PROTECTING AFRICA AND ITS CITIZENRY FROM CYBER-TERORRISM THROUGH JOINT AWARENESS CAMPAIGN PROGRAMMES (JACAP)

[1] Azeez, N A., [2] Fasina, E.P, [3]Ayangbekun, O.J., [4]C.P Ojiako & [5]Venter, I.M.
[1,2,4]Department of Computer Science, University of Lagos, Nigeria
[3]Department of Computer Science, Crescent University, Abeokuta, Ogun State, Nigeria
[5]Department of Computer Science, University of the Western Cape, Bellville, South Africa

ABSTRACT

The recent advancement in Information and Communication Technology in Africa has undoubtedly influenced and even changed, in no small measure, the manner in which people conduct various activities, particularly in academe, industry and government. The introduction of various mobile devices has not only assisted in the progress recorded, but has also enhanced the proliferation of Internet access in the African continent. This recent ubiquitousness of access to the Internet in Africa has also introduced previously unknown cyber threats. The perception that Africa is cyber insecure has hampered the expected economic progress of various nations across the African continent. Investors from developed countries are scared to invest in African countries due to this perceived threat. Various awareness programmes have however been put in place in Africa to sensitise the public on the causes and effects of cyber-attacks. Against this backdrop, this research is aimed at providing joint awareness campaign programme to effectively guarantee security awareness programmes in Africa. The authors develop a Joint Awareness Campaign Programme (JACAP) as the best alternative for creating awareness among people in the continent. The JACAP was designed through the unification of three different awareness campaign programmes. This new initiative for achieving and ensuring the implementation of various sensitization, orientation and education programmes on cybercrime in Africa is considered and adjudged as the most successful, effective and efficient awareness campaign programme based on the outcome of the results obtained.

Keywords: cyber threat, awareness, imitative, security, Africa, Internet, cyberspace, fraudsters, information

1. INTRODUCTION

Information and communication technology (ICT) security needs have become increasingly important for corporate organisations and business establishments (Azeez & Venter, 2012). It is evident that many organisations, institutions and business corporations rely heavily on the latest computing technology to run their day-to-day activities with the issue of security is no more than a mere afterthought. To further justify the usage of internet across Africa, the information depicted in Figure1reveals the rate at which internet is being used is increasing at a geometrical rate. Based on the available statistics, it is crystal clear that the rate at which internet will be used across Africa will have tremendously increased in the next 10 years. Hence, African continent is vulnerable to various attacks (Azeez, Venter, & Tiko, 2011). Security however has to be a major concern for all, if Africa is to have a threat and attack-free cyberspace (ISF, 2003).

It has been established that sub-Saharan Africa holds six of the world's growing economies (INFOSEC, 2003). The entire continent is changing as a result of adoption of the new technologies. The rate at which cyber-attacks is growing in African continent is alarming. According to Microsoft's Security Intelligence Report, attacks in Africa are greater than the global average attacks. To establish the fact that cyber-attack is ravaging the African countries Figure 2 provides a security intelligent report of how each country stands on global world map of cyber-attacks.

It is evident from the available information provided by the CERT (Computer Emergency Readiness Team) coordination unit of Carnegie Mellon University that attacks of different sites across the globe have increased geometrically by 68% (Kruger & Kearney, 2 0 0 6). This development has not only hampered economic growth in most African countries but has also jeopardised development initiatives for technological advancement in academe and many corporations.

The question that arises is how to get over this scourge (cyber insecurity) in the African continent? In finding solutions to this challenge, the authors believe the best approach is to create a formidable security awareness programme which is aimed at creating and maintaining good security behaviour which is pivotal for an effective information security-enabled environment (Furnell , Gennatou, & Dowland , 2002). Hence the authors would recommend abroad general public security awareness campaign; Joint Awareness Campaign Programme (JACAP) as proposed in section VI subsection D.

