Information System Security Threats and Vulnerabilities: Evaluating the Human Factor in Data Protection

Omar Safianu
Department Of Computer Science
Kwame Nkrumah University of Science and Technology,
Kumasi, Ghana

Frimpong Twum
(Corresponding Author)
Department Of Computer Science
Kwame Nkrumah University of Science and Technology,
Kumasi, Ghana

J. B. Hayfron-Acquah
Department Of Computer Science
Kwame Nkrumah University of Science and Technology,
Kumasi, Ghana

ABSTRACT

Researches in information security have all these while been concerned only with technical problems and efforts to improve information security have been software-centered or hardware-oriented. There have been limited attempts in addressing the people who use the computers though they are the greatest loophole in information systems security. This paper examines and addresses the threats end-users pose to systems security. Regardless of the countlessly introduced technological solutions aimed at addressing system vulnerabilities, the human factor is still of greater threat to systems security. The study draws its data from a survey conducted on people who frequently use information systems. Professional and technical inputs were also solicited from IT personnel through interviews. Four experiments were conducted to test the accuracy of the survey. A phony phish system was developed to test respondents' information security consciousness. The goal of the phony phish system was to send phishing emails that can be used to measure the accuracy of the survey. The rest of the experiments were SQL injection, cross site scripting and brute force attack.

The results from the study revealed that, the numerous technical advances in information technology do not always produce more secure environments. Thus, information security cannot be described as solely a technical problem. Computers are operated by people and this means that information security is also a human factor issue. It is therefore suggested, for information and data breaches to be curbed, organizations must adopt a holistic security framework, incorporating the human factor.

General Terms

SQL Injection, SQL Vulnerabilities, Social engineering, Phishing Attack, Cross Site Scripting (XSS), Human Factor

Keywords

Database misconfiguration, Insider threat, Login attempts, Personal security policy, privacy settings

1. INTRODUCTION

Information security refers to the protection of the confidentiality, integrity and access to information [1]. Evidence suggests that, regardless of the number of technical controls in place, organizations will still experience security breaches [2], [3]. The 2007 CSI Computer Crime and Security Survey reported that although 98% of users have anti-virus software, 52% were still infected with viruses [4]. This is because information security is not only a technical problem, but is also a 'people' problem [5]. Evidence suggests that employees' failure to comply with information security guidelines is the cause of the majority of breaches in information security [6].

Efforts to improve Information Security have been software-centered or hardware-oriented. So far, there have been limited attempts in addressing the people who use the systems. A company may have purchased the best security technologies that money can buy, trained their people so they can oversea these technologies, and even hire security personnel to guard the business. The company may still be vulnerable as a result of the human factor.

Information security has to incorporate the system users, but unfortunately, many organizations focus on hardware and software solutions, leaving "people-ware" out of the equation.

This research therefore addresses the human factor in information security. It is hoped the vulnerabilities and the recommendations proposed help individuals and organizations to take a second look at their information security infrastructure.

2. LITERATURE REVIEW

Several studies have identified area of vulnerabilities in information systems but most have focused on a technological solution rather than tackling the human factor to systems security. For example, Philip et al. (2003) [3], Smith (2004) [6], James et al. (2009) [2], Silver (2013) [7], and Anita et al. (2013) [8], have all concentrated their research studies on evaluating technological (hardware/software) vulnerabilities but have all left out the critical human factors that contributes to systems security lapses. Although most of these studies used one of the two broad categories of encryption methods (Symmetric Key methods or Asymmetric Key methods) to secure systems, studies have shown weaknesses in these methods. Encryption though is a very useful tool for protecting the confidentiality of information in storage or in transit, weaknesses in encryption algorithms have permitted intruders access to confidential information. Research has shown that no matter how sophisticated encryption and cryptosystems have become they have retained the same flaw(s) that the first systems contained thousands of years ago. If you discover the key (the method used to perform the encryption) you can determine the message. They concurred that key management is not so much the management of technology but rather the management of people. They, however, did not show how managing people or how the human factor could address the vulnerabilities in encryption algorithms. The breaking of every new cryptosystem makes it imperative for researches to shift attention to other methods of protecting data and one of such methods is evaluating the human factor. Security can be compromised in any software or hardware system. According to Mitsui (1994) [9], the Data Encryption Standard (DES) system which was initially thought to be secured for example was broken into by differential cryptanalysis. Elbaz and Bar-El (2000) [10], found out that the DES algorithm suffers from Simple Relations in its key sand this vulnerability reduces the algorithm strength by one bit. The AES system which is the most advanced method for encryption is not flawless. Cryptography researchers have identified a weakness in the AES security algorithm that can crack secrete keys faster than before [11]. Elbaz and Bar-El (2000) study outlines all the known encryption algorithms and their weaknesses. Shulman (2006) [12] also outlines ten vulnerabilities associated with database infrastructures but none of them talked about the activities end users do that make information systems vulnerable to attacks which is the study focus. Firewall vulnerabilities have also been discussed in the literature. Firewalls protect a trusted network from an untrusted network by filtering traffic according to a specified security policy. Firewalls can be software or hardware and vulnerability studies in them are classified according to the vulnerabilities in the software, the hardware and vulnerabilities due to misconfiguration [13. Software vulnerabilities are flaws that exist in software as a result of poor design, bad programming, etc. that can cause a software system to behave abnormally when triggered by a user or exploited by a hacker [14], [15], [16].

