Don't Wanna Cry: A Cyber Crisis Table Top Exercise for Assessing the Preparedness against Eminent Threats

Ashutosh Bahuguna, Raj Kishore Bisht, Jeetendra Pande

***Abstract*: Cyber Security Exercises are emerged as useful tool for assessing and improving preparedness of the organizations and nations against cyber threats. Cyber security exercises of different types & duration with various objectives are conducted across the globe. These exercises vary from quiz type exercises to full simulated attack based exercises. One such type of exercise is Table Top Exercise (TTX). TTX are discussion based exercises involving decision makers of the participating entities to meet and discuss the response during the hypothetical emergency situations. These exercises primarily focused on to clarify roles and responsibilities, assessment of effectiveness of plans and further improvements in cyber security.**

In this paper we presented Objective, Design and Execution of Cyber Crisis Table Top eXercise (CCTTx) named "Don't WannaCry" conducted for Indian entities. 5 CCTTx involving decision makers from 65 organizations with the objective to encourage self-realization of true cyber security posture of their own entity were conducted in 2017.Exercises were divided into three segments starting with (i) Self-assessment in which participating organization self-assess their cyber security posture in pre-defined 6 domains, followed by (ii) Exercise Play in which participating entity act as a hypothetical entity and respond to the presented cyber crisis situation and finally (iii) Hotwash session was executed with purpose of inducing self-realization of their true cyber security posture. Exercise take away for participants was self-realization and identification of improvement plan to enhance cyber security posture of their entities against the cyber attacks.

These exercises are unique in design, execution and their objective of self-realization by the participating entities. Success of these exercises is evident from the feedback and adoption of exercises for domestic purpose by participating organizations.

***Keywords* : Cyber Security Exercises; Cyber Security Training; Cyber Security Assessment; National Cyber Security; Cyber Security Self-assessment; Table Top Exercises; Cyber Security Preparedness; Cyber Security Drills.**

I. INTRODUCTION

Due to increased adoption of technologies in Government services, businesses and critical sectors, cyber security has become a key concern for organizations and governments. Today, cyber threats exploiting a single vulnerability can lead to major breach and have potential to jeopardize the well being of the nation, businesses and citizens.

Keeping dynamic and advanced cyber threats in horizon, numerous Cyber Security Efforts are initiated by organizations, nations and International forums to protect the ICT and ICT enabled services from cyber attacks. National Cyber security Strategies [1], Critical Information Protection Plans [2], Setting up of CERTs/CSIRTs/ISACs [3] [4], Act & Regulation, Audit & compliance [5] and cyber security exercises [6] [7] are some such initiatives adopted widely to promote secure operations in cyber space and protect interests from cyber attacks.

Cyber security exercises of different types and with different objectives are conducted by academia, national/state governments, organizations, international organizations and critical sectors. Popularity and adoption of cyber security exercises are increasing as came out in European Union Agency for Network and Information Security (ENISA) cyber security exercises stock taking report 2015 [8]. As per ENISA report, there has been an exponential growth in the number of cyber security exercises over the past decade with the trend expecting to accelerate in the coming years.

Based on the objectives and organizing entity, Cyber security exercises can be classified into 3 types (i) National and critical sector exercises (ii) Bilateral exercises & multilateral exercises such as ASEAN CERT Incident Drill (ACID) [9] , cyber Europe [10] and (iii) Academic exercises like UC Santa Barbara International Capture The Flag (iCTF) [11]. Cyber security exercises also vary in design and execution from Table top exercises on hypothetical scenarios to full simulated exercises on the real / real-alike infrastructure. Based on the design and execution exercises can be classified as (i) Discussion based exercises such as quizzes, table top exercises and walk through and (ii) Functional Simulated exercises like drills, inject based exercises [12].

Federal Emergency Management Agency (FEMA) [13] defined Tabletop Exercise (TTX) as an exercise which involves key personnel discussing simulated scenarios in an informal setting. Table top exercises can be used to assess plans, policies & procedures, clarifying roles & responsibilities and identification of improvement plans by evaluation and self-critique which may be conducted after the exercise or progressively through the event.