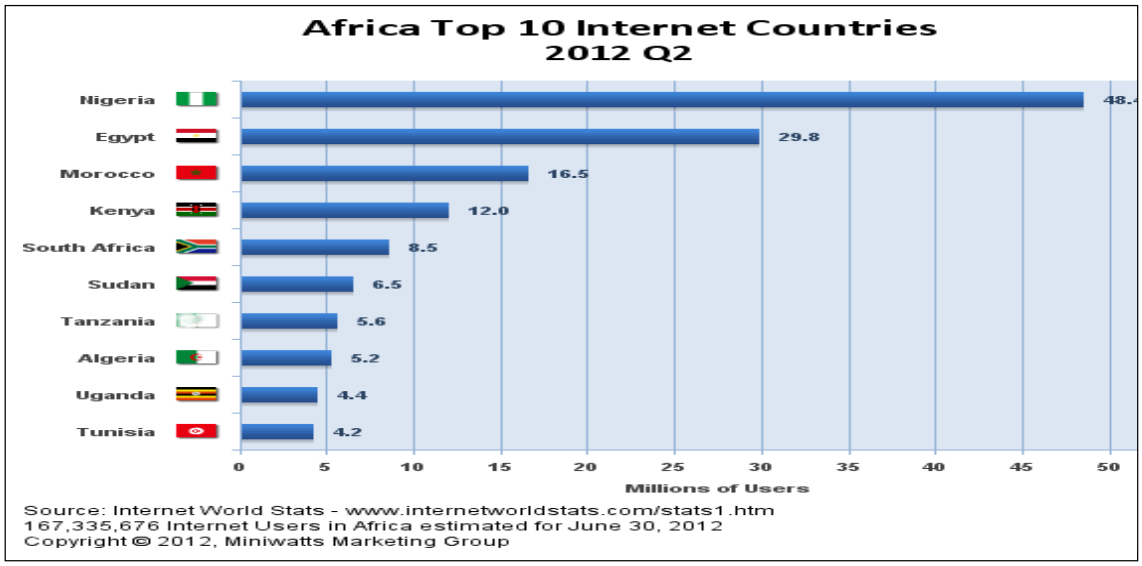

Figure 1: African Top 10 Internet Countries-2012
Source: Internet World Stats- www.internetworldstats.com/stats1.htm

The aim of such a security awareness campaign is to inform the general public about the importance of an attack-free cyberspace in Africa as well as the likely consequences of a security failure or breach in the network, thus creating an awareness and alertness on security issues. The Information Security Forum (ISFOSEC, 2003) defines information security awareness as:

"the degree or extent to which every member of staff understands the importance of information security, the levels of information security appropriate to the organisation, their individual security responsibilities, and acts accordingly" (INFOSEC, 2003).

It should be noted that awareness is not training. The main objective of creating an awareness is to center attention on security. Awareness exhibition, demonstration and explanation are aimed at allowing stakeholders in the information security environment to acknowledge information technology (IT) security challenges and concerns and act accordingly (Martins & Eloff, 2004). It has been established that the learner is the target audience as well as the recipient of information divulged with respect to information security, but that the learner also plays an active role whenever training is organised. Furthermore, awareness depends on getting across to a larger and broader audience with specialized and attractive packaging techniques whereas training has the objective of developing skills and knowledge to simplify job performance (Spurling, 1995).

To comprehensively consider this challenge, awareness programs can be categorised into three distinct groups:

- Past approaches for addressing and creating awareness on information security;
- Present approaches for addressing and creating awareness on information security and
- Future approach for addressing and creating awareness on information security

A review of the literature has been carried out to ensure the categorization as stated above. It has been noted that the inefficiency and weaknesses of some of the current awareness campaign programs are as a result of the environment (establishment) and the type of people implementing it.

Attainment of effective, efficient and dependable information security awareness program would require the combination and aggregation of different information security awareness approaches (Leach , 2003). It is believed that such an approach should consider both the environment as well as the people involved in the process of implementation and would thereby provide a dependable information security awareness program.
The remaining part of the article is organized as follows: Section II briefly explains related work. Section III provides the method used in carrying out the research work while the research questions are stated in Section IV. Section V gives a comprehensive list of awareness programs for information security in Africa. A categorisation of approaches of creating security awareness programs are given in Section VI. Methods and techniques of carrying out awareness programs are presented in Section VII, while the empirical evaluation of the JACAP approach, is discussed in Section VIII. Section IX presents the conclusion of the paper.

2. RELATED WORKS

In a paper presented by Yaacob Ibrahim, the Minister for Communication and Information of Singapore, at a seminar organised by the Information Security Expert of Singapore, he asserted that Singaporeans are currently facing security challenges threatening their digital assets and economy (Yaacob, 2013). To curb these challenges therefore, he suggested and advocated a regular seminar and academic workshop for people of different categories. This approach of creating awareness for achieving attack-free cyber space is weak and flawed because attending workshop and seminar might not be feasible for everybody; it is not everybody that can have interest in attending seminar. More so, the amount participants are usually billed for attending these programmes might not be affordable to all. Hence, the need to come up with a better approach is inevitable.

Connolly et. al., advocate international collaboration among the countries in Africa as the only solution to attack-free cyber space in the continent. In their work, they specifically pointed out that cyber-crime and attacks would have been a scourge of the past had it been international collaboration has been adopted and implemented. They opined that synergy among African countries is essential to the challenge being posed by cyber-insecurity (Chris , Alana , David , & Peter, 2011). The main problems with this approach lie in the economic implication of setting it up (ICT, 2009). What is more, there is no political will to execute it among the government agencies in Africa coupled with the fact that some countries are not fully aware of the implications of cyber-threat to their economy. From the available literatures, the curriculum of various Universities IT curriculums in Africa shows the inclusion of Information Security as a course in countries like Nigeria, South Africa, Namibia, Egypt, Ghana and Cameroun (NSF, 2000). The inclusion of this course has undoubtedly improved the teaching, learning as well as the implementation of skills acquired during the process of teaching. This approach to security awareness is however known with its weakness (Schein , 1985). The training and awareness shall be acquired by few individuals (students and teachers). Also many countries are not showing commitment towards this due to its economic implication. As a result, it does not symbolise a good method of creating security awareness for the entire continent (ISO17799, 2000).

