*OIC-CERT Journal of Cyber Security*
Volume 3, Issue 1 (April 2021)
31 - 40

# Establishment of a Method to Measure the Awareness of OIC-CERT Members

Tural Mammadov[1], Noraini Abdul Rahman[2], and Mohamad Farhan Mohd Rahimi
[1]CERT Gov Azerbaijan, Baku, Azerbaijan
[2]CyberSecurity Malaysia. Kuala Lumpur, Malaysia
[1]**mammadov.t@cert.gov.az,** [2]**noraini@cybersecurity.my**

**ARTICLE INFO**

***Article History***
**Received 01 Sep 2020**
**Received in revised form 16 Dec 2020**
**Accepted 08 Mar 2021**

***Keywords:***
**CERT, awareness test**

**ABSTRACT**

**Cyber threats and incidents have increased massively in the recent years thus it is very crucial in protecting and maintaining the critical infrastructures in organizations. The lack of awareness and active responses could be an issue to be highlighted for the Computer Emergency Response Teams (CERTs), which are responsible for incident handling process and mitigating the exposed risks faced by organizations and nations. Concerned about this, an effort had been made to strengthen awareness level among CERTs to improve the quality of services provided to secure and provide effective cyber security environment for the government and private sectors. This method also helps CERTs to exchange point of contacts, improve effectiveness of collaboration and built trust. In this paper, we proposed an awareness test to the OIC-CERT members which aimed to measure the level of awareness towards responding to incidents assigned to them correctly and in a timely manner. Three stages have been applied to ensure proper incident escalation are made to the team before the outcome being recorded from the respondents, respectively. The findings of this paper will provide an overview of the awareness level, check correctness and reliability of point of contacts, to build challenging environment to response tests on time and correctly and important lessons for the organizations to stay active and precise on the incident handling. On the other hand, the method needs to be improved to encourage the involvement of more respondents that will hopefully provide healthy cooperation among CERT members and getting a better, positive result.**


ISSN 2636-9680
eISSN 2682-9266

## I. INTRODUCTION

The Organization of the Islamic Cooperation - Computer Emergency Response Team (OIC-CERT) consists of cyber security experts from Islamic countries that are responsible for the preparation, identification, recovery, and prevention in handling computer security incidents in in their respective constituencies.

The OIC-CERT mitigate cyber threats or response towards incidents such as intrusions, malware, ransomware, and other malicious cyber activities including providing alerts and incident handling references. The OIC-CERT also conducts awareness programs, campaigns, and collaborations with its members in conducting research aimed at improving the level of knowledge related to the latest cybersecurity incidents.

These teams are working together in OIC-CERT to achieve the same goal of incident response. They respond to any computer security incidents with proper preparation including having complete security tools which is the key to a rapid response, identification and research process on the security incidents, recovery process where issue been handled and mitigated, removing threats and regaining control to pursue the system operational, and prevention phase to identify areas for improvement to avoid recurring issues.

In incident response operations, response time is a critical factor in the effectiveness of the process. In fact, hesitation in responding to incident can be damaging. It is important for the response team to keep the awareness level high, thus, this study was developed. It should also be mentioned that to keep awareness high is not to hurry without being attentive. In this test we will also test attentiveness to check if the incident handled in right way or not?! The main purpose in developing such system was to measure the awareness of the teams and encourage teams to be more active and accurate in incident handling and in cooperation. The OIC-CERT requires rapid and precise response to save time in the aftermath of an attack.

Some approaches have been carried out against the OIC-CERT teams for the purpose of the study. The first step is to collect the email addresses of the representatives from each OIC country team. The email address is used for the purpose of sending test links so that they can respond accordingly. The test results are recorded based on the time taken to respond and how correct the response is. The key elements of the test were the time taken and the accuracy of an incident response team in ensuring a productive and effective response.

Implementing the following study and recommendations should facilitate efficiency and effectiveness of incident response for OIC-CERT.