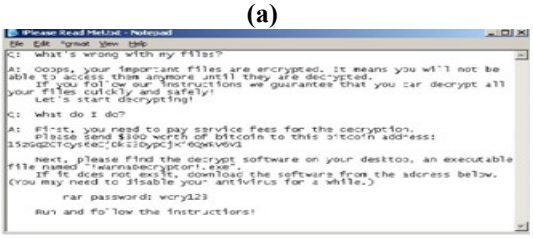
Revised Manuscript Received on October 05, 2019
* Correspondence Author
Ashutosh Bahuguna*, Research Scholar- Uttarakhand Technical University, Dehradun & Scientist- Indian Computer Emergency Response Team.
Raj Kishore Bisht, School of Computing, Graphic Era Hill University, Dehradun, India.
Jeetendra Pande, School of Computer Science & IT, Uttarakhand Open University, Haldwani, India.

Table top Exercises are not only found useful for cyber security preparedness, but also in other critical domains like Disaster Management plans [14], Medical Emergency Plans [15], Nuclear Power Plants, chemical industry [16]. Table top exercises focused on operational, tactical and strategic levels usually invite participation of senior-management, which then have possibility to lead to higher- impact and improvements in existing posture of the participating entities. This paper presents objective, design and execution of Cyber Crisis Table Top eXercise (CCTTx) named "Don't WannaCry". 5 CCTTXs was conducted for 65 Indian organizations in 2017. These exercises were conducted in wake of global WannaCry ransomware attack, which reported to spread and impacted more than 70+ countries in May, 2017 [17] [18]. On positive side WannaCry attack created much-needed awareness and intensify cyber security priorities among decision-makers in businesses. Key Objective of designing & executing Don't WannaCry exercises was to use the opportunity of high-alert situation created by WannaCry ransomware to induce self-realization of cyber security posture in participating entities. Self-realization, defined as knowledge of true self was key approach behind design & execution of these exercises. The adopted approach of CCTTx was reverse of carrot-and-stick approach in cyber security such as Act & Regulations, compliance & Checklists which may lead to entities doing cyber security for sake of compliance only. The execution of CCTTx was designed to enable participating entities through horror story of cyber security (scenario), which let them freely realize their current cyber security posture and identify what they need to improve.This paper is organized as follows: Section 2 presents the exercise design, Section 3 presents the exercise execution, Section 4 discusses evaluation of participant responses and feedback of exercises, finally Section 5 concludes the paper.

II. EXERCISE CRITERIA

Motivation for CCTTx, Don't WannaCry emerged from episode of WannaCry or WannaCrypt Ransomware. WannaCry spreads by using vulnerability in implementations of Server Message Block (SMB) in Windows systems. Ransomware using exploit ETERNALBLUE [19] encrypts the computer's hard disk drive and then spreads laterally between computers on the same LAN. Ransomware also spreads through malicious attachments to emails. Ransom demanded in crypto currency bitcoins to get the decyption key to unlock the system. Fig 1 shows screenshot of infected system and readme!.txt file. This ransomware reportedly spread across more than 70 countries and received global media coverage. This highly critical situation and severity of attack provided opportunity to bring senior management of organizations and governments on board and assist them to assess their cyber security posture and identify required improvement plans to improve their cyber security.CCTTx design involved mainly following 4 elements (i) Identification of Objectives of the exercises (ii) High-level Scenario and Injects for the Exercise (iii) Playbook and Documentation (iv) Planning, Logistics and Invitation to the participants. This section describes these elements of design for Don'tWannaCry CCTTx.

(a)



(b)

Fig 1 Wannacry/WannaCrypt Ransomware (a) infected system and (b) readme file [20]

A. CCTTx Objectives

Exercise was designed based on the recent global ransomware attack to put organizations under hypothetical scenario of the ransomware attack and discuss, assess their capabilities to respond to the dynamic and advanced threat landscape. Objective of exercise was to provide environment for the participating entities to Assess, Realize and Plan for improvement their existing cyber security programs. Two Key objective of CCTTx was to:

(i) Induce self-realization of cyber security posture in senior-management of participating entities; and

(ii) Identification of cyber security improvement plan and priority areas by participating entity for their own organization.

B. Scenario and Injects

CCTTx was divided into 3 major segments (i) Self-Assessment of current cyber security posture (ii) Exercise Play in which participants play role of decision maker for hypothetical organisation (xyz corp.) under hypothetical ransomware attack; and (iii) Hotwash: Post-play assessment to identify strengths, improvement area and realizations of own cyber security posture.

