Authors

Dr. Sanjay Bahl

Director General
CERT-In
Ministry of Electronics and IT, Government of India

Sanjay.bahl@gov.in

Ashoo
Ashutosh Bahuguna

Scientist
CERT-In
Ministry of Electronics and IT, Government of India

bahuguna.a@meity.gov.in

Background:
CERT-In Training & Exercise Programs

- CERT-In has been regularly conducting national & sector-level exercises for the last 14 years. These exercises are designed based on the nature & objective and categorised in the following levels:

  - **Layer I** exercise : Basic level of exercise
  - **Layer II** exercise: Technical Exercise
  - **Layer III** exercise: Operational Exercise
  - **Cyber Crisis Table Top Exercises (CCTTX)**

- CERT-In also conducts trainings on various topics of cybersecurity such as Incident response, Web-application security, network security, malware analysis and others on a regular basis

CERT-In Training & Exercises Program

Cybersecurity trainings and exercises are conducted and supported by National Computer Emergency Response Teams (CERTs) to create awareness, build capacity and assess the cyber security preparedness of the participating entities.

❖Till date CERT-In has conducted 53 Cyber Security Exercises involving **over 600** organizations :

- **15** Indian Cyber Crisis Exercise(ICCE)
- **20** Cyber Crisis Table Top Exercises(CCTTX)
- **18** Sector Specific Exercises

❖Total Annual Training Programs carried out: 28 ~30 involving approximate 30~35 Participants in each program

Limitations of Current Methods for Conducting T&E

It is observed that the following **key limitations** create hindrance in achieving effective outcomes and fall short of appropriate value-addition for the participants:

- Current format in cyber security domain lacks formal application of suitable **Methods & Principles** with regards to **Design & Execution** of these trainings & exercises

- Miss the mark in developing **clear learning objectives** as well as assessing **Learner Attainment**

CERT-In Empirical Investigation

- In pursuit of continuous improvement CERT-In conducted an empirical investigation to make cyber security trainings and exercises more effective by applying **formal learning models and pedagogical principles**

- Adoption of learning methods & taxonomy (Derived from Bloom's revised taxonomy) has assisted us in:

  (a) Assessing needs of specific target participants;

  (b) Designing training content & exercise based on **cognitive requirements of participants;**

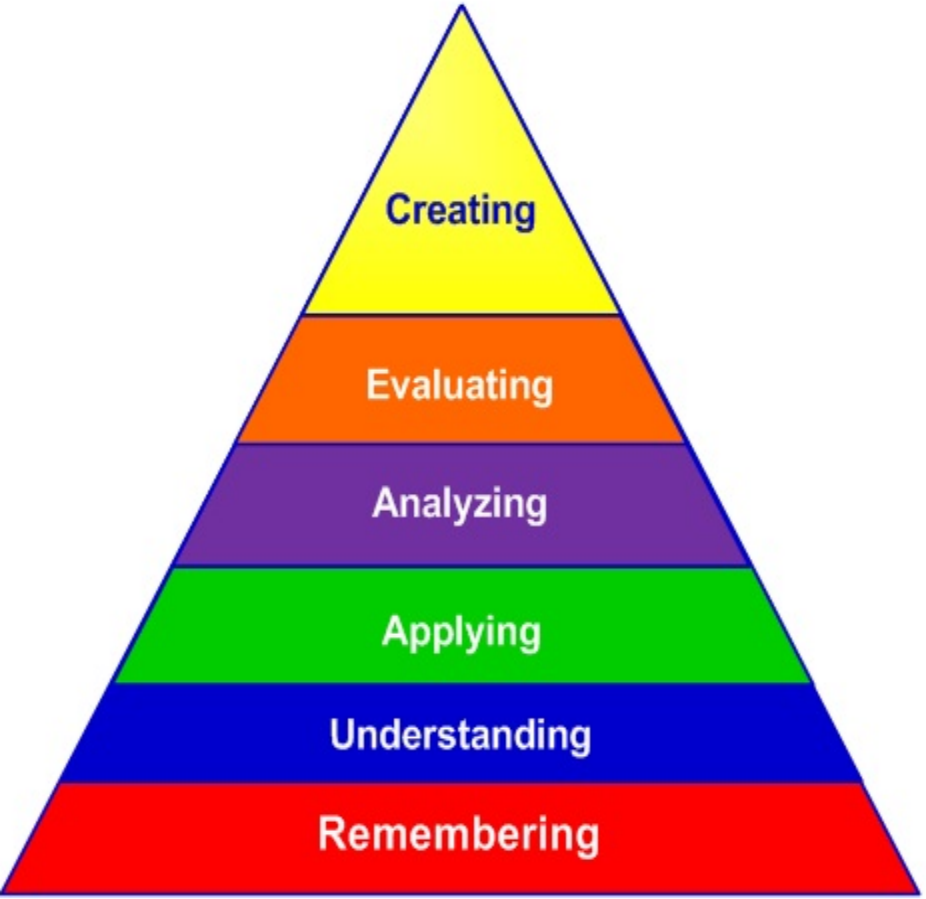
  (c) Assessing the **accomplishment** of participants**; and**