Yan et. al., 2012 developed an architecture for providing information security assurance. The objective is to provide a threat free Internet with a view to preventing attackers from perpetrating evil acts. The architecture is theoretically sound and well explained but was not empirically evaluated (Yan, Zhang, & Zhang). Xu et. al., 2012 provided a scientific approach in solving security challenges on the Internet. In their work they proposed a genetic algorithm for solving security problems. They evaluated previous approaches used for handling this challenge such as fuzzy-C mean algorithm as well as the dynamic programming algorithm. The solution proposed is too technical and scientific and does not provide any evaluative measure to prove its efficiency and reliability (Xu & Liu, 2012). To create a public awareness program on cybersecurity in the public security institutions, a comprehensive archives information digital management system was developed by Li Zhi. This initiative is however constrained by paucity of fund to sustain and implement it (Zhi L. , 2012) especially in a society where there is a broad audience (Copeland & Chiang, 2012). Based on the weaknesses noticed in the above mentioned approaches as established in various literatures and many more literature that are not listed in this paper, the authors therefore considered a better alternative as a solution towards ensuring threat and attack-free cyber space in Africa.

3. METHOD - CONTENT ANALYSIS

Content analysis is the reviewing of existing documentation of related research areas in order to retrieve and extract items of information that are useful to the current research and project (Cassell & Symon, 1994). Content analysis was used to evaluate the various information security awareness approaches.

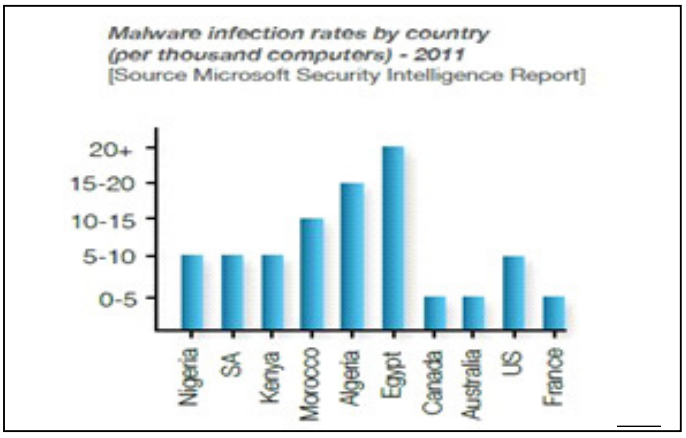

Figure2: Cyber infection rates by country-2011
Source: http://www.infosecisland.com/blogview/22611-On-the-Cyber-Security-Landscape-in- Africa.html

The analysis was carried out using the interpretive approach. According to Mather, the interpretive approach allows a reviewer to read, digest and interpret a given article or document so as to draw connections between these documents and the research area currently being studied (Spurling, 1995).

3.1 Research questions

To investigate the various information security awareness programs, the following research questions were articulated:

- What kind of approaches exist for security awareness campaigns in Africa?
- What are the weaknesses of the existing approaches?
- How do we come up with a new reliable and efficient awareness approach for protecting African citizens from cyber terrorism? Thus how do we conceptualise the proposed joint awareness approach and how can it be implemented in a typical establishment?

To start with, what is hybridisation of security awareness campaign?

Joint awareness campaign programme (JACAP) can be defined as the integration, unification, implementation and utilisation of various awareness campaign programmes to achieve efficient protection of information for individuals and organisations and to ensure the protection of citizens from cyber terrorism.
In order to kick-start this research work, two Universities: the National Open University and University of Lagos in Nigeria were involved. Both tertiary institutions were used because of their proximity to the authors in reaching out to the participants and respondents. A total of 84% valid response was received from the participants. The analysed data yielded the results shown in Table I while its statistical details are provided in section XII.

4. AWARENESS PROGRAMMES FOR INFORMATION SECURITY ACROSS AFRICA

Several information security awareness programmes commonly implemented in Africa:

- International collaboration awareness campaign/sensitization programmes (such as Africa-Asian-Europe collaborative awareness programme) -these operate across borders
- Career orientation programme
- Introduction of courses on information security in colleges and universities
- Organisation of seminars and workshops
- Teachers training and retraining on information security.
- establishing and sustaining information security for enterprise management
- citing / using lessons learnt from previous security challenges
- re-evaluating and re-appraising information security awareness programmes
- Legislative approaches
- Creation of an Information Security Awareness Centre
- Establishment of an information security violation complaint centre
- Getting updates through review and sharing information security cases
- Promulgation of legal action against information security defaulters
- Media orientation / involvement (radio/television)
- Appraising and re-evaluating the effectiveness of the information security awareness program