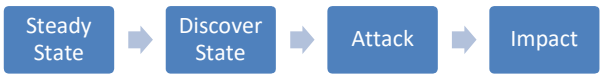
I. Self-assessment

Segment 1 of exercise involve self-assessment of cyber security posture of the entity in 6 domains (i) Initiatives, Challenges & Priorities (ii) Technical Measures (iii) Organizational measures (iv) Legal Measures (v) Capacity Building & Awareness (vi) Cooperation and Information sharing. An open ended questionnaire was designed for this purpose with total 17 questions under 6 domains.

II. Exercise Play

For segment-2 of the exercise hypothetical scenario of the cyber attack (ransomware) targeting hypothetical entity XYZ Corp was designed. Primary objective of choosing the hypothetical entity and scenario instead of real-entities & real-scenario is to provide informal and stress free environment to participants so that participants can freely think, speak and discuss without considering their official-positions.

Scenario was delivered to the participants through video and paper print injects. Injects were designed to be released one-by-one to unfold the scenario. Scenario through injects unfolded in following stages:



Exercise injects along with description are shown in Table 1. Following was the high level scenario designed for the exercise play:

High-Level Scenario "A hacker group goes by the name “Kings” have leaked surveillance tools and exploits and later made publically available. There is possibility of advance cyber attacks against Indian cyber space using the leaked tools. These tools are further utilized by different cyber criminals to perform the targeted attacks for ransomware. XYZ Corp. is targeted by the criminals, their data is available for sale in dark web and further critical systems of XYZ corp get encrypted by the cashflow ransomware. Criminals are asking for ransom in bitcoins and ready to bargain with officials of the XYZ corp."

Table 1: CCTTx Injects

Inject No.	Inject	Description
Ex01	Paper Inject: Blog Post related to release of “LAUGHING BUDHA” exploits.	Security Analysis Blog about the public release of exploits from classified nation-state-level cyber weaponry by hacker group Kingslayer.
Ex02	Video Inject: News Report about Possibility of Cyber Attack against Indian Cyber Space	Media Report about the possibility of Advanced Persistent Threats (APT) [20] and ransomware attack on Indian organizations.
Ex03	Paper Inject: Advisory to Indian Organizations	National CERT issued advisory and alert to the organizations regarding hacking tools and exploits released in public.
Ex04	Video Inject: Webcast on Ransomware	Webcast from security experts on issue of Ransomware cashflow.
Ex05	Paper Inject: Systems of XYZ Corp encrypted by cashflow ransomware.	Systems including the critical machines encrypted by the Cashflow Ransomware. Criminals are asking for payments in bitcoins for providing key to decrypt the systems.
Ex06	Media Queries to XYZ Corp.	Media queries related to damage assessment to the CISO and employee of the organization.

III. Hotwash

Last segment of post-exercise Hotwash was designed with objective of self-realization by participants. This segment was designed for identifying strengths, weak areas, improvement plan and expectations from stake holders during the cyber crisis execution. In Hotwash session participants have to respond for real (own) entity and was guided by following categories questions:

- Whether our cyber security program sufficient to handle crisis situation?
- Where we need to improve?
- What can be done to improve and priority areas?
- How to improve coordination and cooperation in situation of cyber crisis?
- Lesson learned in exercise.

C. Playbook and Documentation

Playbook containing self-assessment questionnaire, Inject wise response sheet, Hotwash questionnaire, feedback on exercise was designed to be distributed to participants. Playbook act as a work document in which participants have to make recording in provided format during the exercise. For post-exercises session, Hotwash guiding questions and feedback form for exercise were provided in playbook. Apart from Playbook, exercise observation sheets to be used by the independent observer for recording the key findings and summarizing the exercises were prepared. NIST Cyber Security Framework [23] and Literature on ISO 27001 [24] were provided to the participants as reference documents.

D. Planning and Logistics

A scenario and inject development team was assigned with the task to formulate the scenario and injects. Exercise Moderator, Observers and whitecell players (for responding to queries of participants and responding with derived injects during exercise) were assigned their respective roles. Invitations were sent to the prospective participants to join CCTTx as player from senior management and Chief Information Security Officer (CISO) of the organization. Presentation/video screens, laptops with internet connectivity, audio/speakers, wireless microphones and roundtable were arranged for executing the exercise.