  (d) Measuring **effectiveness** of the program & its content

Bloom’s Revised Taxonomy (BRT)

- Bloom's revised taxonomy is one of the most widely used models of human cognitive processes. A revised version of the taxonomy was published in 2001
- Provides integral relationship between knowledge and cognitive process by encouraging critical thinking to solve problems
- Using Bloom’s taxonomy for thinking skills, one may explain the gap between objectives and outcomes by noting that expectations involve higher order thinking skills (application, analysis, synthesis, and evaluation) while assignments and evaluation continue to focus on lower order thinking skills (knowledge and comprehension).
- Provides a common way of thinking about and a common vocabulary that increases participants level of precision for better communication
- Bloom’s revised taxonomy identified six domain, from the simple recall or recognition of facts, as the lowest level, through increasingly more complex and abstract mental levels to the highest level which is classified as Creating

Blooms Taxonomy - Revised



BLOOM'S REVISED TAXONOMY

Creating

Generating new ideas, products, or ways of viewing things

Designing, constructing, planning, producing, inventing.

Evaluating

Justifying a decision or course of action

Checking, hypothesising, critiquing, experimenting, judging

Analysing

Breaking information into parts to explore understandings and relationships

Comparing, organising, deconstructing, interrogating, finding

Applying

Using information in another familiar situation

Implementing, carrying out, using, executing

Understanding

Explaining ideas or concepts

Interpreting, summarising, paraphrasing, classifying, explaining

Remembering

Recalling information

Recognising, listing, describing, retrieving, naming, finding

Application of BRT in CERT-In's T&E Program

- Developed a 3-phase program based on pedagogical principles defined in Bloom's revised taxonomy
- The focus area of this program was to build cyber security incident handling capabilities by encouraging critical thinking to solve challenges in the entities operating in Indian cyber space
- Use of taxonomy in program helped in effective need assessment, design and execution of trainings & exercises. The taxonomy was also used for assessing the effectiveness of the program and attainment by the participants
- **This 3-phased program was implemented over a duration of 8 month's and tested successfully on 40+ entities**

Application of BRT – CERT-In's 3 Phased T&E Program

- Developed trainings, exercises, simulations & assessments for participants to improve their capability from Remember (Knowing the basic definitions related to cyber security incident handling) to Create (Designing and developing improvement plans in cyber security incident handling)

- This 3-phase program included activities for 6 steps / domains of learning maturity for higher order thinking skills:

1. **Remembering** (Basic Definitions related to incident Handling)
2. **Understanding** (Ability to explain concepts related to Incident handling)
3. **Applying** (Application of knowledge in responding to incidents)
4. **Analyzing** (Analysis of Artifacts and Incidents)
5. **Evaluating** (Evaluation of existing incident response procedures)
6. **Creating** (Development of Improvement Plan for Incident response)

Cognitive Levels of Participants - Entry Level Assessment

- To assess the Cognitive Level of Participants in the domain of Cybersecurity and specific to Incident Handling a questionnaire was prepared and Participants were required to submit their responses before the start of the program Phase 1
- Questions were mapped to each Level of Bloom's revised taxonomy.

