exchange operations with organizations
  - Issuance of alerts and advisories to organizations
  - International Cooperation for cybersecurity activities

- **Reactive**
  - Incident response operations: CERT-In is national nodal agency for responding to cyber security incidents and cyber security related aspects. Activity is operational on 24X7 basis

- **Assurance**
  - Cybersecurity Exercises - International and Domestic
  - Cyber Crisis Management Plan (CCMP)
  - Cyber security Audits

Threat landscape and Challenges faced during Pandemic (1)

- **Business Continuity Plans (BCP)** and incident response plans are inadequate or even non-existent for dealing with pandemics
  - never anticipated or tested such plans for a situation like this.
- **Covid-19-themed attacks** in the form of malicious websites, phishing emails with malicious attachments that drop malware to steal data and credentials
- **Increased attack surface**
  - VPN, Remote Office Infra, Web meetings, Insecure personal digital devices accessing enterprise applications
- **Poor operational and monitoring controls**
  - Traditional security measures prior to COVID-19 not suitable in current scenario
  - Delays in cyber-attack detection and response due to lack of human analysts in Security Operations
- Need for keeping employees synchronized (especially those working in agile teams), such software increases the risk of hacking sensitive data
- **Increased Potential Insider Threats**
  - IT Sabotage, Intellectual Property Theft, IT Fraud, Espionage, Unintentional Insider Threat
- **Physical Security**
  - Home is new office, how to protect business data at home

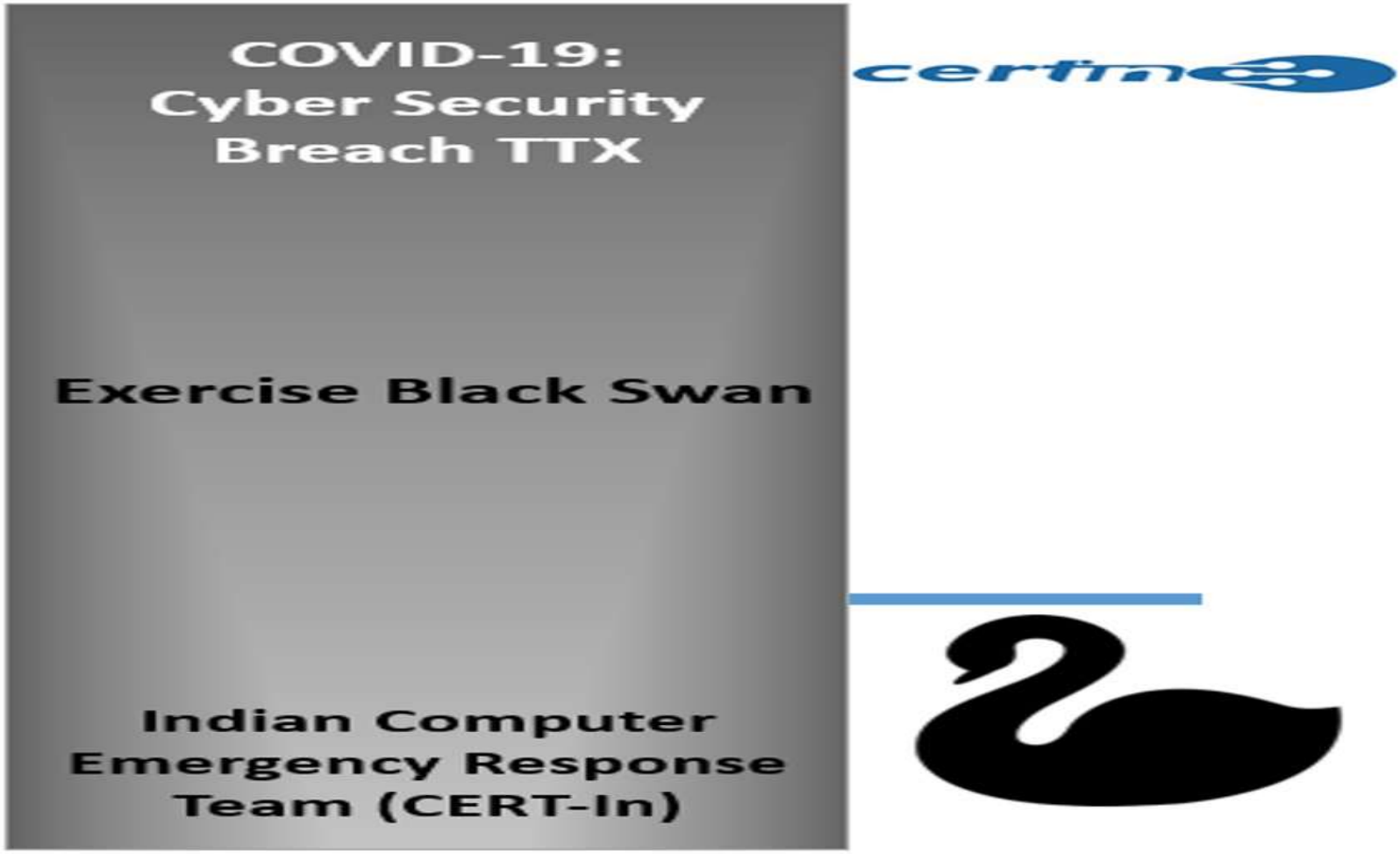
Threat landscape and Challenges faced during Pandemic (2)