III. EXERCISE EXECUTION

5 cyber security exercises were conducted in 2017, 2 in June and 3 in December involving participation from 65 Indian organizations. For execution of CCTTx, exercise team was assigned with specific task of moderator, white-cells and observer. Exercise was executed in moderator-driven session in which moderator displayed, explained and discussed the questions and injects during the exercise. Detailed injects were distributed in print format. Execution of the exercise during 3 phases is shown in

Fig 2.

Duration of exercise was 4 hours with segment-1 & segment-3 of 1 hour each and segment-2 of 2 hours. In segment-1 participant were asked to do self-assessment for their own (real) organization, moderator discussed and clarified the questions during the session. For segment-2 (play), participants were divided into group of 4, participants were asked to wear the hat of hypothetical organization's security team and respond to injects presented by the moderator. Participants were given approximate 15 minutes after release of each inject. In last segment of post-exercise hotwash participants were asked to come out of hypothetical organization and consider what-if same attacks happen on their organization. In Hotwash again participants were guided by the questions to identify improvement plan, expectations from stakeholders, adequacy of existing cyber security controls and lesson learned through the exercise.

IV. EVALUATION AND FEEDBACK

If you are using *Word,* use either the Microsoft Equation Editor or the *MathType* add-on (http://www.mathtype.com) for equations in your paper (Insert | Object | Create New | Microsoft Equation *or* MathType Equation). "Float over text" should *not* be selected.

CCTTx was primarily focused on enabling participating entities to assess their own current cyber security posture and identify improvement areas. Hotwash was the key takeaway for the entities from the exercise. Qualitative analysis of Hotwash data was performed to identify meaning revealed by the response of participating entity. Key points reported in hotwash are as follows:

- Implementation of regular cyber security audits.
- Incident response capabilities need to be built.
- Need to improve cyber security policy implementation.
- Standards to be created/followed for Vulnerability Assessment, Penetration Testing & Security Audit.