## II. RELATED WORK

### A. Computer Emergency Response Team (CERT)

CERT is an organization devoted to ensuring that appropriate technology and system management practices are used to resist attacks on networked systems, to limit damages and to ensure continuity of critical services despite successful attacks, accidents, or failures [1].

CERTs are also known as the Computer Security Incident Response Teams (CSIRTs) in some constituencies. They operate in various sectors such as academic, commercial, critical infrastructure, government, military, and business, among others. However, the special kind of CERT is the national CERTs that operate at the national level and act as a security point of contact for the country [1].

In the other hand, NIRT is also another term of CERT, known as the National Incident Response Team of NCSC (National Cyber Security Centre). The primary aim of the NIRT assistance in crisis situations is to support the company to recover the essential services and business processes of the victim or organizations [2].

The CERT (Computer Emergency Response Team) operation of the NCSC-FI (National Cyber Security Centre - Finland) takes care of the prevention, investigation, and communication tasks in case of information security breaches. The main purpose of the CERT operation is to produce and maintain the cyber situation awareness together with domestic and foreign partners and counterparts. As an essential part of the CERT operation, the NCSC-FI acts as a national point of contact for information security breaches and threats. It also investigates these cases and helps the concerned parties [4].

Computer Emergency Response Teams (CERT) should be established to improve the security cognizance among people. CERT can also help establish new cybercrime laws, train computer forensic teams, and support organizations and users in fighting cybercrime [5].

The establishment of the Computer Emergency Response Teams (CERT) is one of the initiatives to reduce and mitigate cyber threats. [6]

### B. Awareness Test

An attempt was made by a previous study to explore and figure out the local community present weakness facing a cybercrime threat. The motivation for this study was to examine the current awareness skills among the students and local community and help them in how to secure their privacy, services, and smart devices. An online and printed questionnaire was distributed for the participants in Bisha University in Alnamas District. One hundred thirty-five subjects were randomly selected, and all completed the protocol test [3].

The questionnaire sheet was based on the 2nd International Conference


ISSN 2636-9680
eISSN 2682-9266

on Anti-Cybercrimes (ICACC 2017) ideas, and provided a good survey that enables the authors to address the community's awareness and the lack for both an effective anti-cybercrime training courses for strengthening the local community resilience facing such technology crimes; and a good survey, enables authors to address the current needs in using current technology-based services, systems, and applications [3].

The results proved that building a safe and a secure community requires, both governmental and non-governmental institutions to share and integrate their responsibilities and efforts against the growing cybercrimes. It is quite clear that, a legal awareness is very low rate (33%). Also, a cybercrime's knowledge metric gives low rate (38%). Comparing a national anti-cybercrime system versus a global anti- cybercrime system, the study alarms the national institutions to be close to a community for handling cybercrime issue [3].

The study concludes that, the levels of the participants' knowledge in dealing with cybercrime issues and threats is very weak. The lack of security knowledge against a cybercrime risks is quite high. It is noticed that there is a lack of awareness on cybercrime risks, and there is strong desire to receive an anti-cybercrime training and support. In comparing the study results with the previously related studies in literature review in the region, this study gives a good awareness on cybercrimes threats in this area. Future direction can be performed in several areas. The first area would be expanding the number of input parameters in the dataset. The second area would be feature extraction on input variables to cover online awareness aspects. Also, a set of prediction algorithms can be used to predict cybercrime risks [3].

One of the best ways to make sure company employees will not make costly errors regarding information security is to institute companywide security awareness training initiatives that include but are not limited to classroom style training sessions, security awareness website(s), helpful hints via e-mail, or even posters [5].

The Government of Malaysia has been aware of the need for greater awareness and understanding of cybersecurity issues and for developing a positive cybersecurity culture [6].

A study entitled National Strategy for Cyber Security Acculturation and Capacity Building was carried out in 2010 to evaluate current national and CNII awareness education programs and campaigns [6].

To ensure the success of the cybersecurity awareness, acculturation and education programs, coordinated initiatives and efforts have been driven by relevant organizations to increase the level of cybersecurity awareness, best practices and safe use of the Internet across all CNII (Critical National Information Infrastructure) as well as public elements [6].