These studies however are all based solely on evaluating the security of either a technology or an algorithm ignoring the human factor.

The study therefore put forward the following three hypotheses:

H1- System users will respond to phishing attacks via phishing emails

H2- System users will click on a link that ask them to update their login details use weak passwords to access systems

H3- System users use weak passwords to access systems

3. METHOD

The research employed two approaches: experiments and surveys.

3.1 Experiments: Penetration Tests

The purpose of these tests was to find out vulnerabilities that put data at risk by verifying if corporate application systems are exposed to security vulnerabilities that emanate from human errors. The methods used were:

- Social engineering
- SQL injection
- Cross Site Scripting (XSS)
- Brute force attack

3.1.1 Social engineering

Social engineering penetration attempts were performed on corporate employees to find out if they follow security standards and policies. The attack was conducted by developing a phony phish system as shown in fig.1. The goal of the phony phish system was to send phishing emails to aid with measurement for the study. Components of the Phony Phish System are made up of HTML form, PHP scripts, SMTP server, and HTTP server.

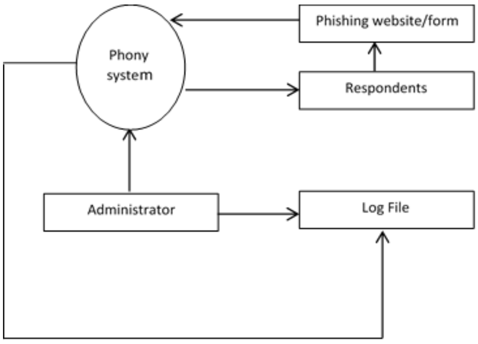


Fig.1: Components of the Phony Phish System

Phishing attack: The study used an unannounced phishing attack to measure accuracy of the survey. The attack requested respondents to visit a page which subsequently asks them to enter specific data to continue. The email was formulated as follows:

Hello,

I got your mail from a colleague who thought you would like this video. At least, I think it is one of the funniest videos I have seen in a long time.

http://bitly.com/1IeLs6s

Regards, Issa.

The raw data gathered from this social engineering attack is tabulated in table 1.

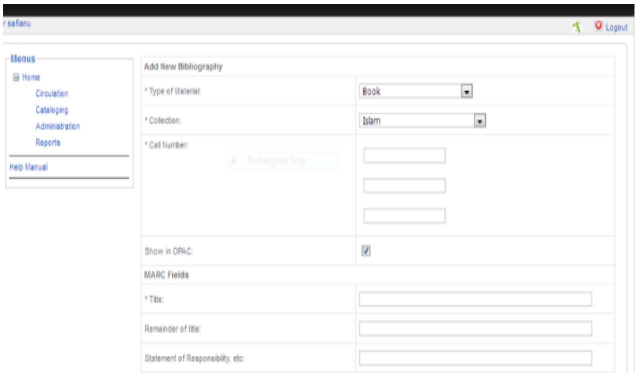
Table 1: Emails sent in social engineering attacks

No. of emails sent	43	
Reachable	Responded	No-Response
	28	8
Non-Reachable	7	

It should be noted that, unlike real phishing attacks, no actual information was collected from the respondents, no software was installed on their systems, and the security of their systems was in no way compromised in this experiment.