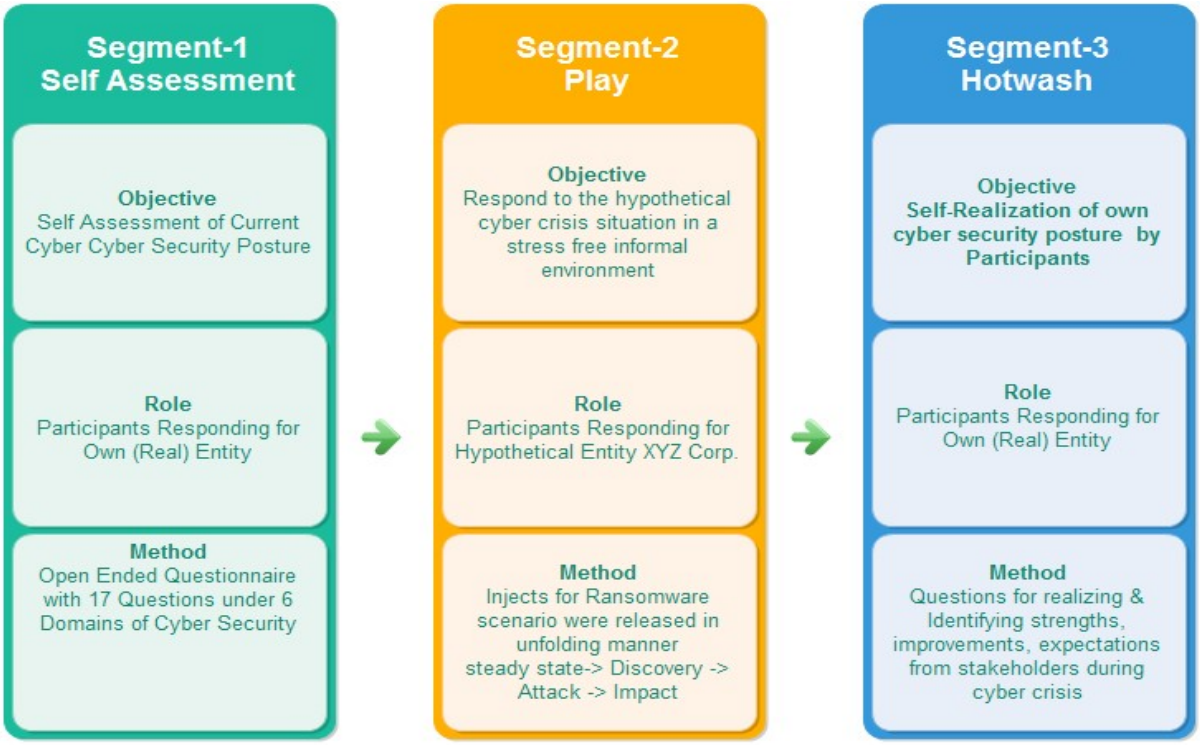


Fig 2: CCTTx Execution

- Need of sharing Technical Information & Knowledge with community.
- Implementation of Cyber hygiene rules for users of IT systems.
- Formation of dedicated teams to handle cyber security issues.
- Need for mechanism for regular updates and situational awareness.
- Need of robust cyber security policies, Routine audits and strict compliance are priority area.
- Malware signature/IOCs database may be created for verification of malicious artifacts.
- Need of Training and awareness programs for the entities
- Information classification scheme may be defined and adopted.
- Manpower resources are challenge in cyber security.
- Need of more technical hands-on trainings for team.
- Sector specific crisis exercises with more frequency may be conducted.
- Need to setup Threat information exchange platform at national level.

Fig 3. Feedback received from organizations is highly encouraging with maximum of participants ranking

Feedback on CCTTx was collected from participants on 5-point Likert scale with 1 as worst and 5 as excellent rank. Feedback on following parameters was taken in the playbook:

- How relevant was the Exercise to your organization? (scale 1[worst] to 5[Excellent])
- How useful was the Exercise? (scale 1[worst] to 5[Excellent])
- How would you rank the Exercise overall? (scale 1[worst] to 5[Excellent])
- How would you rank the scenario design? (scale 1[worst] to 5[Excellent])
- How would you rank the instructions given through injects? (scale 1[worst] to 5[Excellent])
- How would you rank the time allotment during this drill? (scale 1[worst] to 5[Excellent])

Feedback received from 65 organizations is plotted in

5(Excellent) and 4 (Very Good) for these exercises. With respect to time allocated for exercise, 6 participants marked rank 3(average) which may be considered in future exercises by increasing time of exercise by half hour.