- Example Questions in the Questionnaire:
  - **Applying Level** - Have you ever handled any cyber security incident or participated in any Cyber security exercise. If yes, Please give brief details of the incident / exercise

  - **Analyzing Level** - What sort of incident analysis / evidence collection and technical analysis was performed by you or your team

Phase -1: Remembering & Understanding

Bloom's revised taxonomy (Steps / Domains)	Phases of CERT-In Training-cum-Exercise Program	Assessment Points (AP)
Understand	Phase-I : Training-Cum-Briefing Session & paper exercises	AP1: Assess participants ability to demonstrate understanding of the concepts and ability to explain & outline cyber security incident handling related concepts.
Remember		

Phase-2: Applying & Analyzing

Bloom's revised taxonomy (Steps / Domains)	Phases of CERT-In Training-cum-Exercise Program	Assessment Points (AP)
Analyze	Phase-II: Simulated Cyber Crisis Exercise	AP2: Assessment of capabilities via cyber security simulation exercise based on artifact & incident analysis and their application of knowledge in handling the incidents while making suitable inferences supported by evidences.
Apply		

Phase-3: Evaluating & Creating

Bloom's revised taxonomy (Steps / Domains)	Phases of CERT-In Training-cum-Exercise Program	Assessment Points (AP)
Create	Phase-III: Debriefing & playbook session	AP3: Assessment of participant's capabilities in: (i) Determining current preparedness of their own organization in handling cyber security incidents and; (ii) (ii) Designing & developing improvement plan for their organizations.
Evaluate		

Exercise Results & Analysis (Sample size 42)

AP0 - Entry Level Assessment of Cognitive Stages of participants in Incident Handling

Cognitive Levels – Cyber Security Incident Handling	Results of Assessment
Creating (Development of Improvement Plan for Incident response)	**0 / 42**
Evaluating (Evaluation of existing incident response procedures)	**0 /42**
Analyzing (Analysis of Artifacts and Incidents)	**0/42**
Applying (Application of knowledge in responding to incidents)	**1/42**
Understanding (Ability to explain concepts related to Incident handling)	**Responses (Correct=38%, Partially Correct=27%, Incorrect=35%)**
Remembering (Basic Definitions related to incident Handling)	**Responses (Correct=56%, Incorrect=44%)**

