Factor Analytic Approach to Computer Network/Information Security Awareness in South-Western Nigeria

B.K. Alese, Ph.D.[1*], O.J. Olojo, M.Tech. [2], O.S. Adewale, Ph.D.[1], A.A. Adetunmbi, Ph.D.[1], and S.O. Falaki, M.Ed.[1]

[1] Department of Computer Science, Federal University of Technology, P.M.B. 704 Akure, Nigeria.
[2] Department of Computer Science, College of Education, Ikere-Ekiti, Nigeria.

[*]E-mail: kaalfad@yahoo.com

ABSTRACT

This study was designed to investigate Computer Network Security awareness using a factor analytic approach with Principal factoring method. The principal objective of the study principally was to determine and identify how many latent constructs actually influence Computer Network Security usage and the underlying relationship among them. The work also sought to investigate whether there exists any regularity and order in Computer Network Security Usage. The study also sought to determine whether the nature of an establishment would influence the usage of computer network security measure.

Data was collected from Computer Network users from seven states of the South Western part of Nigeria. A 43 item questionnaire was designed based on different security measures/procedures on Computer Security measures/procedures on Computer Network. The questionnaire used Likert scale structured questions to elicit responses on the frequency of usage of security procedures on the Network. The questionnaire was validated and a test for internal consistently gave Cronbach alpha co-efficient of 0.85. A total of 430 respondents were sampled.

The findings of the study revealed that 14 factors constitute the dominant influence internal attributes on Computer Network Security usage. There was regularity in the pattern of usage. The variables of similar characteristics and in the same family of internal attributes exhibit the same pattern of loadings. It was also observed that the nature of an establishment greatly influences the type of security measures/procedures used. The most frequently used network security measure was found to be "monitor host and network activities" while "availability of any personal cryptographic tools" was found to be the least used measure.

From these findings, the following recommendations were made: Adequate attention should be paid on those 14 internal attributes that were identified and enlightenment campaigns be mounted to disclose to computer network users, the advantages inherent in computer network security usage. Each establishment should identify their peculiar security measures/procedures so as to use them appropriately.

(Keywords: information systems, computer security, network security, network usage)

INTRODUCTION

Security can be defined as freedom from risks and dangers. According to Robinson (2005), a system is generally said to be secured if there are measures taken to avoid a "bad" outcome, where the definition of bad greatly depends on the application scenario. According to this study, the accepted concept of security includes availability, authenticity, authority, integrity, confidentiality and reliability. A great deal of security mechanisms supporting these concepts have been developed, especially since the growth of internet, and have gained wide acceptance in military, business and consumer applications.

As a result of the growing interest in the use of computers, especially in the area of Information Technology, the problem of protecting the confidentiality and integrity of information transmitted on networks has started to generate wide spread attention. Alese (2000), asserted that correct data which are legitimately held must be protected from all forms of unwanted access. Steps must be taken therefore to ensure that no one has an unauthorized access to data belonging to others.

Access control can be introduced at several levels. The system administrator needs certain privileges to obtain access to programs which generate new directories and to impose memory space restriction.

Individual users can access their directories freely, but with caution. Users should not be allowed to access other users directories without valid permission. There is no doubt that data/information is an integral part of the resources of an organization and the world at large, its integrity must however be maintained. Information is power and the data from which information is derived must be adequately protected from unauthorized users. When data is corrupted or gets into the wrong hands, it can spell doom for the original owners of such data. With the proliferation of data communication and networks, the problems of security and privacy become more acute.

The issue of security deals with the collection and use, or misuse, of computer stored data. Alese (2004), observed that security has long been an object of concern and study for both data processing systems and communication facilities. With the developments in information Technology and recently, the landmarks in Internet, the problems may be more acute. Network security is broad and encompasses physical, technical and administrative controls. Security measures protect data/information from malicious or accidental misuse or destruction by controlling access to such data. Network security measures, however, do not mean that intruders will be totally kept out. According to Orhnozee (2002) the objectives of good security measures include:

- dissuade an intruder from attempting an unauthorized access;
- deter intruders to such an extent that they can be detected and apprehended;
- and, make the cost and risk of intrusion greater than the intruder's potential gain.

To select an appropriate set of network security measures therefore, one needs to evaluate the threat, environment, determine whether the main concern is to physically protect the hardware from accidental or malicious damage and access, and/or to protect programs and users data from accidental and malicious modification, disclosure, and destruction. Once that has been established, appropriate security techniques can be selected and applied. Because the data of an organization can vary in type and degree of sensitivity, employees need to be able to exercise flexibility in handling and protecting the data.

The security-related decisions one makes, or fails to make, as an administrator determines how secure or insecure your network is, how much functionality your network offers, and how easy your network is to use. However, you cannot make good decisions about security without first determining your security goals. Until you have determined what your security goals are, you cannot make effective use of any collection of security tools because you simply will not know what to check for and what restrictions to impose. For example, your goals may probably be different from the goals of a product vendor. Vendors are no doubt trying to make configuration and operation of their products as simple as possible, which implies that the default configurations will often be as open (i.e., insecure) as possible. While this makes it easier to install new products, it also leaves access to those systems and other systems through them open to any user who wanders by.