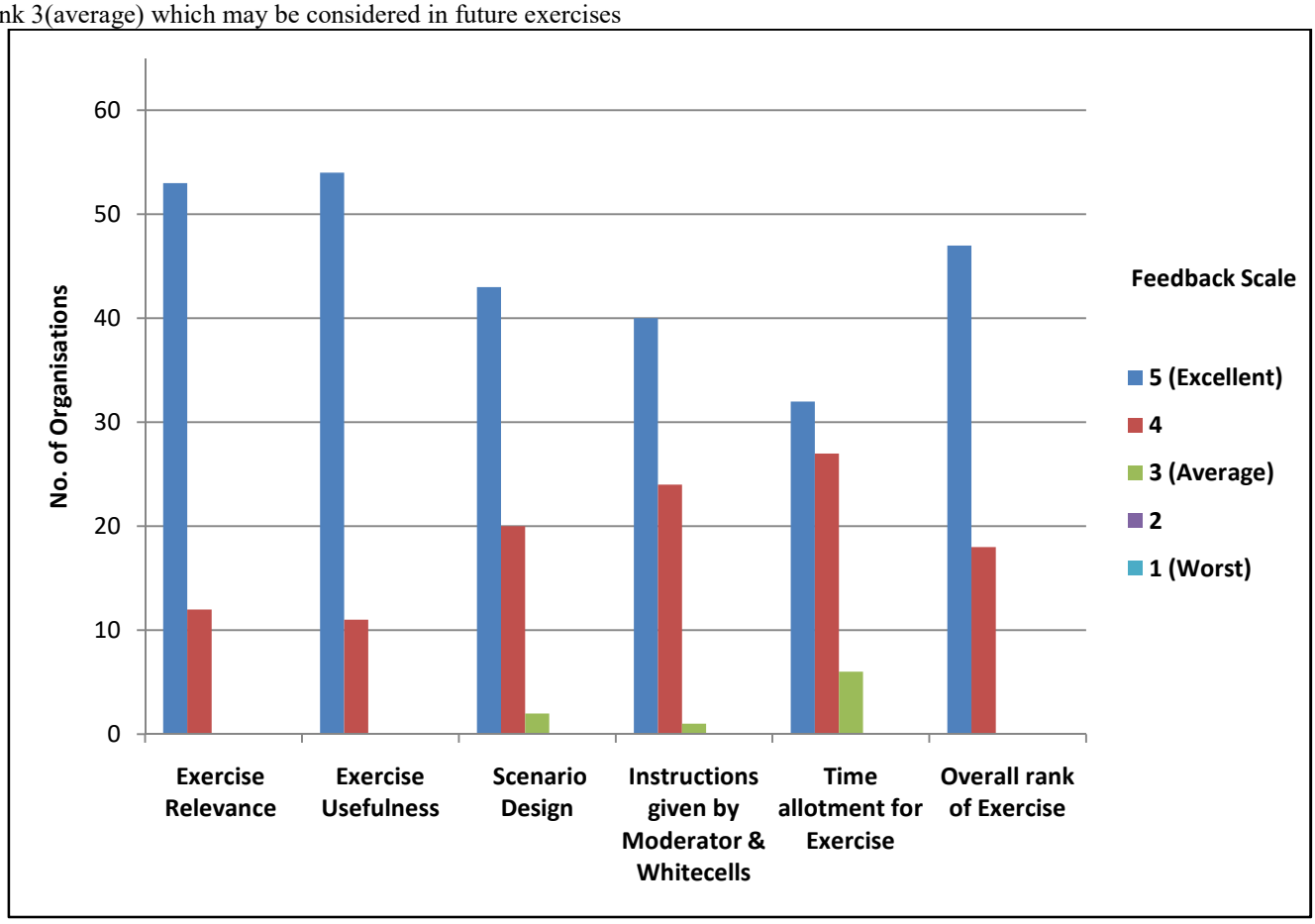


Fig 3: Feedback of Participant on CCTTx Exercises

V. CONCLUSION

Cyber Crisis Table Top Exercises (CCTTx) "Don't WannaCry", were designed and executed in wake of global ransomware WannaCry/WannaCrypt attack. 5 CCTTx were conducted in 2017 involving participants from 65 organizations. We discussed about detail design and execution of the CCTTx which involved three main segments of self-assessment, exercise play and post-exercise hotwash.

Inducing realization of their own cyber security posture and identification of the improvement plans by participants was key objective of designing and conducting these exercises. This approach had shown potential to make better impacts than self-assessment alone in which participant's response may influenced by mental tendency of substitution of questions for answering an easier question [25].

CCTTx exercises were successful and able to make impact as evident from further requests for conducting CCTTX and organizations are adopting them for conducting in-house exercises. Feedback of participants on CCTTx was very highly positive. Exercise Relevance, usefulness, design and execution was marked very-good to Excellent by participants. Formal evaluation methods for exercise evaluation such as Kirkpatrick training model [26]will be adopted in future exercises.

REFERENCES

1. E. Luiijf, K. Besseling and P. d. Graaf, "Nineteen national cyber security strategie," International Journal of Critical Infrastructures, vol. 9, pp. 3-31, 2013.
2. European Union Agency for Network and Information Security (ENISA), "Critical Information Infrastructures Protection approaches in EU," ENISA, 2015.
3. Indian Computer Emergency Response Team, "CERT-In," Ministry of Electronics and IT, 2017. [Online]. Available: http://www.cert-in.org.in. [Accessed 13 September 2017].
4. ICS-CERT, "Home," [Online]. Available: https://ics-cert.us-cert.gov/. [Accessed 24 April 2017].
5. Government of India, Information Technology Act 2000, New Delhi: Ministry of Electronics and IT, 2000.
6. U.S. Department of Homeland Security, "Cyber Storm: Securing Cyber Space," U.S. Department of Homeland Security, 4 October 2016. [Online]. Available: https://www.dhs.gov/cyber-storm. [Accessed 30 May 2017].
7. A. Ahmad, "PhD thesis A cyber exercise post assessment framework: In Malaysia perspectives," University of Glasgow, 2016.
8. European Union Agency For Network And Information Security (ENISA), "The 2015 Report on National and International Cyber Security Exercises - Survey, Analysis and Recommendations," ENISA, 2015.
9. The Diplomat, "New ASEAN Cyber Drill Kicks Off in Vietnam," [Online]. Available: https://thediplomat.com/2017/09/new-asean-cyber-drill-kicks-off-in-vietnam/. [Accessed 10 January 2018].