3.1.2 SQL Injection

An error-based SQL Injection attack string was formulated to ascertain if the corporate web application was vulnerable to attacks. Two criteria were used to detect vulnerability. Firstly, the web app has to allow execution of queries from the url, and secondly, it should show an error for some kind of query. An error shown to the end user is an indication of SQL vulnerability. A web page that is properly configured shouldn’t execute any SQL statement from the end user. However, that was not the case for the web app under investigation. The page displayed before the injection of the SQL statement is shown BY fig.2.



Add New Bibliography

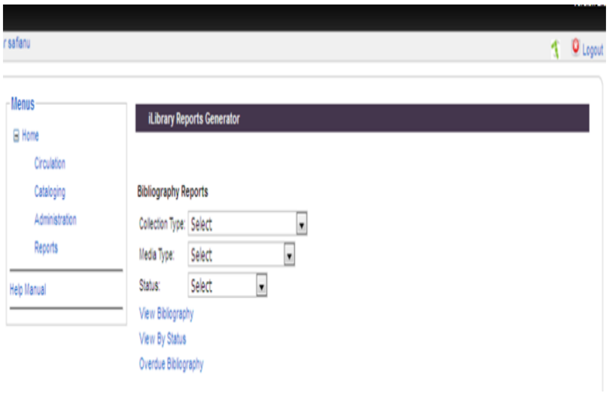
* Type of Material:	Book
* Collection:	Islam
* Call Number:	
Show in OPAC:	☑
MARC Fields	
* Title:	
Remainder of title:	
Statement of Responsibility, etc:	

fig.2: The page shown before the attack

The query included in the URL was: xxx-server/library/iLibAdmin?id=1 or x=1 (the names of the web resources were replaced with xxx for security reasons). Since “x=1” is not a valid SQL syntax it won’t execute but will throw an exception (error). It must be noted that several queries were tested with the URL and all show a kind of error.

3.1.3 Cross Site Scripting (XSS)

Cross Site Scripting vulnerabilities most often happen when user input is incorporated into a web server's response (i.e., an HTML page) without proper validation. To do this, a java script (<script>alert('123')</script>) was injected in the url. The page before the attack is as shown by fig.3.



Bibliography Reports

Collection Type: Select

Media Type: Select

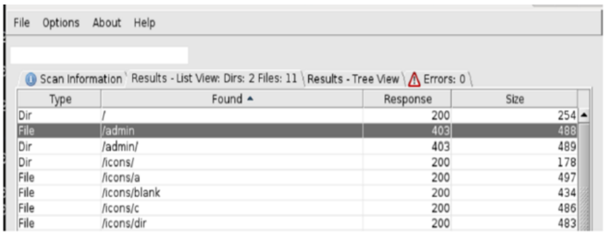
Status: Select

fig.3: Page before XSS attack

3.1.4 Brute Force Attack

Brute force attempts were made to reveal some of the human factors that can make data vulnerable to attacks. To do this the admin webserver interface was accessed. OWASP DirBuster, which is an open source (third party) software, was used for the test. The admin xxx-server/xxx/admin webserver was found to be running an Apache webserver on port 81. Accessing the root URL of this site resulted in the display of a blank page. A quick enumeration scan of the system looking for common directories and files was made.

To prepare a targeted brute force attempt against this system, a custom dictionary file based on the content of the web app was compiled fig.4. The initial dictionary consisted of 66 custom words, which were then put through several rounds of permutations and substitutions to produce a final dictionary file of 3,240 words. This dictionary file was used along with the username “admin” against the protected section of the site.



Type	Found ▲	Response	Size
Dir	/	200	254
File	/admin	403	488
Dir	/admin/	403	489
Dir	/icons/	200	178
File	/icons/a	200	497
File	/icons/blank	200	434
File	/icons/c	200	486
File	/icons/dir	200	483

fig.4: Listing of the system’s folders

The brute-force attack uncovered a password for the admin user. These credentials were leverage to successfully gain unauthorized access to the protected portion of the system.