Your goals will be largely determined by the following key tradeoffs:

- ***Services Offered Versus Security Provided.*** Each service offered to users carries it own security risk. For some services, the risk outweighs the benefit of the service and the administrator may choose to eliminate the service rather than try to secure it.
- ***Ease of Use Versus Security.*** The easiest system to use would allow access to any user and require no passwords; that is, there would be no security. Requiring passwords makes the system a little less convenient, but more secure. Requiring device – generated one-time passwords makes the system even more difficult to use, but much more secure.
- ***Cost of Security Versus Risk of Loss.*** There are many different costs to security, such as, monetary (i.e., the cost of purchasing security hardware and software like firewalls and one-time passwords generators), performance (i.e., encryption and decryption) take time and ease of use. There are also many levels of risk: Loss of privacy, data and service. Each type of cost must be weighed against each type of loss.

The goals of an establishment should be communicated to all users, operations staff, and managers through a set of security rules called a "security policy".

What is Computer Network Security?

According to Stalling (1997), computer security can be defined under six major headings, all of which come together to make up network security. According to him, these include confidentially, authentication, integrity, non-repudiation, access control and availability.

Confidentiality: This involves the protection of transmitted data from passive attacks. With respect to the release of message contents, several levels of protection can be identified. The broadest service protects all user data transmitted between two users over a period of time. For example, if a virtual circuit is set up between two systems, this broad protection would prevent the release of any user data transmitted over the virtual circuit. There are also narrower forms of this service, which include the protection of single message or even specific fields within a message. According to Alese (2004), these refinements are less useful than the broad approach and may even be more complex and expensive to influence. Another aspect of confidentiality is the protection of traffic flow from analysis. This requires an attacker not being able to observe the source and destination, frequency, length or other characteristics of the traffic on communications facility.

Authentication: The authentication service is concerned with assuring that a communication is authentic (that is, data is from the right source). In the case of a single message, such as a warning or alarm signal, the function of the authentication service is to assure the recipient of the message that is the source it claims to be from. In the case of an ongoing interaction, such as the connection of a terminal to a host, two aspects are involved. First, at the time of connection initiation, the service ensures that the two entities are authentic (that is, each is the entity it claims to be). Second, the service must assure that the connection is not interfered with in such a way that a third party can masquerade as one of the two legitimate parties for the purpose of authorized transmission or reception.

Integrity: This ensures that only authorized parties are able to modify and transmit information on computer systems. As with confidentiality, integrity can apply to a stream of modification, which includes writing, changing status, deleting, creating or delaying transmitted messages, messages as a single or selected fields within a message. The most useful and straightforward approach is a local stream protection. A connected-oriented integrity service, one that deals with a stream of messages, assures that messages are received as sent, with no duplication, insertion, modification re-ordering or replays. The destruction of data is also covered under this service. Thus, the connection-oriented integrity service addresses both message stream modification and denial of service. On the other hand, a connection-less integrity service is the one that deals with individual messages only, without regards to any larger context. It generally provides protection against message modification only. Kent (1993) points out that a hybrid service can be offered for applications that require some protection against replay and reordering but do not require strict sequencing.

We can make a distinction between the service with and without recovery. Integrity service relates to active attacks, hence one is concerned with detection rather than prevention. If a violation of integrity is detected, then the service may simply report this violation and some other portion of software or human intervention is required to recover from the violation.

Non-Repudiation: Non-repudiation prevents either the sender or receiver form denying a transmitted message. Thus, when a message is sent, the receiver can prove that the message was in fact sent by the alleged sender. Similarity, when a message is received, the sender can prove that the message was received by the alleged receiver.

Access Control: This requires that access to information resources may be controlled by or from the target system. Within the context of network security, access control means controlling the access to host systems and applications via communication links. To achieve this control, each entity trying to gain access must first be identified or authenticated, so that access rights are not given to wrong individuals.

Availability: This requires that assess to information is only given to an authorized user when needed. A variety of attacks can result in the loss or reduction in availability. Some of these attacks are amenable to authentication and encryption, whereas others require some sort of physical action to prevent or recover from loss of availability of elements of distributed system.

RESEARCH METHODOLOGY

A well–structured questionnaire was used for this study. The questionnaire was divided into three sections. The first section required respondents to supply information on their personal data; such as locality, sex, profession and age. The second

section consisted of question items on the names of the establishments, number of branches, network facilities available, operating systems in use, qualifications of the respondents, area of specialization, etc. The third section consisted of 43 question items regarding the various security measures/procedures of information on the computer network. Respondents were required to indicate their responses for the 43 different items. The frequency of usage of the security measures was based on 5–point Likert scale of 1 (very often), 2 (often), 3 (occasionally), 4 (uncommon) and 5 (very uncommon).

The instrument was pre–tested through a pilot survey using 200 computer network users in Akure (Ondo State), Lagos (Lagos State), Osogbo (Osun State), Ibadan (Oyo State), Ado – Ekiti (Ekiti State) and Abeokuta (Ogun State). The results of the pilot survey were analyzed to show lack of ambiguity or misinterpretation of question items. Cronbach alpha model was used to determine the internal consistency.

The responses to the instrument were collated and subjected to factor analysis using both orthogonal and oblique rotations.

Principal components method of factoring was used while Kaiser–Mayer Olkin (KMO) measure of sampling adequacy was applied to test whether the partial correlations among variables was small. Bartlet's test of sphericity was carried out to confirm multi-colinearity between the variables.