The National Security Council of Malaysia, with Cybersecurity Malaysia as the technical expert

agency, have co-organized a periodic national cyber crisis entitled X-Maya since 2008. The main objective of the drill is to exercise the workability of the National Cyber Security Response, Communication and Coordination Procedure and to raise awareness of the national security impact associated with the significant cyber incidents among CNII [6].

Securing CNII against cyber threat activities requires the efforts of the entire nation. The government alone cannot sufficiently secure the CNII. It calls for a public-private-community cooperation in addressing the matter. The government can take the lead in many of these efforts, provided it is supported by the private and community sectors [6].

Focusing on the technical task of the incident response team, the use of the right technical tools that support the work methods can greatly increase the effectiveness of CSIRTs. The effectiveness may lie in the field of lead time of solving the incident, on the financial level and on increasing team knowledge and shared situation awareness within the CSIRT [7].

The initial assessment of the size and risk of a specific cyber security incident is ascertained on an ad hoc basis and is predominantly based on the knowledge level of the CSIRT team member who first gets the incident reported [7].

The CSIRT's success depends on many factors, such as the technical resources at their disposal and team members' level of knowledge and skills. In addition to these factors, a team's success also depends strongly on the participation and cooperation of individual CSIRT members and other individuals, teams, and departments within and outside the organization [7].

Hence, teamwork is of the utmost importance in incident handling. Teams have the potential to offer greater adaptability, productivity, information processing capacity, and creativity than any one individual can offer. Moreover, teamwork is vital to transforming individual members' disparate incident knowledge into a shared awareness of the evolving situation [7].

## III. METHODOLOGY

The implementation and measurement on the effectiveness of the method can be divided into several stages.

The initial stage is about gathering the emails of the PoC member teams which will participate in the tests. The email addresses include representatives from the OIC-CERT. A valid email address is needed from each of the representatives to ensure the test link is being sent.

The second stage is about sending emails with a unique test link to each team to measure the response time of the teams. The time will be measured automatically and each team after clicking will see his/her response time and response rate. The Administrator will share the general response time and rating list for all teams after each test.


ISSN 2636-9680
eISSN 2682-9266

The last stage is to improve the test scenarios to harden the requirements and test skills of team members with real incident scenarios. It is important to ensure that the measurement is not only how quick the time taken for the teams to respond to the incidents, but it is also important to analyse how correct the teams act instead of to respond incidents or tickets opened to them. This approach will train the teams to respond rapidly and attentively, in order to correctly handle the required tickets or incidents.

## IV. ANALYSIS AND RESULTS

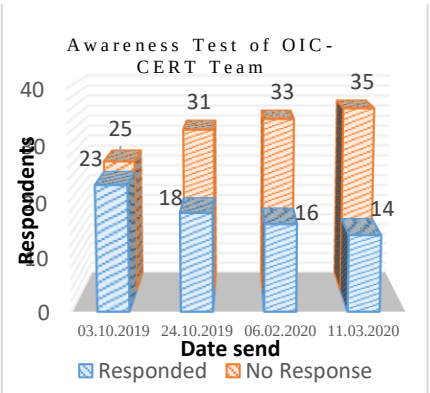


Fig. 1: Awareness Test of OIC-CERT Team

Figure 1 above illustrates the OIC-CERT Team Awareness Test statistics recorded from October 2019 to March 2020.

According to Figure 1, there are upward and downward trends in the response recorded respectively on two variables. The responding team decreases steadily in the number of respondents during the test period conducted. The unresponsive team shows an increase in the number of non-responses over time.

The latest result on 11th March 2020 shows the highest difference in the gap between the responding participants and the non-responding participants which is 21 people. This issue occurs due to two identified factors which are no response from the respondent, and email addresses that do not work or do not reach the recipient. The percentage for teams who respond quickly and correctly will be affected negatively if the number of respondents continues to decrease over time.