3.2 Surveys

3.2.1 Smoke-screen approach

A smoke-screen approach was used in the survey as it is more effective to capture the respondents’ security awareness if they are not aware of their awareness being assessed. This is because the respondents might act differently if they knew that their awareness was being assessed. Thus, the survey was entitled “Effectiveness in student-staff relationship”. The title was chosen so that the respondents would not realize that the survey was about information security.

The survey consisted of 7 scenarios out of which 2 were general scenarios used as diversion from the covert subject. The 5 other questions had the real purpose of investigating respondents’ tendency to:

- Click on links from unverified senders
- Install programs as requested by an unknown person
- Give away username and password
- Using weak or strong password

3.2.2 Interviews

To augment data to the questionnaires, ten IT professionals were interviewed. The IT professionals work in various roles in the IT industry. Their views were solicited on the practices and behaviours (human factors) that employees exhibit that can make data and information vulnerable to attacks and theft. The interview was unstructured which allowed open responses. The responses were transcribed and analyzed.

3.2.3 Entropy Formulae

The entropy formula was used to measure the password strength of respondents. The entropy formulae states that E=log2 (x)*L where E is the entropy, x is the pool of characters used in the password and L is the length of the password. An $E \geq 80$ bits signifies a strong password and $E < 80$ bits signifies a weak password. The entropy was calculated by looking at the pool of characters used by respondents.

4. RESULTS

The results of this study are presented in two parts. The first part concerns with the experiment results. The second part deals with the surveys.

4.1 Experiments

The variables that were tested for the social engineering experiment were:

Respondents tendency to install programs requested by an unknown person

Respondents’ tendency to give away username and password

Respondents' password strength

Out of the 43 email messages sent through the phony phish system, 25 respondents followed the link within the email message and visited the experiment website. The termination of the experiment website was at a time when the website was still reporting visits and as such the correct percentage of unique visits is likely to have been higher. All the people who followed the link and visited the first page of the website also clicked the 'continue' button to proceed. This was evidenced by the number of emails collected in a log file. This confirmed the respondents did not accidentally clicked on the first page, as making the same mistake consecutively would have been unlikely. The study therefore concludes respondents are likely to respond to phishing emails attacks and other attacks from hackers. H1 is therefore supported.

Out of the 43 email messages sent for the second attack, 19 respondents followed the link within the email message and visited the experiment website. The attack was performed to see if respondents will click on a link that asks them to enter their credentials. Unlike real phishing attacks, no actual information was collected from the respondents. This study was interested in finding out whether they are likely to click on a link that asks them to update their log in details. The result from the study revealed respondents are likely to give away their login credentials to attackers and the repercussion could be great. H2 is supported.

One of the issues in information security vulnerability is in relation to password. Data on the kind of characters respondents used for their password were collected. This our study view it as a way to measure the strength or weakness of respondents' password as having a weak password can make an information system vulnerable to attacks.

The study revealed that respondents use a phrase, numbers, lower case letters, upper case letters, or a combination of them to generate their passwords.

On average, respondents use up to seven (L=7) characters to generate their password. In computing for E in various combinations the following results were derived:

A password generated from the pool of lowercase characters only: E=log2 (26) *7= 32 bits

A password generated from the pool of alphanumeric characters: E=log2 (36)*7=36 bits

A password generated from the pool of alphanumeric and symbols: E= log2 (57)*7= 40 bits

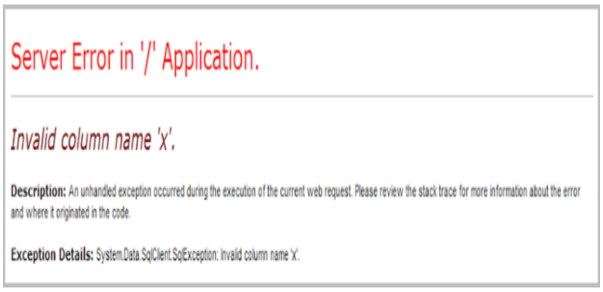
A password generated from the pool of all the keyboard characters: E= log2 (94)*7=45 bits.