DATA ANALYSIS AND RESULTS

This chapter presents the results of the factor analysis. The factor analysis by principal components was adopted in the data analysis for the purpose of partitioning the experimental variables into factors that influence network security awareness. The purpose of factor analysis was to summarize interrelationships and establish levels of variances in decision variables as they influenced a given phenomenon. The following reports were generated in the factor analysis using Statistical Package for Socials Sciences (SPSS) Version 10.0:

(a) Descriptive Statistics

(b) Correlation matrix

(c) Kaiser–Mayer Olkin (KMO) and Bartlett's test

(d) Communalities

(e) Total variance Explained (Eigenvalue)

(f) Total variance Explained (Extraction and Rotation Sums of Squared Loading)

(g) Rotated component matrix Quartimax

(h) Component Score coefficient matrix

Descriptive Statistics: The descriptive statistics give the mean and standard deviation of the sample population on each decision variable. The descriptive statistics are presented in Table 1. From this table, there is simple evidence that "monitor host and network activities" was rated as the highest variable that affect network security awareness, as it has the highest mean (3.36). "Availability of any personal cryptographic tool" on the other hand seems to be the least important variable affecting network security awareness level, as it has the least mean (1.68). This shows a lot about the trend and level of awareness of users.

Correlation Matrix: The correlation matrix calculated presents the degree of pair-wise interrelationships of the decision variables. A positive value in the correlation matrix shows a positive relationship, a negative value shows a negative relationship and a zero value indicates lack of relationship. The general trends of correlation values evidence the fact that most of the variables do not have very strong pair-wise relationships as the values fall between ±0.002 and ± 0.334.

Kaiser – Meyer – Olkin (KMO), Bartlett's Tests and Underlying Assumptions: Table 2 shows the KMO and Bartlett's test of sphericity. The KMO measure of sampling adequacy is 0.822 which shows that the sample is very adequate. The table also shows a Chi-square of 3372.98 and a significant level of 0.000 (3 places of decimal). Hence, the Bartlett's Test is not significant which further indicates that the sample is adequate.

Table 1: Descriptive Statistics

	Mean	Std. Deviation	Analysis N
c1 - Security clearance of personnel	3.33	1.49	377
c2 - Protection password	3.07	1.50	377
c3 - Infromation classification and security formulation	2.83	1.49	377
c4 - Audit trial of transactions	2.87	1.47	377
c5 - Storage devices for hardware	3.24	1.52	377
c6 - Protection of removable storage devices	3.10	1.81	377
c8 - Backup of data files	3.02	1.45	377
c9 - Encryption of files	2.71	1.26	377
c10 - Disallowing eavesdropping equipment	2.64	1.28	377
c11 - Availability of equipment for strong authentication	3.01	1.35	377
c12 - Software mechanisms to identify users of computer system	3.24	1.35	377
c13 - Hardware mechanisms to identify users of computer system	3.00	1.37	377
c14 - Confinement	2.64	1.43	377
c15 - Any cryptographic tool on your operating system?	2.12	1.00	377
c16 - Any personal cryptographic tool?	1.68	.86	377
c17 - Blockage of your channels	2.69	1.45	377
c18 - Dedication of a system to one kind of process at atime	2.80	1.38	377
c19 - Secure internet gateway	3.23	1.54	377
c20 - TCP/IP service access policy	3.00	1.44	377
c21 - Radiation shielding	2.71	1.35	377
c22 - Access control	3.14	1.49	377
c23 - Threat monitoring	3.34	1.42	377
c24 - Memory protection	3.22	1.48	377
c25 - States of privilege	3.05	1.46	377
c26 - Reliability of processor	3.14	1.54	377
c27 - secure modem pools	3.06	1.52	377
c28 - Configured modem pools to deny unauthorized users	2.84	1.35	377
c29 - Secured public access system	3.18	1.48	377
c30 - The use of system security tools	3.02	1.43	377
c31 - Keeping up-to-date	3.26	1.42	377
c32 - Request for vendors' support	2.68	1.31	377
c33 - Assistant of incident handling team	2.64	1.27	377
c34 - The use of digital signature	2.82	1.47	377
c35 - Secure hash standard	2.72	1.42	377
c36 - Use of automated standard	2.94	1.44	377
c37 - Use of an ordered sequence of password	3.00	1.46	377
c38 - Deactivate unnecessary host services	2.85	1.42	377
c39 - Ensure proper server host configuration	2.79	2.50	377
c40 - Monitor host configuration	2.96	1.39	377
c41 - Extreme caution in obtaining software over the internet	2.88	1.43	377
c42 - Restriction of access to subnet	2.88	2.57	377
c43 - Monitor host and network activities	3.36	1.35	377

Table 2: KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.822
Bartlett's Test of Sphericity	Approx. Chi-Square	3372.098
	df	861
	Sig.	.000

Thus, the matrix of the test battery is not an identity matrix and hence it is invertible and the factor analysis model is suitable. For the validity of factor analytic approach, it is assumed that observations are independent and errors are uncorrelated between awareness levels. The scales are additive and each pair of awareness is bi-variate normal distribution.

Table 3 gives the results of extracted communalities of all the variables. It shows the proportion of the variance of a variable explained by the common factors. From the table, it is very clear that "the use of automated standard" has the least percentage (37.7%) of variance that can be predicted or explained by other 42 variables. On the other hand, "Secure hash standard" has the highest variation (71.6%) that can be accounted for by the other 42 variables.

A comparison of the responses by respondents on the Likert scale (Table 4) indicates that the "use of automated standard" is negatively skewed while the "secure of harsh standard" is positively skewed. Thus, while the "use of automated standard" is less influenced by other 42 variables the "secure of hash standard" is greatly determined by other 42 variables.

These results reveal the importance attached to the use of automated standard. The communality of 71.6% of the variation in the "secure of hash standard" can be predicted by the usage of other variables studied. Thus, an improvement in the usage of other variables will have corresponding effect on the secure of hash standard.