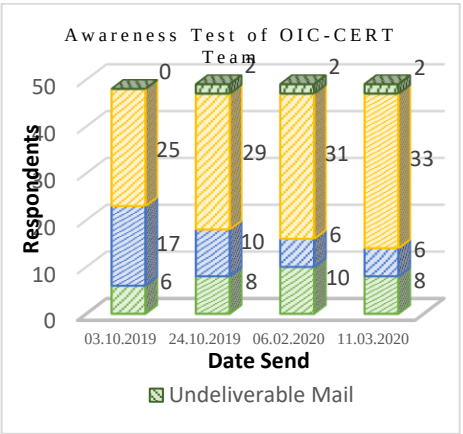


Fig. 2: Detailed Analysis of Awareness Test of OIC-CERT Team

As the number of respondents decreases during the test period, the quantity of teams that responded correctly on the incident or tickets opened to them certainly shows a small number.

Figure 2 shows the measurement of the awareness test's effectiveness, including the problem encountered during the test. The number of correct responses on the first two test dates shows a lower amount than the incorrect responses. However, the correct responses on 6th February and

11th March 2020 shows a positively higher result than the number of incorrect responses. The result indicates the successfulness of the team that managed to respond accordingly to the main purpose of this test.

Figure 2 also illustrates the rising amount of unresponsive team over time showing a large gap compared to the responded team. Apart from that, the undeliverable emails displayed in the figure also affected the outcome of this test, even though came out with very small numbers.

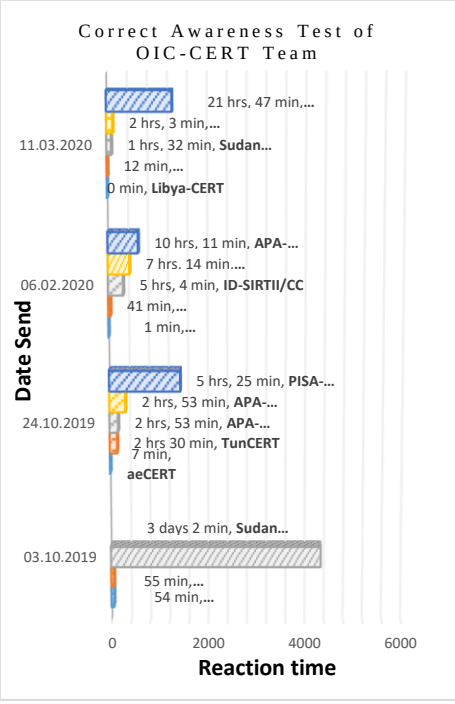


Fig. 3: Correct Awareness Test of OIC-CERT Team

Figure 3 above illustrates a detailed analysis of the top 5 teams that able to quickly and correctly responded the test.

These teams can be classified as undergoing this test successfully coinciding with the main purpose of this test being conducted. These teams have shown the positive level of awareness and encouragement to be more active in incident handling and in cooperation.

Based on Figure 3, the quickest response was logged from the Libya-CERT in recording 0 minute to respond the test correctly on 11th March 2020. On average, the above analysis displays that the time taken to obtain the correct response is less than one day.

After some tests, we revealed some issues that not only to get better results, but also, we need to get OIC-CERT corporation and information exchanges to be effective. They are:

1. The responses of the teams is not good enough as some teams do not respond at all.
2. With the tests it is possible to reveal that some teams' emails are not working properly or not getting emails which is not normal for the PoC contacts as they are used for communications and other purposes.
3. The teams' information and contact details need to be updated and controlled on a regular basis.

Pursuant to the issues listed above it was decided to have a system for member teams that will require the teams to update contact details and Point of Contact (PoC) information by themselves on a regular basis such as automatic update of the member's


ISSN 2636-9680
eISSN 2682-9266

data. This will assist the process as follows:

- All member teams' data to be up to date.
- All member teams' information and point of contacts will be available to all member teams.
- It will help to shake "sleeping" teams with alerts and push messages and encourage them to be active as well by updating team information and participate in information exchange on a regular basis (once a quarter).
- It will help the secretariat to activate and involve those inactive teams in activities within the OIC-CERT.
- It will automate the registration of new members.
- It will give opportunity to hold online voting for the new members.