Therefore, the overall strength of password of the respondents can be described as very low since the length of password of majority of the respondents is 7 which will give an E< 80 bits. To have an E ≥80 bits security, a password will need at least an L=13 from the pool of all keyboard characters. **H3** is also supported.

In the SQL Injection attack two criteria were used to detect vulnerability:

- Does the web app allow execution of queries from the url?
- Does the server throw back exception (error) to the browser?

An invalid SQL query was included in the URL of the system and run. The query included in the URL was: "xxx-server/xxx/?id=1 or x=1". As "x=1" is not a valid SQL syntax the query did not execute but throws an exception error. It was found out during the attacks that the system displayed an error for some queries. Fig.5 shows the experiment result.



Server Error in '/' Application.

Invalid column name 'x'.

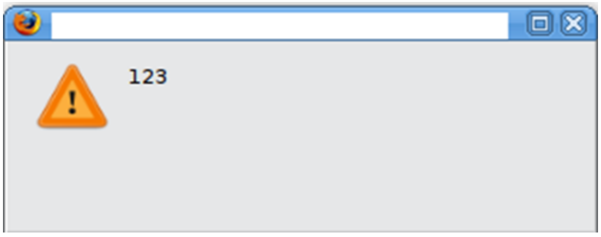
Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Data.SqlClient.SqlException: Invalid column name 'x'.

fig.5: The page shown after attack

An error displayed to the end user is an indication of a SQL vulnerability and hence data vulnerability. This could be classified as human factor because the database system was not configured properly by the developers.

During the Cross Site Scripting (XSS) a basic JavaScript was injected into the system's URL in order to test if this vulnerability persists in the system. The result shown by fig.6 indicate there is an XSS vulnerability because the application echoed back the JavaScript payload (<script>alert('123')</script>) on the page returned by the server.

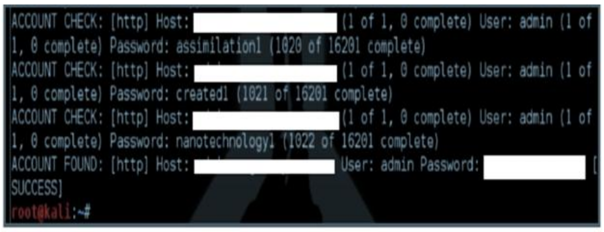


123

fig.6: Cross Site Scripting (XSS) test result

This could also be attributed to human factor because the system lacks a filter that checks for malicious (dangerous) content.

The experiment also found out the system is vulnerable to brute force attacks. A dictionary file was used along with the username "admin" against the protected section of the site (fig.7).



```
ACCOUNT CHECK: [http] Host: [redacted] (1 of 1, 0 complete) User: admin (1 of
1, 0 complete) Password: assimilation1 (1020 of 16201 complete)
ACCOUNT CHECK: [http] Host: [redacted] (1 of 1, 0 complete) User: admin (1 of
1, 0 complete) Password: created1 (1021 of 16201 complete)
ACCOUNT CHECK: [http] Host: [redacted] (1 of 1, 0 complete) User: admin (1 of
1, 0 complete) Password: nanotechnology1 (1022 of 16201 complete)
ACCOUNT FOUND: [http] Host: [redacted] User: admin Password: [redacted] [
SUCCESS]
root@kali:~#
```

fig.7: Using dictionary word to discover the password

The brute-force attack uncovered a password for the admin user. These credentials were leverage to successfully gain unauthorized access to the protected portion of the system. Human factor can be linked to the successful break into the security of the system because the system allowed several attempts of logins. The system should have put a mechanism in place that locks users out of the system after two or three attempts of logins.

4.2 Surveys

The survey investigated respondents' tendency to:

- Click on links from unverified senders
- Install programs as requested by an unknown person
- Give away username and password
- Using weak or strong password

The email could only be delivered to 36 respondents out of 43. 7 recipient email addresses were unreachable. Out of the 36, only 28 responded. Hence, the total number of participants in the survey is considered to be 28 representing 65.11% response rates.

When probed with the question "Have you ever responded to an online request to provide your account or profile details? 21 (75%) said Yes, whilst 7 (25%) said No.

When quizzed on how they formulate their passwords, the responses given were as shown by fig.8.