Table 5 gives the result of the extracted factors. Fourteen (14) factors are extracted using principal component analysis. The factors accounted for 58.959% of the total variance. This implies that there are fourteen substantively meaningful uncover related pattern of relationship among the variables. In other words, we say there are 14 different kinds of influence on the data, which presents fourteen categories in which computer network security awareness in these localities can be classified.

As can be seen from Table 5, 14 patterns involve 58.959% of variation in the data. The 14 factors are rotated to the terminal solution. The percentage (%) of variance from the rotation sums of squared loading shows that factor 1 has 7.830% degree of comprehensiveness and strength while factor 14 has 2.812%.

Analysis of the high loadings items on each of the 14 factors was undertaking in Table 6 to determine the underlying relationships that exist among the loaded items on the factors.

An analysis of each of the 14 factors clusters of items proffers a recipe for naming the factors.

Clusters of Loadings For Computer Network Security Awareness Profile:

Tables 7 – 20 present the 14 factors addressed above.

DISCUSSION

The component matrix is presented in table 6. It presents the initial loadings as the principal components. The initial factor extraction is achieved by the Ncriterium approach which is based on the social science rule which states that only the variable with loading equal to or greater than 0.4 in absolute term and the percentage greater than 1 should be considered meaningful and extracted for factor analysis (Ogum, 2004).

Table 3: Commonalities (Extraction Method: Principal Component Analysis)

	Initial	Extraction
c1 - Security Clearance of Personnel.	1.000	.603
c2 - Protection Password.	1.000	.598
c3 - Information Classification and Security Formulation.	1.000	.477
c4 - Audit trial of Transactions.	1.000	.588
c5 - Storage Devices for Hardware.	1.000	.606
c6 - Protection of Removable Storage Devices.	1.000	.561
c8 - Backup of Data Files.	1.000	.659
c9 - Encryption of Files.	1.000	.627
c10 – Disallowing Eavesdropping Equipment.	1.000	.534
c11 - Availability of Equipment for Strong Authentication.	1.000	.649
c12 - Software Mechanisms to Identify Users of Computer System.	1.000	.641
c13 - Hardware Mechanisms to Identify Users of Computer System.	1.000	.624
c14 – Confinement.	1.000	.575
c15 - Any Cryptographic Tool on your Operating System?	1.000	.692
c16 - Any Personal Cryptographic Tool?	1.000	.634
c17 - Blockage of your channels.	1.000	.686
c18 - Dedication of a System to one kind of process at a time.	1.000	.603
c19 - Secure network Gateway.	1.000	.640
c20 - TCP/IP Service Access Policy.	1.000	.560
c21 - Radiation Shielding.	1.000	.532
c22 - Access Control.	1.000	.560
c23 - Threat Monitoring.	1.000	.640
c24 - Memory Protection.	1.000	.556
c25 - States of Privilege.	1.000	.624
c26 - Reliability of Processor.	1.000	.587
c27 - Secure Modem Pools.	1.000	.584
c28 - Configured Modem Pools to Deny Unauthorized Users.	1.000	.603
c29 - Secured public access system.	1.000	.466
c30 - The use of system security tools.	1.000	.502
c31 - Keeping up-to-date Information.	1.000	.535
c32 - Request for Vendors' Support.	1.000	.590
c33 - Assistant of Incident Handling Team.	1.000	.547
c34 - The Use of Digital Signature.	1.000	.542
c35 - Secure Hash Standard.	1.000	.716
c36 - Use of Automated Standard.	1.000	.377
c37 - Use of an Ordered Sequence of Password.	1.000	.574
c38 – Deactivate Unnecessary Host Services.	1.000	.574
c39 - Ensure Proper Server Host Configuration.	1.000	.737
c40 - Monitor Host Configuration.	1.000	.474
c41 - Extreme Caution in Obtaining Software Over the Internet.	1.000	.582
c42 - Restriction of access to subnet	1.000	.727
c43 - Monitor host and network activities	1.000	.579

Table 4: Comparison of Responses on Use of Automated Standard and the Secure of Hash Standard

Response	Likert Scale	FREQUENCY		% OF USER	
		Use of Automated Standard	Secure of Hash Standard	Use of Automated Standard	Secure of Hash Standard
Uncommon	1	80	103	18.3	23.6
Occasionally	2	121	115	27.8	26.4
Often	3	16	19	3.7	4.4
Very Often	4	16	19	3.7	4.4
Very common	5	108	90	24.8	20.6

Table 5: Total Variance Explained

	Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	7.023	16.722	16.722	3.289	7.830	7.830
2	2.294	5.461	22.183	2.192	5.219	13.049
3	1.936	4.610	26.793	2.088	4.972	18.021
4	1.603	3.816	30.609	2.044	4.866	22.887
5	1.457	3.468	34.077	1.887	4.492	27.379
6	1.359	3.235	37.312	1.861	4.430	31.809
7	1.305	3.107	40.419	1.673	3.984	35.794
8	1.233	2.937	43.356	1.557	3.706	39.500
9	1.200	2.857	46.213	1.529	3.640	43.140
10	1.117	2.660	48.872	1.480	3.524	46.665
11	1.093	2.602	51.474	1.442	3.434	50.099
12	1.085	2.584	54.058	1.311	3.120	53.219
13	1.046	2.492	56.550	1.230	2.929	56.148
14	1.012	2.409	58.959	1.181	2.812	58.959

Extraction Method: Principal Component Analysis.