Table 1: Evaluation of Various Approaches of Creating Awareness Program

Category of awareness program	Awareness programme	Effectiveness rating
Past awareness program approach	Organisation of seminars and workshops/ Public enlightenment	Excellent
	Citing / using cases of lessons learn from previous information security challenges	Good
	Career orientation programme	Fair
	Teachers training and retraining	Fair
Present approaches for addressing and creating awareness on information security	Media orientation / involvement (radio/television)	Good
	Getting updates through review and sharing information security incident cases	Average
	Establishment of IS violation complaint centre	Fair
	Introduction of courses on information security in colleges and universities	Excellent
	Establishing and sustaining information security for enterprise management	Good
Future approach for addressing and creating awareness on information security	International collaboration awareness campaign/sensitization programmes (such as Africa-Asian-Europe collaborative awareness programme) since the operate across the borders	Excellent
	Promulgation of legal action against IS defaulter	Good
	Introduction of IS education in high school	Fair
Proposed/Joint approach for addressing and creating awareness on	Organisation of seminars and workshops/ Public enlightenment	Excellent as evident from the above
	Introduction of courses on information security in colleges and universities	
	International collaboration on awareness campaign/sensitization programmes (such as Africa-Asian-Europe collaborative awareness programme) since the operate across the borders	
	Appraising and re-evaluating the effectiveness of the information security awareness program	

5. CATEGORIZATION OF APPROACHES FOR INFORMATION SECURITY AWARENESS PROGRAMS IN AFRICA

A. Past approaches for addressing and creating awareness on information security

i. Organization of seminars and workshops/ public enlightenment

This is one of the earliest approaches adopted for creating awareness on information security (Stanton , Stam, Mastrangelo, & Jolton, 2005) Seminars and workshops stand as the medium to inform, orientate and sensitise the public about the causes, effects and solutions of threat and attack in the cyberspace. Doing this has assisted the entire public to safeguard the society from any cyber-attacks. The weakness for this approach is that it is not everyone that has time to attend this program.

ii. Using lessons learnt from previous information security challenges

To create awareness built on a solid foundation; several examples of previous cyber threats and attacks are cited. This form of awareness has undoubtedly proved the authenticity of the evil works of cyber criminals.

iii. Career orientation programme

The purpose of this is to create awareness among the students at secondary or high schools level. It is aimed at creating awareness through various courses in IT at colleges and universities that are of immense benefit to a cyber-crime free society in Africa. The career orientation program has provided students with a good insight into their relevant career paths and identifies useful areas of specialisation (Hansche , 2001). The objective is to give students information about career paths such as computer science, information technology which include information security. The main challenge of this awareness campaign program is its cost implication.

iv. Teachers training and retraining

The need for this awareness strategy is very important. When teachers receive training, they become updated on the type of fraud being committed in the cyberspace and will be more informed on how to handle various vulnerabilities. The cost of training and willingness of teachers to attend the awareness training programme are the obstacles.

B. Present approaches for addressing and creating awareness on information security

i. Media orientation / involvement (radio/television)

Media houses are considered the commonest source of information and medium of news to the citizenry. Awareness becomes more pronounced when media are involved. Media houses need to disseminate, sensitize and orientate the population on cyber insecurities. Cost of the media involvement is the only impediment.

ii. Getting updates through review and sharing information security incident cases

Another important awareness campaign in information security is citing 'relevant cases' about cyber-attacks. People who were affected by cybercrime could be asked to share their experiences to allow others to learn from their cases.

iii. Establishment of an Information Security Violation Complaint Centre

In few countries in Africa, there are information security violation complaint centres where victims of cyber-attacks could lodge complaints. Information received through these centres have been helpful and in fact has been used to track attackers. Apart from this benefit, the information gathered through these centres has been useful in getting updates on the fraud and vulnerable activities on the internet (Matveev, 2002)

iv. Introduction of courses on information security in colleges and universities

One significant approach for the creation of security awareness across African countries would be to 'catch' students of higher learning young. More than 65% of universities in Africa do not offer information security as a compulsory course in their computer science curricula. Most students that are well informed about information security did extracurricular professional programmes (Taylor , 2002). Against this backdrop, it is essential for all countries in Africa to strive to include information security as a course in their computer science curricula programme.

v. Establishing and sustaining information security for enterprise management

An information security management system (ISM) is a set of standard rules, guidelines and procedures that has to do with the management of information security (Teare & Da Veiga , 2003).The main objective of ISM is that an establishment or organization should design an information security framework for implementing and maintaining a comprehensive and articulate set of policies, systems and processes to prevent information insecurity (Furnell , Gennatou, & Dowland , 2002)

C. Future approach for addressing and creating information security awareness

i. International collaboration awareness campaign/sensitization programmes (such as Africa-Asian-Europe collaborative awareness programme)