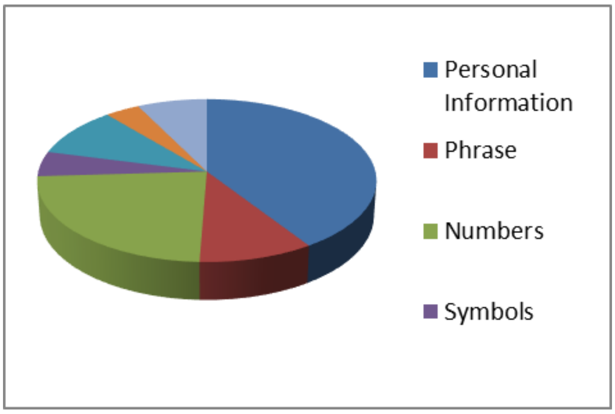


fig.8: Characters used by respondents to generate passwords

The study revealed majority of the respondents use personal information for their password.

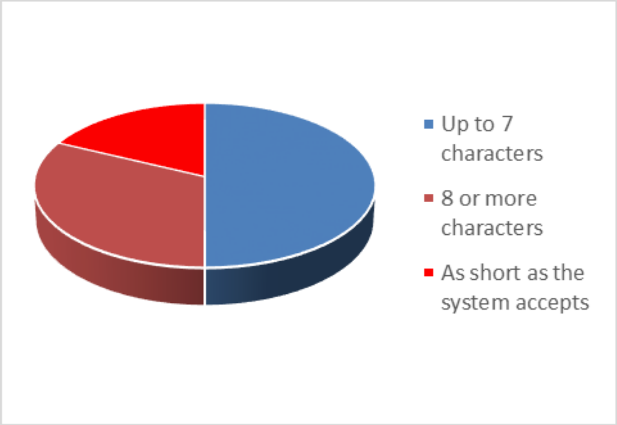


fig.9: Length of generated passwords

Fig.9 shows majority of the respondents use up to seven characters for their passwords.

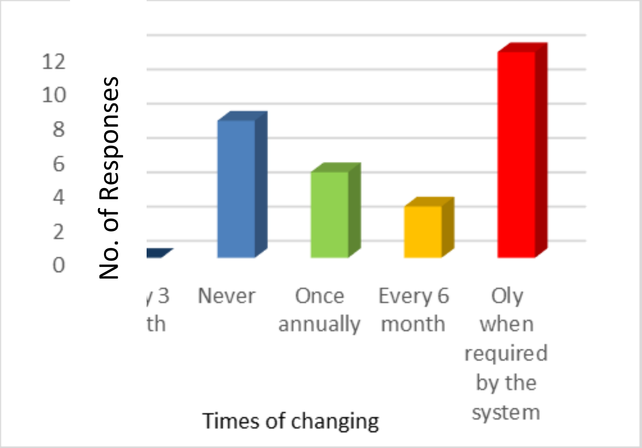


fig.10: Rate at which respondents change their passwords

The study also revealed a number of the respondents never changed their passwords and a considerable number also change their passwords only when a system requires them to do so (fig.10).

Table 2: Responses on logging off unattended computers

Variable	Yes	%	No	%	Total
When leaving work premises	11	39.28%	17	60.71%	28/100%
When attending office meeting	9	32.14%	19	67.85%	28/100%
When using the wash room	5	17.85%	23	82.14%	28/100%
When closing from work	25	89.28%	3	10.71%	28/100%

As demonstrated by table 2, respondents do not log off their unattended computers and this is one of the human actions that can put information at risk. The repercussion of this attitude is that one can have access to these computers at the detriment of the main user and the data and information contained in the computers will be insecure.

Table 3: Other responses from the survey

Variables	Yes	No	Total
Preventing others from watching when typing	19 (67.85%)	9 (32.14%)	28 (100%)

password			
Opening email or attachment From unrecognized address	18 (64.28%)	10 (35.71%)	28 (100%)
Sharing username or password with someone else	7 (25%)	21 (75%)	28 (100%)
Entering credentials on website whose address Does not start with "https"	17 (60.71%)	11 (39.28%)	28 (100%)
Installing updates from unverifiable sources	16 (57.14%)	12 (42.85%)	28 (100%)

Table 3 shows that respondents exhibit certain behavior that put data at risk.