All the above mentioned items motivated us to create another system where we can handle all those issues and integrate the awareness algorithm as a subsystem. It will give us opportunity to do a test on fully operational and complete system, measuring the awareness of teams and generating automatic statistics and so on.

## V. DISCUSSION

A general finding from the awareness test system of OIC-CERT members is that the number of respondents throughout the period are still small in numbers and decreasing. Instead, the number of the non-responses has shown an increased in numbers. It is important to ensure that the teams email addresses are reachable and ensure the teams cooperate accordingly to this test.

The support from the teams will ensure the real overview of the study to get better result of the overall participation. Apart from that, the positive outcome corresponds with the objective of this system as some of the teams have successfully responded to the incidents correctly in a timely manner. The result complied with the aim of the study to measure the effectiveness of the system to indicate not only how quick the teams responded the incidents, but also how correct they acted to the task.

Some improvements can be done in the future to increase the involvement of the participants. The PoCs need to be updated from time to time to ensure the participants receive the required test links. It is recommended to use the automatic update of the member's data to ease the process of the system onwards.

Apart from that, the team needs to improve on responding to incidents such as the need for better tools in support of teamwork. Alternatively, it may be due to the resistance to changein he way the teams have always worked, for example when it comes to use tools to estimate size and risk of an incident. This was always done based on team members' skills and experiences with similar incidents and there is no obvious need to do things differently [7].

## VI. CONCLUSION

This study was conducted among OIC-CERT members in a same, particular period with unique test link via email delivery. The delivery time was selected so that the email delivery time to be the working time of all members around the world. It was 13.00 GMT+4. Another thing considered was that the response time of each team calculated according to email delivery time – response time. Where it means email delivery time was unique for each team as the system is sending the emails with the pause not secure itself not to stuck in spam filters. The results conclude that the highest record registered (60%) is from the no response attribute, excluding about (3%) of undelivered emails and it is noticed that there is a lack of awareness for incident response. There is about (37%) of commitment from several teams that successfully responded to the test, including about (10%) teams that correctly react to the incident in a timely manner, were recorded. This study gives a good awareness for OIC-CERT members in actively mitigating cyber security incidents with proper incident management and rapid handling.

Future improvements and considerations can be made in several areas. The main aspect is to enhance the initiative in obtaining and updating the newest PoCs from the members involved, especially representatives from OIC-CERT. Second, ensuring the involvement and participation of all participants involved in this test to obtain more accurate test results. Also, highlight the objectives and purpose of the test performed to measure the time taken and the accuracy of participants in dealing with incidents.

## VII. ACKNOWLEDGEMENT

We would like to thank members of OIC-CERT for participating in the awareness test and contributing the publication of this paper.

## VIII. REFERENCES

[1] M. S. Hashim, and R. A. Ahmad, "The Organization of Islamic Conference – Computer Emergency Response Team (OIC-CERT)," Answering Cross Border Cooperation, 2011.

[2] T. Pahi, M. Leitner, and F. Skopik, "Analysis and Assessment of Situational Awareness Models for National Cyber Security Centers," 2017.

[3] E. I. M. Zayid, and N. A. A. Farah, "A Study on Cybercrime Awareness Test in Saudi Arabia – Alnamas Region," 2017.

[4] J. Pöyhönen, V. Nuojua, M. Lehto & J. Rajamäki, "Cyber Situational Awareness and Information Sharing in Critical Infrastructure Organizations," Information & Security: An International Journal 43:2, 236-256, 2019.

[5] K. P, and J. Takkalaki, "Information Security Threats, Awareness and Cognizance," 2015.

[6] F. Abdullah, N. S. Mohamad, and Z. Yunos, "Safeguarding Malaysia's Cyberspace against


ISSN 2636-9680
eISSN 2682-9266

Cyber Threats: Contributions by CyberSecurity Malaysia," 2018.
[7] R. V. d. Kleij, G. Kliinhuis, and H. Young, "Computer Security Incident Response Team Effectiveness: A Needs Assessment," 2017.