Cyber-attacks affect international networking affiliations. Many of the attackers collaborate internationally to achieve their illicit acts. An international cyber-crime prevention programme and agency need to be established to prevent this. The aim is to study how these acts are being perpetrated in Africa and how they can be thwarted.

ii. Promulgation of legal action against security defaulters

Promulgation of stringent legal action against anyone found exercising illegal cyber activities is a way to curb various attacks (Cassell & Symon, 1994).A specific law should be promulgated against this offence.

iii. Introduction of information securityeducation in high schools

It has been established that young people between the ages of 15-17 years are currently engaging in cybercrimes such as phishing and dictionary attacks across African countries like South Africa, Nigeria and Burkina-Faso (McCroskey & Richmond, 1990). To curb youths from such crime, adequate sensitisation and awareness program should be offered at high (secondary) school level.

D. JACAP approach for addressing and creating awareness on information security

To achieve a dependable and well-oriented awareness program in the continent, the following joint awareness programmes are proposed:

i. Organization of seminars and workshops/public enlightenment
ii. Introduction of courses on information security in colleges and universities
iii. International collaboration on awareness campaign/sensitization programmes
iv. Appraising and re-evaluating the effectiveness of the information security awareness programme for i, ii and iii.

The proposed approach for creating an information security awareness program is depicted in Figure 3. The first stage of the approach is the organisation of seminars and workshops. This stage involves targeting both the learned and non-educated categories. The participants should be encouraged to participate by giving them incentives in terms of food and necessary materials such as books detailing the action of cyber attackers.

The next stage is the introduction of courses related to information security in all colleges, polytechnics and universities. Currently many universities in countries like South Africa, Nigeria, Ghana and Cameroun are offering courses in information security as electives; it is thus optional for a student to register for these courses. Information security should be considered a core subject so that all students have a clear understanding of cybercrime and its threat, before they leave their universities. International collaboration is essential for an efficient and effective rollout of information security awareness. Cyber criminals have developed a collaborative measure for ensuring smooth execution of various cyber-criminal acts. To circumvent this effort, a strong anti-cyber-criminal awareness should be established among all the countries in Africa.

Awareness program re-appraisal is another important aspect of an information security awareness program. Failure of awareness programs is usually recorded only when there is an evaluative mechanism to get feedback about the awareness program. If there is a good evaluative mechanism, the weaknesses and strength of such initiative will be easily determined and corrective measures can be taken. In order to affirm the usefulness and efficacy of this proposed joint approach, questionnaires were distributed to lecturers and students in tow Nigerian institutions to know the acceptability and importance of the awareness program in each category. The results obtained as presented in Table II supports the acceptability of the hybridised approach.

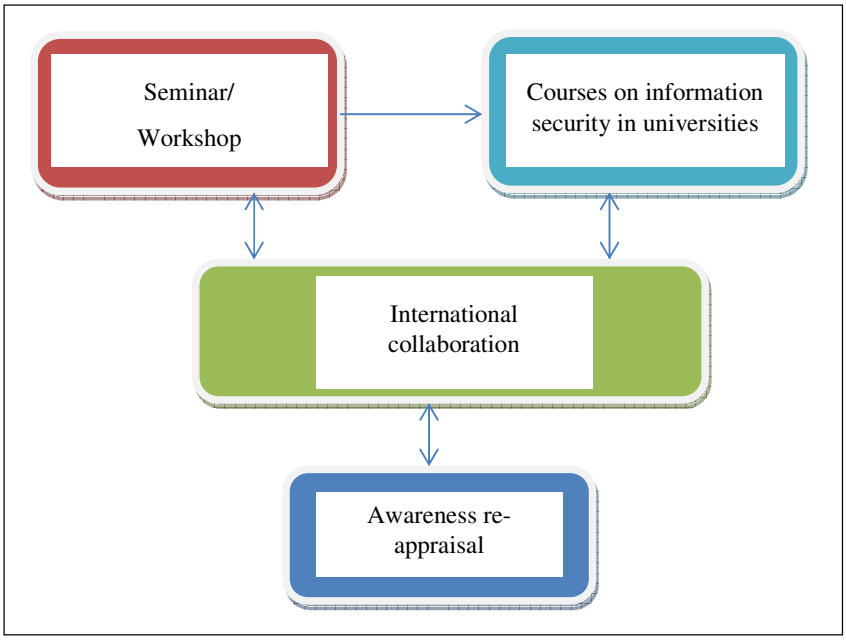

Figure 3: JointAwareness Campaign Programme (JACAP) for addressing and creating awareness on information security in Africa.

Table 2: Rating and evaluation of hybridized awareness program in Africa.