Table 6: Rotated Component for Security Procedure Usage

	Rotated Component for Security Procedure Usage	1	2	3	4	5	6	7	8	9	10	11	12	13	14
C31	Keeping up-to-date Information	.672													
C22	Access Control	.585													
C30	Use of System Security tools	.583													
C40	Monitor Host Configuration	.526													
C26	Reliability of Processor	.426													
C36	Use of automated Standard	.426													
C27	Secure Modern Pools		.688												
C10	Disallowing eavesdropping equipment		.593												
C11	Availability of equipment for strong authentication		.489												
C14	Confinement		.415												
C2	Protection Password			.688											
C13	Hardware Mechanism to identify user computer system.			.574											
C8	Back up of data files			.519											
C33	Assistance of incident handling team			.480											
C34	Memory Protection			.419											
C32	Request for Vendor's support				.712										
C34	The use of digital signature				.532										
C38	Deactivate unnecessary host service				.524										
C18	Dedication of a system to one kind of process at a time				.438										
C28	Configure modern pools to deny unauthorized (i)					.686									
C37	Use of ordered sequence of password					.596									
C20	TCP/IP Service Access policy					.579									
C15	Any cryptographic tools on your o/s						.786								
C16	Any personal cryptographic tools						.766								
C21	Radiation shielding														
C23	Threat Monitoring							.723							
C43	Monitor host and network activities							.62							
C1	Security clearance of personnel								.607						
C3	Information classification and security formulation								.579						
C42	Restriction of Access subnet									.837					
C19	Secure network gateway									.688					
C6	Protection of removable storage devices										.642				
C5	Storage devices for hardware										.605				
C29	Secure Public Access System														
C35	Secure hash standard											.719			
C25	States privilege											.547			
C41	Extreme caution in obtaining software cover internet														
C17	Blockage of your channels												.715		
C12	Software mechanism to identify users of computer system.												.454		
C9	Encryption of files													.670	
C4	Audit trial of transactions														
C39	Ensure proper server host configuration														.800

Table 7: Factor 1- Up-to–Date Information, Confidential and Configured Factor

Loadings	The usage of network security
0.672	Keeping up-to-date information
0.585	Access Control
0.583	Use of system security tools
0.526	Monitor host configuration
0.426	Reliability of processor

Table 8: Factor 2- Strong Authentication and Equipment Usage Regulation

Loadings	The use of network Security Procedure
0.688	Secure modern pools
0.593	Disallowing eavesdropping Equipment
0.489	Available equipment for strong authentication
0.415	Confinement

Table 9: Factor 3 - Password Protection and Seeking Assistance Factor

Loadings	The use of network security Procedure
0.688	Protection of password
0.574	Hardware mechanisms to identify users of computer system
0.519	Back up of data files
0.480	Assistance of incident handling team
0.419	Memory protection

Table 10: Factor 4 - Periodic Checking and Elimination of Unnecessary Services

Loadings	The use of network security Procedure
0.712	Request for vendor's support
0.532	The use of digital signature
0.524	Deactivate unnecessary host services
0.438	Dedication of a system to one kind of process at a time.

Table 11: Factor 5 - Access Policies, Sequence Password and Configured Modem Pools

Loadings	The use of network Security Procedure
0.686	Configured modern pools to deny unauthorized users
0.596	Use of ordered sequence of password
0.579	TCP/IP service Access policy

Table 12: Factor 6 - Use of Cryptographic Tools

Loadings	The use of Network security procedure
0.786	Any cryptographic tools on your o/s
0.766	Any personal cryptographic tools?

Table 13: Factor 7 - Monitoring of network activities

Loadings	The use of Network Security Procedure
0.723	Threat Monitoring
0.620	Monitor Host and Network Activities

Table 14: Factor 8 - Personnel Clearance and Information Classification

Loadings	The use of Network Security Procedure
0.607	Security clearance of Personnel
0.579	Information classification and security formation

Table 15: Factor 9 - Network Restriction

Loadings	The use of Network security procedure
0.837	Restriction of access subnet
0.688	Secure Internet gateway

Table 16: Factor 10 - Storage Devices Protection

Loadings	The use of Network security procedure
0.642	Protection of removable storage devices
0.605	Storage of devices for hardware

Table17: Factor 11 - Hash Standard and State of Privilege

Loadings	The use of Network security procedure
0.719	Secure hash standard
0.547	States of privilege

Table 18: Factor 12 - Integrity

Loadings	**The use of Network security procedure**
0.715	Blockage of your channels
0.454	Software mechanisms to identify users of Computer system

Table 19: Factor 13 - Data Encryption

Loadings	The use of Network security procedure
0.670	Encryption of files

Table 20: Factor 14 - Proper Host Configuration

Loadings	The use of Network security procedure
0.800	Ensure proper server host configuration

In this research, Ncriterium is adopted in order to allow the variables to have a free loading and be able to ascertain the exact number of factors that the variables can load on without intervention. A

further investigation of the table reveals that a total of fourteen (14) factors were extracted.

In order to obtain a meaningful factor loading, the principal component matrix was rotated by orthogonal transformation by varimax, equamax and quartimax; then oblique transformation by promax.

After a careful examination of the results of orthogonal and oblique rotations, quartimax seemed to be the most appropriate. This is because whereas varimax and equamax failed to converge after 25 iterations, Quartrimax converged at 24 iterations.

The results also show that the use of automated standard, radiation shielding, extreme caution in obtaining software over the internet and ensuring proper server host configuration failed to load on any factors. This, by implication means that each of these procedures is rarely used. The practice whereby software is obtained over the internet without caution is dangerous as such software can be prone to Trojan horses or viruses. Jagboro (2003), warned that software should only be obtained from known sources.