- Pandemic has forced everyone to conduct business in a nonstandard manner
  - Unfamiliar environment - more chance of errors – more advantage to adversaries
- Hybrid model (Office:WFH) in effect
  - 80% of IT/ITES workforce has switched to Remote/WFH
  - Most sectors have adopted to WFH, willingly or unwillingly, to varying degree
- Rapid digitization across all sectors
  - especially Health, Telemedicine, Education etc. without secure architecture
- Increased reliance on Digital Payments, Entertainment, e-Commerce activities – enhancing risk of cyber frauds
- Heightened Risk to Healthcare data / availability of IT systems
- Need for continuous availability of E-Governance and online services
- Exploitation of human weakness - Opportunistic attacks and frauds -Craving for information on pandemic conducive for Social engineering attacks
    - Coronavirus themed phishing and malware campaigns
- Misinformation campaigns

Responses during COVID-19 Pandemic (1)

- CERT-In incident response were operational and manned 24X7 during pandemic lock-down
- 20 specific advisories & alerts related to COVID-19 pandemic and secure usage of teleworking, VPN and web-conferencing software were issued by CERT-In
- 300+ threat intelligence alerts were sent to over 700 CISOs of key organizations and stakeholders in the country advising Indicators of compromise for enabling proactive preventive actions and security cyber infrastructure at entity level
- 40+ Cyber Threat Information Bulletin were released by CERT-In related to COVID-19 cyber-attack campaigns.
- As part of CCMP an advisory on Securely Managing Business Continuity during Crisis situation due to COVID- 19 Pandemic was issued by CERT-In.
- Interaction sessions were conducted with auditing organizations to formulate audit guidelines to continue quality audits in pandemic situations. Guidelines issued in public domain

Black Swan Table Top Exercise Series (2)



CERT-In conducted 3 “Black Swan” Table Top Exercises involving 200 participants from 75+ organisations. Theme of the exercises were disruptions and cyber-attacks due to COVID-19 pandemic

Areas of collaboration and Recommendations (1)

- International Cooperation
  - Member of FIRST
  - Member of APCERT
  - Research Partner of APWG

- Memorandum of Understanding (MoU) with 13 Countries

- Working groups on Secure Digital Payments and IoT security at APCERT

- Cooperation with Product and Security vendors
  - IT and security vendors operating in the country

- Collaborative efforts
  - Sectoral CERTs, CISOs of critical sectors, ISPs
  - Data Security Council of India (DSCI)
  - Industry Associations in IT and non IT areas

Areas of collaboration and Recommendations (2)

- Crisis and Communication protocol check exercises – Most international exercises are limited to technical aspects only
- Involvement of senior decision makers in International exercises
- International platform for facilitating collaboration and cooperation during cyber crisis
- Collaboration regarding mandatory implementation of DNSSec, DMARC and BGPSec
- Harmonization of information exchange rules/laws among nations
- Collaboration regarding facilitation of Whois records to national CERTs
- Supply chain security issues needs to be addressed at multilateral/ international forums
- Development of norms for ISPs to prevent malicious activities through clean pipes
- Initiative and programs to build cyber resiliency to counter previously unknown threats & situations

THANK YOU