Awareness	**Usefulness and acceptability rate**
Organisation of seminars and workshops/ Public enlightenment	75%
Introduction of courses on information security in colleges and universities	77%
International collaboration on awareness campaign/sensitization programmes (such as Africa-Asian-Europe collaborative awareness programme) that operate across borders	80%
Appraising and re-evaluating the effectiveness of the information security awareness program	78%

6. STEPS TOWARDS EFFECTIVE JACAP IMPLEMENTATION

Many approaches and methods are available to convey an IT security awareness campaign (Cassell & Symon, 1994). The choice of the method depends on the complexity of the awareness campaign program and the resources being considered. Some of the techniques or methods an information security awareness campaigner may adopt, include: Web-based sessions, Agency wide e-mail messages, Videotapes, Web-based sessions, Computer-based sessions, Teleconferencing sessions, In-person, Instructor-led, IT security days or similar events, Pop-up calendar with security contact information and monthly security tips.

In order to ensure a threat and attack-free cyberspace awareness campaign programmes for Africa, the following six principles of Culture of Information Security (Schein , 1985) must be sustained as explained hereunder.
It should be noted that the effective implementation of a joint information security awareness campaign program can only be realised if the six principles of information security are implemented (see Figure 4).

The six principles are:

1) Awareness
2) Responsibility
3) Response
4) Cooperation
5) Ethics
6) Reassessment

Figure 4: principles of "Culture of Information Security"
Source: Schein, E. H. (1985). Organizational Culture and Leadership: A Dynamic View. San Francisco,Jossey-Bass.

a) **Awareness:** all the stakeholders in information and communication technology should be well informed and aware of what should be done to ensure safety and security of information. They should be informed of the implication of not applying security measures to guard and protect their information.
b) **Responsibility**: users of ICT should be aware of their duty and responsibility to reliably secure information on a network according to their respective role in the organisation.
c) **Response**: since ICT is a dynamic phenomenon, all the users should respond appropriately and timely when the need arises regarding the required protection of information.
d) **Cooperation:** through coordinated responses and adequate information sharing, stakeholders in information security should cooperate for dependable information on the network.
e) **Information ethics and rules**: for any shared information there must be strict adherence to rules and ethics governing information sharing.
f) **Reassessment:** this is necessary to monitor and adjust the shortcomings in existing information security approaches and policies. Doing this will encourage improvement to security policies.

7. ANALYSIS OF REPORT OF DISTRIBUTED QUESTIONAIRES

It should be noted that for a questionnaire to be designed for this type of survey, it should cut across all categories of people it is supposed to represent, we choose respondents from two different universities, namely: University of Lagos, Lagos, Nigeria and the National Open University of Nigeria (NOUN). (See the questionnaire attached)
There are 12 awareness programmes under study, 4 from the past approach, 5 from present approach and 3 from future approach, all of which have different levels of responses. Respondents were asked to choose from 4 options, namely excellent, very- good, good and average, replicated for each of the awareness programmes. We now want to choose 3 of the best awareness programmes that will perfectly suit the new joint awareness programme in Africa.
As we can see, the "excellent" option is the best of all the options available in each of the levels of the 12 awareness programmes in literal meaning, but can we just choose any option due to their response ratio without proper confirmations? We need to analyse which option will best be chosen and know which particular awareness programmes should be shortlisted for optimal result.

8. DATA ANALYSIS

From the Analysis of variance tables below (see Table III), the hypothesis to be tested is given as:

H_1: There is no difference in the significance of each treatment options VS
H_2: There is significant difference among the treatment options

From Table III, the calculated F value (41.61155) is far greater than the critical region of the tabulated critical F value (2.866266), thus we reject the null hypothesis. The P value is also very small which confirms that the alternative hypothesis should be favoured, thus we conclude that there is a statistical evidence to show that the options are significantly different in preference from the respondents. Test for interaction is not significant (0.43832<2.363751). This confirms that there is no correlation between treatment options and awareness programmes.
Table III
To further analyze the data since we rejected our null hypothesis, we wish to know which one is better by pair-wise comparison from a procedure called the Tukey Pair-wise Comparison test which is done below:

TABLE 3:

ANOVA

Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Sample	0	2	0	0	1	3.259446
Columns	1321.167	3	440.3889	41.61155	8.63E-12	2.866266
Interaction	27.83333	6	4.638889	0.43832	0.848273	2.363751
Within	381	36	10.58333			
Total	1730	47				

Tukey Criterion, $T=q_{\alpha}\sqrt{\frac{MSE}{n}}$ =3.5497 where q_{α} is the studentized range distribution with degrees of freedom r and n-r.

The hypothesis test is given below and the condition for rejection is when the absolute difference of the mean values of a given pair is greater than the T value.