Factor 1: Keeping Up-to-Date Information, Confidential and Configured Factor

The variables that load significantly high on this factor are mostly those procedures that deal with keeping up-to-date information and controlling access to information on computer systems. Besides, security measures that involves installation and hardware assurance are also loaded on this factor. Keeping up-to-date information has the highest loading of 0.672 which accounted for 45.16% of the variance. The factor also accounts for 34.22%, 33.99%, 27.67% and 18.15% of the variances in access control, use of system security tools, monitor of host configuration and ensuring the reliability of processor, respectively.

The common factor, which produced the highest variance in the data set, explained 7.830% of the total variance in the computer network security awareness pattern. Each of the variables that load on this factor has a correlation: (r): $0.426 \leq r \leq 0.672$.

That this factor accounted for the highest proportion of variance is not unexpected. Access control and keeping up-to-date information remain the cheapest, hence the commonest, security measures in most computerized establishments. According to Stalling (1999), access points are typically used by unauthorized users. He maintained that having many access points increases the risk to an organization's computer and computer facilities. Networks linked to networks outside the organization allow access into the organization from all others connected to that external network. A network link typically provides access to a large number of computer services, and each service, has a potential to be compromised. Hence, controlling such access is a welcome development.

Wack and John (1991) observed that wide – open Network poses security threats on the computer. He added that many sites are configured intentionally to wide-open computer network access without regard to potential abuse.

Factor 2: Strong Authentication and Equipment Usage Regulation.

This factor accounted for 5.219% of the total variance explained. There are four variables that loaded significantly high on this factor. Two of the variables deal with authentication of data while one deals with disallowing eavesdropping equipment. The factor accounted for 47.33% of the variance in secure modem pools. The factor also accounted for 35.16%, 23.91% and 17.22% of the variances in Disallowing eavesdropping equipment, strong authentication equipment and confinement.

Each of the variables that loaded on the factor has a correlation: (r): $0.45 \leq r \leq 0.688$.

Authentication, according to Alese (2004), refers to the process of proving a claimed identity to the satisfaction of some permission-granting authority.

Strong authentication is therefore a procedural mechanism that enables users to obtain access to computing resources. Alese (2004) submitted that modem pools need to be configured to deny access to unauthorized user.

Alese (2004), submitted that system that can be accessed from the modem pools should require very strong authentication such as provision of smartcards and authentication tokens.

Factor 3: Password Protection and Assistance Seeking Factor

This factor accounted for 4.972% of the total variance explained. Five variables loaded significantly on this factor. Three of the variables

That password protection has the highest loading on this factor is not unexpected. Passwording, either of data file or the entire computer system usage is a common phenomenon. It remains the cheapest security measure used by computer network and indeed internet users.

Factor 4: **Periodic Checking and Elimination of Unnecessary Services**

This factor has four variables loaded on it. The factor accounted for 4.866% of the total variance explained. It has a strong correlation r: $0.438 \leq r \leq 0.712$ with request for vendor's support (0.712), use of unnecessary host services (0.524) and dedication of system to one kind of process at a time (0.438). The factor also generated 50.69%, 28.30%, 27.46% and 19.18% of the variances in the variables respectively.

Factor 5: Access Policies, Sequence Password and Configured Modem Pools

This latent factor explained 4.492% of the total variance in all the battery of 43 tests. It has a strong correlation r :$0.579 \leq r \leq 0.686$ with configured modem pools to deny unauthorized users (0.686), use of ordered sequence of password (0.596) and TCP/IP service Access policy (0.579). The factor also generated 47.06%, 35.52% and 33.52% of the variables respectively.

Vinton (1993) reported that wide open policies is one major factor against the security of information on the computer network. He maintained that many sites are configured unintentionally for wide-open access without regard to the potential abuse. He therefore recommended that new and existing network users need to take strong and specific measures to improve computer security. He added that these measures should include creating a TCP/IP service policy, using strong authentication such as one time password and using a secured gateway that can implement network access policies. Strong authentication could involve requesting of a one-time password.

Factor 6: Use of Cryptographic Tools

The factor accounted for 4.430% of the total variance explained. There are only two variables that are loaded on this factor. Each of the variables deals with the use of cryptographic tools. The variable cryptographic tools on your operating system generated 61.78% while personal cryptographic tools generated 58.68% of the variances in each of the variables. Though this factor is the most consistent and stable of all the factor extracted, it is the least used by computer network users as could be seen in table 3.1.

There are many cryptographic tools available to ensure data integrity. A very popular cryptographic tool is the cryptographic checksums which is a tool used to determine whether or not a file has been changed.

Factor 7: Monitoring of Network Activities

This factor accounted for 3.984% of the total variance explained. Two variables, loaded on this factor. The factor has a high loading correlation (r): $0.723 \leq r \leq 0.620$. The factor also generated 52.27% and 38.44% of the variances in the variable, respectively. Waddington (2002) submitted that monitoring involves looking at several parts of the system and searching for anything unusual. He concluded that it is only by maintaining a constant vigil that one expects to detect security violations and react to them on time.

Factor 8: Personnel Clearance and Information Classification

The variables that loaded significantly high are either dealing with personnel clearance or information classification. Security clearance of personnel has a loading of 0.607 while information classification and security formulation has a loading of 0.579. The factor also accounts for 36.84% and 33.52% of the variances in respective variables. It has a reasonably high loading correlation: (r): $0.579 \leq r \leq 0.607$. This common factor, explained 3.706% of the total variance explained.