5. FINDINGS

The following are human factor vulnerabilities that emerged during the survey and experiments. These vulnerabilities include acts performed without intent or malicious purpose by an authorized user (respondents).

Clicking on links from unverified senders - The study shows that quite a number of the participants (49.52%) would followed a link that requested them to change their credentials while 42.85% of the respondents would follow a link that requested them to download updates. Clicking on links from unverified sources can lead to security breach. It is one of the ways employed by phishing attackers and social engineers to persuade another person to give them the information that they want. This is very effective as it can utilize strategies that bypass computer technology.

5.1 Lack of strong password and inappropriate password and login/logout procedures

The study found out that quite a number of the respondents engage in practices that could compromise their passwords. It was established that 46.73 % of the respondents change their passwords only when the system requires them to do so and 31.52 % never changed their password. On password strength, it was found out that 35.86 % of the respondents use up to seven characters to generate their password. Their password entropy was calculated which showed that their overall password strength was weak. The usage of a weak password, writing down and sharing of passwords with others, and reusing the same password on different systems are some of the bad practices that respondents involved in. Passwords are to protect data from access from unauthorized individuals both internally and externally. If the password is compromised, the security of the system is at stake.

5.2 Leaving computers unattended

The study shows unattended computers poses significant threat to data other threats do. A significant number of unauthorized accesses occur when someone sits down at another user's computer, facilitating access to sensitive data and email messages. The study revealed that majority of the respondents leave computers unattended.

5.3 Database misconfiguration

During the SQL injection attack an sql query was injected into the system which was able to communicate with it. This normally arises when the database is not configured properly especially when validating user-supplied data and construction of SQL statements such that user-supplied data cannot influence the logic of the statement.

5.4 Lack of mechanism to lock users after several login attempts

The system seems to have a weak lock out mechanism or none at all. This was apparent during the experiment when several passwords were gathered through brute force attack and used on the system. Several log in attempts were made with the passwords. Account lockout mechanisms are used to mitigate brute force password guessing attacks. Accounts are typically locked after 3 to 5 unsuccessful login attempts and can only be unlocked after a predetermined period of time, via a self-service unlock mechanism, or intervention by an administrator.

5.5 Lack of well-established personal security policy and inconsistency in privacy settings

The study revealed that lack of consistence in privacy settings is one of the human factors that put data and information at risk. Email was found to be one of the routes attackers use to access a network since breaking the security perimeter is much harder today. When users use the corporate network to send and receive emails they are putting the network and data at risk. As users have access both to the internal network and the Internet, their desktop computers are usually less hardened than other systems.

5.6 Unauthorized application use

Unauthorized applications used by users in corporate networks can compromise security of these networks. The unauthorized applications are mostly downloaded from untrusted web sites. Using unauthorized applications on business networks can place sensitive corporate data and employees' personal information at risk. The study revealed that email applications are the most commonly used unauthorized application, followed by social media.

5.7 Insider threat

Sometimes the problem is not that users ignore security threat but the users are the threats themselves. The study revealed that if employees are unhappy with their jobs, disgruntled with their manager, or feeling vindictive for any reason, they can become insider threats who deliberately damage or leak data.

6. CONCLUSIONS

The study results shows that although technology and processes represent foundational pieces of information security framework, technology alone was not enough to keep an organization secure from data breaches. A third component is needed to complete the picture: people. People can either be the weakest or the strongest link in the security chain. Therefore, there is the need to bring IT and human security together under a true information security management system. The increasing reliance on technological components of information security makes securing information system increasingly challenging. Most problems occurring while using IT and information systems occurred from humans, so humans are important factors that affect information securities effectiveness. Security is not solely a technical problem therefore people and organizations need to understand is also human factor issues which need adequate attention in order to achieve an effective information security management.

Based on the findings of the study, it is recommended that for the human factor in information security to be managed effectively, the following should be taken into consideration.