H_0: There is no statistical difference in the significance of each pairs VS
H_1: There is significant difference in the pair of the treatment options
Excellent &V.good |18.66667-9.5|=9.166667>3.5497*
Excellent & Good |18.66667-6.75|=11.916667>3.5497*
Excellent & Average |18.66667-5.083333|=12.83334>3.5497*
V.good& Good |9.5-6.75|=2.75<3.5497
V.good& Absolute |9.5-5.083333|=4.4166667>3.5497*
Good & Absolute |6.75-5.083333|=1.66667<3.5497
By comparison, it is clear that statistically, there is significant difference in all except the fourth and sixth pairs. This means that statistically there is superiority in mean choices among them but the "excellent" option has the highest priority.
We should also analyze each of the three periods of programme approaches to know which one is best to be used according to their options. This is demonstrated below:

Table IV

SUMMARY FOR PAST AWARENESS

Groups	*Count*	*Sum*	*Average*	*Variance*
Column 1	4	70	17.5	45.66667
Column 2	4	43	10.75	10.91667
Column 3	4	29	7.25	8.25
Column 4	4	18	4.5	1

Table V

ANOVA

Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	378.5	3	126.1667	7.665823	0.004003	3.490295
Within Groups	197.5	12	16.45833			
Total	576	15				

$T=q\alpha\sqrt{\frac{MSE}{ni}}$ =8.5195

Excellent &V.good |17.5-10.75|=6.75<8.5195
Excellent & Good |17.5-7.25|=10.25>8.5195*
Excellent & Average |17.5-4.5|=13>8.5195*
V.good& Good |10.75-7.25|=3.5<8.5195
V.good& Absolute |10.75-4.5|=6.25<8.5195
Good & Absolute |7.25-4.5|=2.75<8.5195

Table VI

SUMMARY FOR PRESENT AWARENESS

Groups	*Count*	*Sum*	*Average*	*Variance*
Column 1	5	94	18.8	24.7
Column 2	5	48	9.6	4.3
Column 3	5	33	6.6	4.3
Column 4	5	25	5	3

Table VII

ANOVA

Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	570.8	3	190.2667	20.96602	8.65E-06	3.238872
Within Groups	145.2	16	9.075			
Total	716	19				

$T=q\alpha\sqrt{\frac{MSE}{ni}}$ =5.4562

Excellent &V.good |18.8-9.6|=9.2>5.4562*
Excellent & Good |18.8-6.6|=12.2>5.4562*
Excellent & Average |18.8-5|=13.8>5.4562*
V.good& Good |9.6-6.6|=3<5.4562
V.good& Absolute |9.6-5|=4.6<5.4562
Good & Absolute |6.6-5|=1.6<5.4562

Table VIII

SUMMARY FOR FUTURE AWARENESS

Groups	*Count*	*Sum*	*Average*	*Variance*
Column 1	3	60	20	12
Column 2	3	23	7.666667	0.333333
Column 3	3	19	6.333333	1.333333
Column 4	3	18	6	3

Table IX

ANOVA

Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	404.6667	3	134.8889	32.37333	8E-05	4.066181
Within Groups	33.33333	8	4.166667			
Total	438	11				

$T=q\alpha\sqrt{\frac{MSE}{ni}}$ =5.3387

Excellent &V.good |20-7.66667|=12.33333>5.3387*
Excellent & Good |20-6.33333|=13.66667>5.3387*
Excellent & Average |20-6|=14>5.3387*
V.good& Good |7.66667-6.33333|=1.33334<5.2287
V.good& Absolute |7.66667-6|=1.66667<5.3387
Good & Absolute |6.33333-6|=1.33333<5.3387

We reject the null hypothesis for all the three awareness category according to the above tables, meaning there is statistical difference in option levels across all the awareness approaches and from their respective pair-wise comparisons, it is clearly indicated that the "excellent" option is the preferred option to choose.

9. CONCLUSION

No doubt that the "excellent" option is statistically the best we must seek for an optimum plan for a joint awareness campaign programme and from table I, the three awareness programmes with an excellent effectiveness rating(namely Organization of seminars and workshops/public enlightenment, introduction of courses on information security in colleges and universities, international collaboration on awareness campaign/sensitization programmes) are picked for optimization of the Proposed/joint awareness approach for addressing and creating awareness on information security. This is also confirmed by the usefulness and acceptability rate displayed in Table III.

Cyber insecurity has negatively impacted upon both the economic and academic growths of the African continent. The analysis of various approaches currently being used and the approach that is considered to be more appropriate have been discussed, analysed and implemented. Based on the effectiveness of the newly developed approach, it is on of no doubt that its adoption in sensitising the entire African populace will be of immense benefit to the whole continent. The insecurity currently being experienced will definitely find its way out of Africa. Having tested this approach (Joint Awareness Campaign Programme (JACAP) for creating awareness in Africa, the authors hereby wish to recommend it to the government of all countries in Africa for a full-scale implementation.