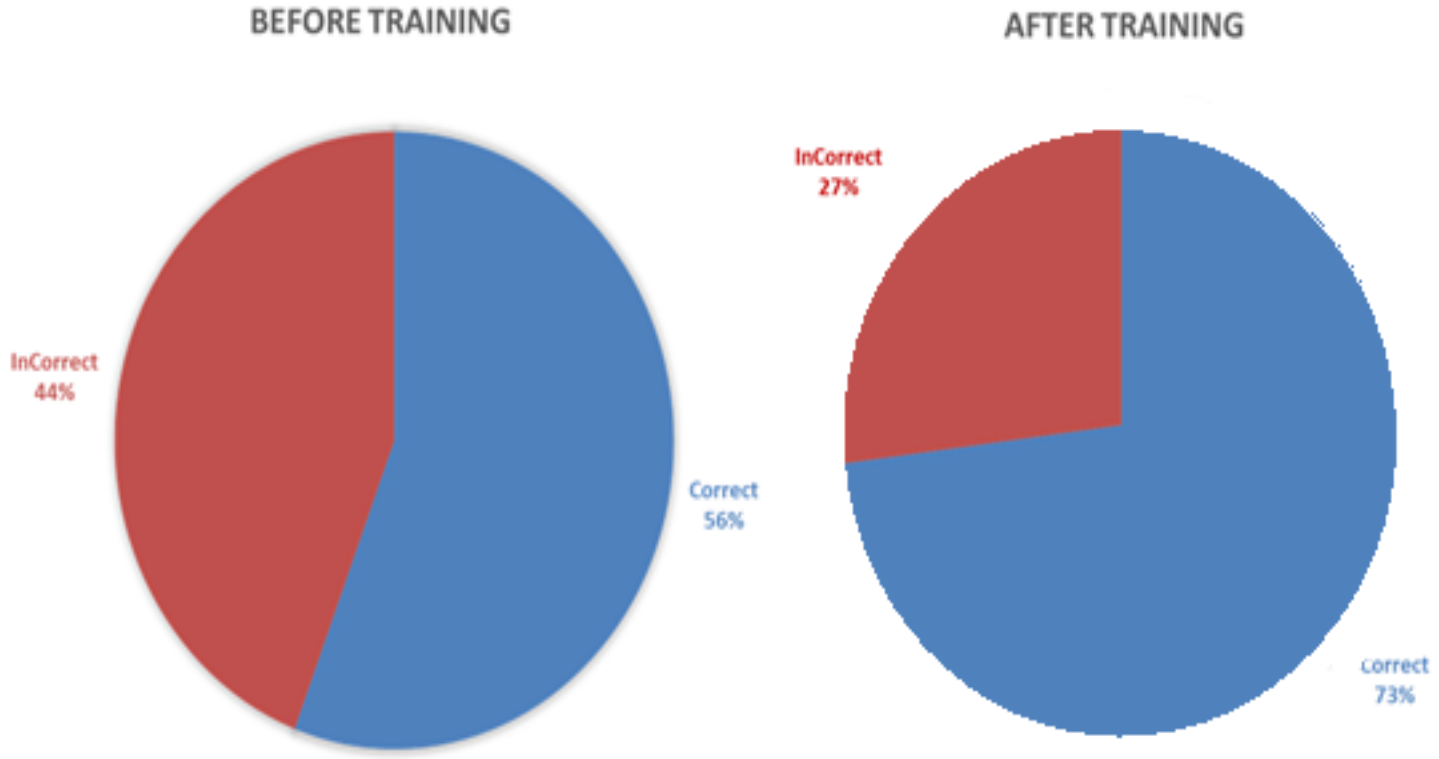
Phase-1: Training-Cum-Briefing Session & paper exercises

- **AP-1: Assessment After Training-Cum-Briefing Session & paper exercises**

- Based on responses for “remembering” & “understanding” in AP0, training sessions on “Basic Incident Handling & Triage details”, “Advance Persistent Threats”, “Fundamentals of Malicious Code and Web based Attacks” were designed & delivered

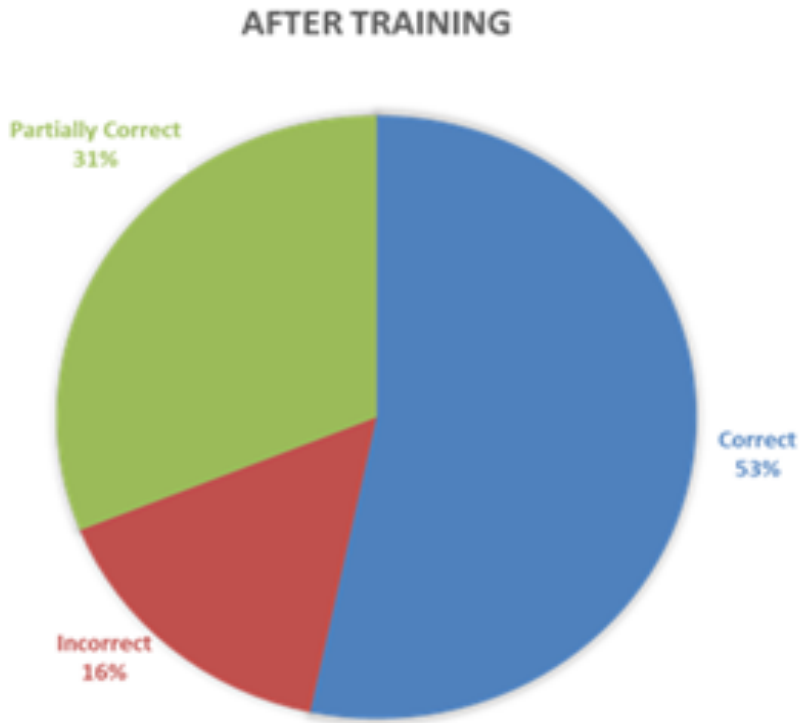
- Paper exercises were introduced in between each technical session. Exercises included E-mail header analysis, log analysis, Malware runtime analysis and network traffic analysis so as to improve understanding of concepts