- Security awareness: Security awareness, training and education are some of the most effective countermeasures against the human factor threats to information security.
- A strong password should be enforced. Functionalities that prevents a user from setting a password that does not meet certain criteria should be enforced.
- Organizations should use "timeouts" for all PCs to ensure that users are automatically logged out or that PCs are locked, to minimize the risk of insider attacks.
- Organizations should institutionalize standard codes for secure conduct in business Information security policies, which must be an integral part to an organization's code of business conduct and need to be read, understood, and followed.
- For information security threats to be curbed, organizations must adopt a holistic security framework, incorporating the human factor vulnerability to it. Based on the findings of this research, it is recommended that the following security framework should be adopted:

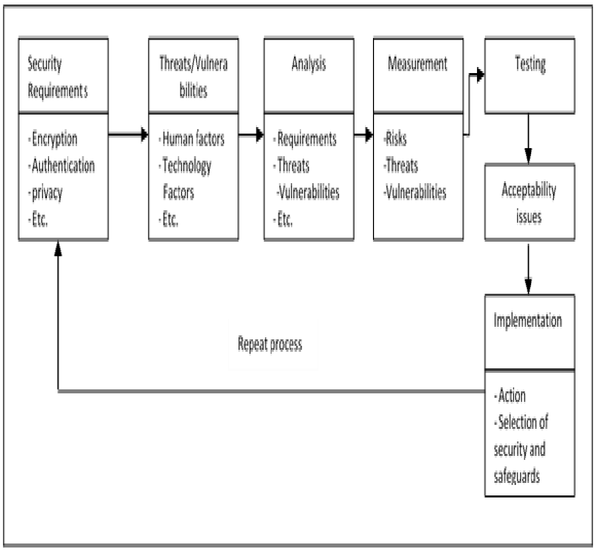


Fig. 11: A holistic framework for information security

7. REFERENCES

[1] Kruger, H.A. and Kearney, W.D. (2006). A prototype for assessing information security awareness. *Computers and Security, 25*, 289-296

[2] James, A. K., Barton P. M., Eduardo, C. and Elisa, H. (2009) "First principles vulnerability assessment," (http://research.cs.wisc.edu/mist/VA.pdf), (accessed 2014 February 21)

[3] Philip S. A., Robert H. A., Richard M., and Michael S. (2003)The vulnerability assessment and mitigation methodology. Santa Monica: RAND.

[4] Moore, H. D. (2007). Exploiting Vulnerabilities. Presentation Slide, Secure Application Development (Secappdev.org)

[5] Lesia, L. C and McCauley-Bell, P. R (2007). The human factors issues in information security: What are they and do they matter? *In Proceedings of the Human Factors and Ergonomics Society*, pages 439–443.

[6] Smith, R. D. (2004) Public servers vulnerability assessment report. Swansea: SANS Institute

[7] Silver, P. (2013) Vulnerability assessment with application security. WA : F5 Networks, Inc.

[8] Anita, G., Kavita, K. and Kirandeep, K. (2013) Vulnerability assessment and penetration testing. *International Journal of Engineering Trends and Technology* 4 (13).

[9] Matsui, M. (1994) Linear cryptanalysis method or DES cipher. *Advances in Cryptology-EUROCRYPT '93*, pp 386-397

[10] Elbaz, L. and Bar-El, H. (2000). Strength assessment of encryption algorithms. Tokyo: Discretix Technologies Ltd.

[11] Bogdanov, A., Khovratovich, D., and Rechbereger, C. (2011) Biclique Cryptanalysis of the full AES. http://research.microsoft.com/en-us/projects/cryptanalysis/aesbc.pdf

[12] Shulman, A. (2006). Top ten database security threats. Foster City, CA: Imperva Inc.

[13] Kashefi, I., Kassiri, M., and Shahidinijad, A. (2013) A survey of on security issues in firewall: a new approach for classifying fire wall vulnerabilieties. *Internationla Journal of Engineering Researh and Applications (IJERA)* 3 (2). pp. 585-591

[14] Stoneburner, G., Goguen, A., and Feringa, A. (2002). Risk Management Guide for Information Technology Systems – Recommendation of the National Instituteof Standard and Technology (Special Publications).National Institute of Standard and Technology (NIST).

[15] OWASP Organization. (2013). "The Open Web Applications Security Project," (https://www.owasp.org/index.php/Category), (accessed on April 3, 2014)

[16] Kaspersky Lab. (2013). "Software vulnerabilities," (http://www.securelist.com/en/threats/vulnerabilities?chapter=35), (accessed on June 20, 2014)