REFERENCES

1. N.A. Azeez, and I.M Venter "Towards achieving scalability and interoperability in a Triple-Domain Grid-Based Environment" 11th Annual Information Security South Africa Conference ISSA 2012 , Johannesburg , South Africa, 15 – 17 August 2012 (Paper 26) (ISBN-978-1-4673-2158-7, IEEE Catalog Number: CFP1266I-CDR)
2. N.A. Azeez, Isabella M. Venter and Iyamu Tiko, "Grid Security Loopholes with proposed countermeasures" , 26th International Symposium on Computer and Information Sciences 26-28 September 2011, Imperial College, London, UK. Grid Security Loopholes with proposed countermeasures, Springer Verlag, London
3. Kruger, H. A., & Kearney, W. D. (2 0 0 6). A prototype for assessing information security awareness. Computers & Security, 289 – 296.
4. ISF. The standard of good practice for information security. Version4.0. Information Security Forum; 2003.
5. ISO 17799. Information technology, code of practice for informationsecurity management. Geneva: International StandardsOrganisation; 2000.
6. Leach J. Improving user security behaviour. Computers and Security2003;22(8):685–92.
7. MartinsA,Eloff JHP.Measuringinformationsecurity,<http://philby.ucsd.edu/wcse291_IDVA/papers/rating-position/Martins.pdf>;2001 [accessed August 2004].
8. Schlienger T, Teufel S. Information security culture – fromanalysis to change. South African Computer Journal 2003;31: 46–52.
9. Spurling P. Promoting security awareness and commitment.Information Management and Computer Security 1995;3(2):20–6.
10. Stanton JM, Stam KR, Mastrangelo P, Jolton J. Analysis of end usersecurity behaviours. Computers and Security 2005;24(2): 124–33.
11. Taylor BW. Introduction to management science. 7th ed. PrenticeHall; 2002.

12. Teare G, Da Veiga A. Information security culture and awareness.Paper presented at the 2003 ISSA Conference, Sandton Convention
13. Furnell SM, Gennatou M, Dowland PS. A prototype tool for informationsecurity awareness and training. Logistics InformationManagement 2002;15(5/6):352–7.
14. Hansche S. Designing a security awareness program: Part 1, information.Systems Security January/February 2001:14–22.
15. Matveev, A. V. (2002). The Advantages of Employing Quantitative and Quantitative Methods in Intercultural Research. Bulletin of Russian Communication Association "THEORY OF COMMUNICATION AND APPLIED COMMUNICATION", 59-67.
16. McCroskey, J. C., & Richmond, V. P. (1990). Willingness to communicate: Differing cultural perspectives. The Southern Communication Journal, 56, 72-77.
17. Cassell, C., & Symon, G. (1994). Qualitative research in work contexts. Qualitative methods in organizational research, 1-13.
18. International Comparison of ICT Trend" by the Ministry of Internal Affairs and Communications (2009)
19. Copeland, W., & Chiang, C.-C. (2012). Securing Enterprise Mobile Information. International Symposium on Computer, Consumer and Control (pp. 1-4). IEEE Computer Society.
20. Xu, L., & Liu, G. (2012). Analyzing algorithms of information security. International Conference on Computer Science and Electronics Engineering (pp. 1-4). IEEE Computer Society.
21. Yan, C., Zhang, Q., & Zhang, Z. (2012). Study on Information Security Assurance Architecture in Internet. International Conference on Computer Science and Electronics Engineering (pp. 1-4). IEEE Computer Society.
22. Zhi, L. (2012). The Construction of Comprehensive Archives Information Digital Management System in the Public Security Service Institutions. International Conference on Communication Systems and Network Technologies (pp. 1-5). IEEE Computer. http://www.infosecisland.com/blogview/22611-On-the-Cyber-Security-Landscape-in-Africa.html
23. Schein, E. H. (1985). Organizational Culture and Leadership: A Dynamic View. San Francisco,Jossey-Bass.
24. Schlienger, T. and S. Teufel (2002). Information Security Culture - The Socio-Cultural Dimension in Information Security Management. In: M. A. Ghonaimy, M. T. El-Hadidi and H. K. Aslan, Eds. Security in the information society: visions and perspectives. IFIP TC11 International Conference on Information Security (Sec2002), Cairo, Egypt, Kluwer Academic Publishers.
25. N0 : http://www.internetworldstats.com/asia/sg.htm
26. N2: https://www.ida.gov.sg/About-Us/Newsroom/Speeches/2013/Speech-by-Dr-Yaacob-Ibrahim-Minister-for-Communications-and-Information-at-the-Information-Security-Seminar-2013
27. N2B Chris Connolly, Alana Maurushat, David Vaile & Peter van Dijk (2011), "An Overview of International Cyber-Security Awareness Raising and Educational Initiatives" Research report commissioned by the Australian Communications and Media Authority.
28. National ScienceFoundation Solicitation NSF 01-11, "Federal Cyber Service:Scholarships forService (SFS) A Federal Cyber Service Training and Education Initiative Program Solicitation", Fall 2000
29. Cassell, C., & Symon, G. (1994). Qualitative research in work contexts. Qualitative methods in organizational research, 1-13.