Factor 9: Network Restriction

The variables that loaded significantly high on this factor are mostly security measures that deal with network restrictions. Restrictions of access subnet has a high loading of 0.837 while the usage of internet gateway has a loading of 0.688. The factor also accounts for 70.06% and 47.33% of the variances in Restriction of access subnet and secure internet gateway respectively. This

common factor explained 3.640 of the total variance in the network security awareness pattern. Each of the variables that loaded on the factor has a correlation (r): $0.688 \leq r \leq 0.837$.

Stallings (1999) suggested that when computers are networked, the network administrator should make use of a firewall in order to restrict access to traffic on the subnet. He added that access in and out of the subnet through the firewall should be limited to only that are required in order to be consistent with services provided.

Factor 10: Protection of Storage Devices

This factor accounted for 3.524% of the total variance explained. All the variables deal with storage devices. The factor generated 41.22% of the variation in protection of removable storage devices and 36.60% storage devices for hardware. It has a loading correlation (r): $0.605 \leq r \leq 0.642$.

Factor 11: Hash Standard and States of Privilege

Factor 11 accounted for 3.434% of the total variance explained. Two variables were loaded on this factor. The variables have high loading correlation
r: $0.547 \leq r \leq 0.719$.

Factor 12: Integrity

Factor 12: accounted for 3.12% of the total variance explained. Two variables loaded on this factor. They are "Blockage of your channels" (0.715) and "software mechanism to identify users of computer system". (0.454). Alese (2004), defined integrity as the state of information such that it is complete, correct and unchanged from the last time in which it was verified to be in an" integral" state.

Factor 13: Data Encryption

The common factor "Data Encryption" has a reasonable correlation of 0.670. The factor explains 2.929% of the total variance in the network security awareness profile. The use of Encryption is a veritable tool for ensuring security of data on the computer network.

Davies and Price (1980) reported that a lot of methods are available to ensure the overall security of the system. These methods include access control techniques, password, physical protection and encryption/decryption techniques.

Factor 14: Proper Host Configuration

The variable "ensure proper server host configuration" has a high significant loading (0.800) on this factor. It is the only variable with a high correlation. The factor explained 2.812% of the total variance in the computer network security awareness profile.

Component Score Coefficient Matrix

It must be noted that a factor can be estimated as a linear combination of the original variables. Factor component score coefficient matrix (Appendix 3), expresses such linear relationships. It can be used to estimate the level of network information security awareness based on the fourteen factors. This is achieved by forming a linear equation of the weighted standard scores of the íth networked establishment on the variable.

If the standard scores of the networked establishment in the 43 variables under consideration are Si_1, Si_2 Si_3……Si_{43}; then, the network information security awareness level of the establishment considering the fourteen factors, denoted by E_j, j = 1, 2, ……14. are defined by:

$E_1 = (-0.67)\ S_{11} - (0.066)\ S_{12} + (0.023)\ S_{13} + \ldots\ldots\ldots + (0.021)S_143$

$E_2 = (-0.053)\ S_{21} - (0.055)\ S_{22} + (0.034)S_{23} + \ldots\ldots\ldots\ldots - (0.045)S_243$

$E_3 = (0.041)S_{31} + (0.086)\ S_{32} - (0.028)\ S_{33} + \ldots\ldots\ldots\ldots - (0.012)S_343$

.

.

.

.

$E_{14} = (0.064)S_{14,1} - (0.003)S_{14,2} + (0.113)S_{14,3} + \ldots\ldots\ldots - (0.047)14,43$

For each of the factors, a system of equations for the sample population of the following general form is obtained.

$$\begin{pmatrix} B_{11}S_1+b_{1,2}S_2+b_{1,3}S_3+\ldots\ldots\ldots\ldots\ldots\ldots b_{1,113}S_{43} \\ \\ \\ B_{m,1}S_1+b_{m,2}S_2+b_{m,3}S_3+\ldots\ldots\ldots\ldots\ldots\ldots b_{m,43}S_{43} \end{pmatrix} = \begin{pmatrix} E_1 \\ \\ \\ E_m \end{pmatrix}$$

CONCLUSIONS

Computer theft cannot be totally eliminated, but departments can greatly reduce it by following these simple rules:

- implement an identification system for employees, visitors and trade persons,
- provide adequate security for the facility and ensure that barriers exist for the protection of computers, through the use of physical security devices, electronic intrusion detection or security-cleared guard force,
- implement a security awareness program that suits the department, and
- inform employees that they will be held responsible for organization assets lost or stolen because of carelessness.

Although there are no simple solutions, computer theft can be controlled in a cost-effective manner through a team effort from everyone in the workplace – ministers, directors, managers and all employees. All the 14 identified factors that determine and influence the usage of computer network security measures/procedures should be seriously focused so that the country could be freed from the incidence of hackers and crackers.