Phase -1 Continue…



“Remembering”

Phase -1 Continue…



“Understanding”

Phase-1 Continue…

After training, assessment of learner attainment was measured by involving subjective & objective questions on incident handling. The results indicates that:

- participant's remembering & understanding of the concepts related to Incident Handling has improved; and

- T&E Programs in stage-1 were effective in meeting the goal, however there is scope of further enrichment of the program to improve attainment of more participants at desired level

Phase -2: Applying & Analyzing - Simulated Cyber Crisis Exercise

AP-2: Assessment of capabilities in Handling the Incidents & Artefact Analysis

- Cyber Crisis Scenario along with technical artifacts were designed based on some recent incidents in the country and same were simulated during the exercise

- Performance evaluation of participants was done based on application of incident handling knowledge and analysis of the artefacts

- Simulated exercises provided an opportunity to all participants to apply their knowledge & conduct analysis on incident. This was earlier experienced by only one organization (Applying – 1/42)

Phase -2: Simulated Cyber Crisis Exercise Results

Grade	No. of Org.
Excellent	8
Good	22
Average	5
Improvement Required	7

Phase -3: Evaluating & Creating- Debriefing Session

AP-3: Assessment of capabilities participants in Evaluating their own performance in simulated exercise and creating an Improvement Plan for Incident response

- Exercise debriefing session was carried out by CERT-In
- Participants worked on Playbooks to evaluate their posture to handle cyber incident based on their performance in cyber crisis exercises
- Based on above inputs organizations were asked to develop improvement plan for incident response function at their organizations
- All organizations participated for the first time in Phase-3 and were able to use higher order thinking skills (highest cognitive level) for incident response function

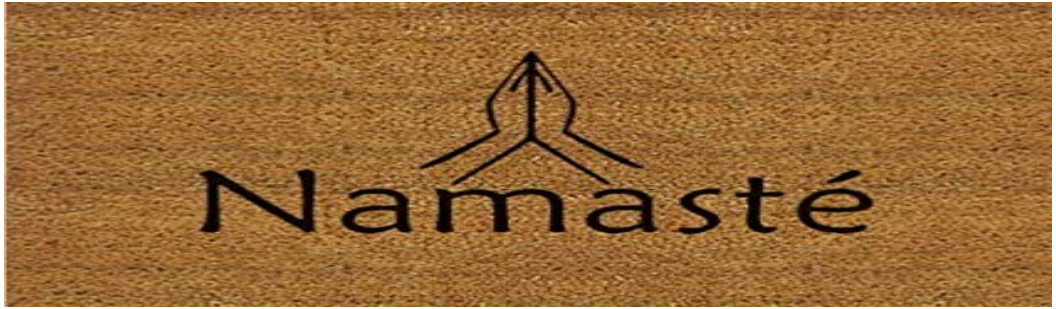
Conclusion

- CERT-In researched and implemented this 3-phased program over 8 month's duration and tested it successfully for 42 entities

- The participants reactions were positive, they were able to think critically while using higher order thinking skills and this improved their quality of experience with CERT-In

- Taxonomy provided an opportunity to design T&E program based on cognitive requirements of participants, conduct assessment of learner attainment & effectiveness of training by providing a common way of thinking about and a common vocabulary that increases participants level of precision for better communication

- CERT-In's results show that this pedagogy has a tangible potential to improve on existing capacity building endeavors in the domain of Cyber Security



certin
Handling Computer Security Incidents

Thank You!