10. ENISA, "Cyber Europe 2016," [Online]. Available: https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme/ce-2016. [Accessed 15 January 2018].
11. B. Boe, N. Childers and G. Vigna, "Hacking for Fun and Education: Organizing the UCSB iCTF," Fifth Annual Graduate Student Workshop on Computing, no. 5, pp. 19-20, 2010.
12. U.S Department of Homeland Security, "Homeland Security Exercise and Evaluation Program (HSEEP)," DHS, 2013.
13. Federal Emergency Management Agency (FEMA), "Emergency Planning Exercises," [Online]. Available: https://www.fema.gov/emergency-planning-exercises. [Accessed 14 January 2018].
14. R. Perry, "Disaster Exercise Outcomes for Professional Emergency Personnel and Citizen Volunteers," Journal of Contingencies and Crisis Management, vol. 12, pp. 64-75, 2004.
15. D. Dausey, J. Buehler and N. Lurie, "Designing and conducting tabletop exercises to assess public health preparedness for manmade and naturally occurring biological threats," BMC Public Health, 2007.
16. Federal Emergency Management Agency (FEMA), "FEMA's Downloadable Tabletop Exercises:Emergency Planning Tools To-Go," [Online]. Available: https://www.fema.gov/media-library-data/1383656415271-1d53ef9b8a660026233b82d3f69bc369/Tabletop_Exercises.pdf. [Accessed 14 January 2018].
17. The Guardian, "What is WannaCry ransomware and why is it attacking global computers?," [Online]. Available: https://www.theguardian.com/technology/2017/may/12/nhs-ransomware-cyber-attack-what-is-wanacrypt0r-20. [Accessed 15 January 2018].
18. Indian Computer Emergency Response Team (CERT-In), "WannaCry/WannaCrypt Ransomware - Critical Alert," 2017.
19. Trend Micro, "Massive WannaCry/Wcry Ransomware Attack Hits Various Countries," Trend Micro, 2017.
20. Symantec, "Ransom.Wannacry," 2017.
21. T. Colin, "Advanced Persistent threats and how to monitor and deter them," Network Security, vol. 2011, no. 8, pp. 16-19, 2011.
22. Ministry of Electronics and IT, "National Cyber Security Policy," Ministry of Electronics and IT, 2013.
23. National Institute of Standards and Technology (NIST), Framework for Improving Critical Infrastructure Cybersecurity, NIST, 2014.
24. ISO/IEC, ISO/IEC 27000 family - Information security management systems, International Organization for Standardization (ISO), 2013.
25. D. Kahneman, Thinking, Fast and Slow, Penguin Books, 2012.
26. A. Smidt, S. Balandin, J. Sigafoos and V. Reed, "The Kirkpatrick model: A useful tool for evaluating training outcomes," Journal of Intellectual and Developmental Disability, vol. 34, no. 3, p. 266–274, 2009.

AUTHORS PROFILE

Ashutosh Bahuguna is currently working as a Scientist at Cyber Emergency Response Team of India under Ministry of Communication and IT, Government of India. He have many publications to his credit in the field of Cyber and Information Security.

Dr. Raj Kishor Bisht is Associate professor at department of Mathematics/Computing, Graphic Era Hill University, Dehradun. He did M.Sc (Maths) and qualified JRF- NET (CSIR) in Mathematical Sciences. He obtained his Ph.D. from Kumaun University Nainital. He also did MCA from Uttarakhand Open University, Haldwani and qualified USET in Computer Science and Applications. He has more than 13 years of teaching experience. He has 10 research papers published in various national and international journals and 4 research papers published as conference proceedings to his credit. He has also been awarded Young Scientist Award from Uttarakhand Science Congress.

Dr. Jeetendra Pande is working as an Assistant Director(Research) and Assistant Professor of Computer Science Department at Uttarakhand Open University, Haldwani.