REFERENCES:

1. Alese, B.K. 2000. "Vulnerability Analysis of Encryption/Decryption Techniques of Computer Network Security". M.Tech. Thesis, Federal University of Technology, Akure, Nigeria.
2. Alese, B.K. 2004. "Design of Public Key Cryptosystem using Elliptic Curve". Ph.D. Thesis. Federal University of Technology, Akure, Nigeria.
3. Davies and Price. 1980. *Security for Computer Networks.* John Willey and Sons: New York, NY.
4. Jagboro, C. 2003. " The Ins and Outs of Door Locks". *Security Management*. 37(2): 48 – 53.
5. Kent, S. 1993. *Architectural Security: Internet System Handbook Reading.* M.A. Addison – Wesley, New York, NY.
6. Ogum, G.E. 2004. "Foundation & Postgraduate Course in Multivariate Analysis". Unpublished Lecture Notes on Research and Statistics, Nnamdi Azikwe University, Awka.
7. Orhozee, E. 2000. "More Promising E – Governance strides in Nigeria". *PC World West Africa*. August Edition. I.T. Media Group.
8. Robinson, G. 2005. "Devising a Strategy Keyed to Locks". *Security Management*. 36(1): 55 -56.
9. Stalling, W. 1997. "Infosecurity and Shrinking Media". *ISSCA Access*. 5(2):19 – 22.
10. Stalling, W. 1999. *Cryptography and Network Security: Principles and Practice*. Prentice Hall; Princeton, NJ.
11. Vinton, C. 1993. "A Password: A New Proactive Password Checkers". Proceedings, 6th National Computer Security Conference.
12. Wack and John. 1991. "Establishing A Computer Security Incident Response Capability". NIST Special Publications: Washington, DC.
13. Waddington, R. 2002. "Policy Development". In: *Information Systems Security: A Practitioner's Reference*. Van Nostrand Reinhold: New York, NY. 411 – 427.

ABOUT THE AUTHORS

Dr. B.K. Alese, *MNCS, MACM, MIEEE*, is a Lecturer I in the Department of Computer Science, Federal University of Technology, Akure, Nigeria. He holds a B. Tech. degree in Industrial Mathematics from The Federal University of Technology(1997). His M.Tech. and Ph.D. degrees in Computer Science are from the same University, in 2000 and 2004, respectively. Dr. Alese joined the Federal University of Technology, Akure in 1998. He is the former Assistant Director of the Post Graduate Diploma Programme of the University and is a current member of the University Senate and various committees. His Research interests are information security, quantum communication, computer networks, and digital signal processing. He has more than 40 publications in both local and international journals and conference proceedings. He is a member of numerous professional organizations such as Nigerian Computer Society, Association for Computing Machinery, and Institute of Electrical and Electronics Engineers. He is actively involved in Postgraduate Supervision and is currently supervising many Postgraduate Students both at Masters and Doctoral levels.

Mr. A. O. Adetunmbi, *MIEE,* received his B.Tech. and M.Tech. degrees in Computer Science from the Federal University of Technology in 1994 and 2000 respectively. Currently, he is a Lecturer at the Department of Computer Science, Federal University of Technology, Akure. He worked with the Department of Computer Science, University of Ado – Ekiti, Nigeria from 2001 to 2004. He was a Post Graduate Research Fellow of the Institute of Computing Technology, China Academy of Sciences, Beijing China. His Research interests are information security, machine learning, and natural language processing. He is a graduate Student Member of IEEE.

Prof. S. O. Falaki, F*NCS FCPN, MACM, MIEEE, MNSE, CORENM,* is a Professor of Computer Science at the Federal University of Technology, Akure, Nigeria. He holds two M.Sc. degrees in Electrical and Electronics Engineering and Computer Science from Leningrad Polythecnical Institute (1969) and University of California (1974), respectively. He obtained his Ph.D. degree in Electrical and Electronics Engineering from University of Lagos (1981). He was a Lecturer at the University of Lagos and joined Federal University of Technology, Akure in 1983. Professor Falaki is a Fellow of Nigeria Computer Society, and Computer Professionals Registration Council of Nigeria. He is a member of many professional organizations such as Institute of Electrical and Electronics Engineers, Association for Computing Machinery, and Nigerian Society of Engineers. He is also CREN Registered. His research interests are digital signal processing systems with emphasis on the hardware design and implementation of digital filters, computer networks, computer system architecture, and mini- and microprocessor systems. He has supervised more than 30 students at Masters and Doctorate degrees levels. He has equally held many administrative positions both within and outside the University. He has over 70 publications to his credit in both local and International Journals and Conference Proceedings.

Dr. Olumide Sunday Adewale *MIEE,* received a B.S. (Combined Honours) in Computer Science with Mathematics from the then Ogun State University (now Olabisi Onabanjo University), Ago-Iwoye, Nigeria, a M.Tech. in Computer Science, and a Ph.D. (Computer Science) from the Federal University of Technology. He is a Senior Lecturer in the Department of Computer Science, Federal University of Technology, Akure, Nigeria. He was an associate member of the International Centre of Theoretical Physics, Trieste, Italy between 2000 and 2005. He has published a number of articles at both local and international reputable journals. He currently sits on the First Bank of Nigeria Plc Nigeria Professorial Chair in Computer Science of the Federal University of Technology, Akure, Nigeria. His research areas include web-enabling applications, modeling and simulation, high-performance and high-availability computing, grid computing, and tele-traffic engineering

Mr. Jethro Olojo, obtained his B.Sc. (Edu) and M.Ed. degrees in Mathematics Education from University of Nigeria Nsukka, Nigeria. He also obtained PGD and M.Tech degrees in computer Science from Federal University of Technology, Akure, Nigeria. He is lecturer at the College of Education, Ikere Ekiti, Nigeria.

SUGGESTED CITATION

B.K. Alese, O.J. Olojo, O.S. Adewale, A.A. Adetunmbi, and S.O. Falaki. 2007. "Factor Analytic Approach to Computer Network/Information Security Awareness in South-Western Nigeria". *Pacific Journal of Science and Technology*. 8(2):351-366.