Towards Minizing Human Factors in End-User Information Security

Taurayi Rupere, Mary Muhonde
University of Zimbabwe
Computer Science Department
P.O.Box MP 167
Harare, Zimbabwe
{taurai.rupere, muhondemmm}@gmail.com, trupere@science.uz.ac.zw, muhondem@cut.ac.zw

ABSTRACT: *Today, many hardware and software solutions are available to enhance information security, but there is limited research regarding the human factor in information security. Other researchers have revealed that the application of information security technologies alone does not always result in improved security. Human factors immensely contribute to the security of information systems. This research study therefore addresses the missing link in information security, that is, the end-user working with the information system. In this study, a survey was carried out in two state universities in order to establish the human factors that compromise information security. The major factors established were divided into four categories namely, Social Engineering, Carelessness, Bad Password behavior and Security training. Results showed that Failure to refer to Information Technology (IT) policy (under Social Engineering) and lack of information security training (security training) were the major drivers in compromising information security. Findings from the survey were used to design a model aimed at reducing human factors in information security, called the Human Factors Collaboration Reinforcement model (HFCRM). Since this proposed model is based on collaborative monitoring of security policy violation, an information security policy was consequently designed, so as to facilitate the implementation of the model.*

Keywords: Human Factors in Security, Information Security, Human Error Security Incident, Security Automation, End User

Received: 21 August 2012, Revised 9 October 2012, Accepted 15 October 2012

1. Introduction

Of late, efforts to improve Information Security have been software-centred or hardware-oriented. So far, there have been limited attempts in addressing the security challenges faced by users. Recently, it has been discovered that system users, including their interaction with computers are the greatest loophole in Information Systems security. [10], further highlight that humans are the weakest link in information security. 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 hence there are consequences of bad design and security culture becoming adequate [5].

In the context of this research study, human factors in information security constitutes all those activities erroneously done by system users, that reduce information security, regardless of having all the technical measures e.g. firewalls, Intrusion Detection

Systems and anti-virus being in place. Human factors refers to all those un-intentional activities done by system users that compromise the security of the system such as improper use of passwords, input errors, forgetting to log out of systems, not following procedures, ignorance, and users who give their passwords to co-workers so they can fix some problem when they are out of the office. Such activities are opposed to insider threats which comprise malicious activities meant to attack a system by people entrusted to work with an information system, especially employees. Further, human factors in this context, does not refer to any local or international malicious activities by employees of an organization or unauthorized people intentionally meant to attack a system, sometimes known as "*insider threats*". Examples include illegally changing sections of code, giving IP addresses of the organization's servers to competitors, activities such as phishing, wiretapping, password cracking and identity theft. In this research, focus is on those activities erroneously done by system users, but that result in an information system being left vulnerable to attacks. It is the behaviour of end-users that can expose a system to security threats. In order for an organization to fully implement information system security, it has to address the human side as well; otherwise the security will be incomplete, making the system susceptible to attack.

In addition, some security experts have rejected the fact that automation of procedures can minimize human errors in information systems security. Research has revealed that, information security cannot be completely automated because the majority of human interactions with systems are difficult to automate [7] [6]. The solution lies in some strategy that is not automation.

2. The Significance of Human Factors in Information Systems Security

Since people are the ones who utilize technology, it is imperative that every security system depends on the human factor. The use of technical solutions has so far proved to fall short in handling the human factor, making it necessary to invest in the people using the systems .In addition, Schneier in Nikolakopoulos [12] states that "…*technology cannot solve the security problems and believing so shows a lack of understanding of the problems and technology*". Strategies to assist organizations in identifying their information security shortfalls have been developed by the University of Findlay Centre for Terrorism Preparedness (2003).

2.1Consequences And Copying With Human Errors In Information Security

[3] highlighted that distribution of improper, inaccurate, or confidential information, information system interruption, a compromise in integrity of information, significant economic loss and inability to deliver services are the main consequences of human errors in Information security.

Various strategies of coping with human error have been done on automation by [4] [3] [1] and other solutions as the Standard Operation Procedure (SOP) and the Brown solution to human error [2]. Several approaches can be used to deal with human error, including error avoidance and interception together with recovering from error. Temporal replication with re-execution seems to provide meaningful solutions, but suffers the disadvantage of being resource-hungry and complexity of implementation. Any combination of the approaches yields the best solution to the human error problem but all these strategies seem to be challenging to implement.

2.2 Risk Perception, Information Processing Biases Social Factor Influence

When making behavioural decisions, individuals will often decide based on their estimates of the risks associated with the various options. Many of the risks associated with information security are of a cumulative nature. This means that the likelihood of an event occurring on a given day or at a given time might be extremely small, but over time, this chance increases [5] [13]. However, individuals are generally quite poor at understanding this cumulative risk ((Slovic (2000) in [13], and hence, they might be more likely to take small risks, as they may not appreciate the full consequences. There is also optimism bias where most people do not believe that they are at risk themselves. Instead, such people tend to believe that negative outcomes are far more likely to occur to others (Gray & Ropeik, 2002 in [13]). Optimism bias is particularly prevalent in information security, as evidence suggests that most users tend to believe that hackers would not value the information on their computers, and hence, users are unlikely to see themselves as potential targets [9]. Optimism bias is also particularly prevalent in situations where users expect to see warning signs if they are vulnerable. This could be true of security risks, and evidence suggests that people will often erroneously believe that if they fail to see warning signs, they are exempt from future risks. Essentially, people will underestimate the likelihood that their actions or inactions could result in a security breach.

Group norms can also influence individuals' security behaviour. People generally follow group norms, and therefore if the group considers information security to be an important and serious problem, then it is more likely that the individuals within that

group will value and follow the security policies. Conversely, if risk-taking is accepted within the group, then it is likely that greater risks will be taken. Group norms can also affect individuals' password behavior through trust of peers [9] [13].

3. Methodology

A case study research on two universities was used using the mixed research paradigm. A preliminary survey was carried out at the University of Zimbabwe (UZ) in order to verify the existence of human errors in information security, using the Millennium Library Management System. The "*Millennium Library Management System*" consisted of four modules namely the Circulation sub-system, Reserve, Acquisitions and Cataloguing subsystems. It operates in the main library and other six sub-libraries of the same institute. Another preliminary survey was also carried out at Chinhoyi University of Technology (CUT) that uses the Eagle Integrated System for specifically the database subsystem. Respondents who provided information about the daily operation of the Millennium main library system were chosen using the census. Random sampling was used to select three groups of respondents. The ***first*** one is the group of students who used the University of Zimbabwe library. The variety of students from different faculties using the library, served as a measure against sampling bias. ***Second*** is the group of students from the Computer Science department (University of Zimbabwe). This group of respondents was specifically chosen to determine whether they exhibited the same or different human errors as their counterparts whose computer competency is likely to be lower. ***Third*** is the group of mixed students (i.e. students from various faculties, including Engineering, Business, Hospitality, and Agriculture) from CUT.

The Observation schedule was used to observe security habits of the UZ main library staff, who work on the circulation desk. It was designed to collect data on items such as leaving a logged on computer unattended, referring to written down passwords and allowing a colleague to use one's logged on computer. Data was gathered from observations made during the processes of issuing out books, returning borrowed books, paying of fines and registration of new library patrons.

The research also used questionnaires which were issued to Library end users, database users from CUT and UZ faculty of science students who used an e-learning platform called Towards Student Integrated multimedia E-learning (TSIME). They solicited information regarding their password behaviour, rate of IT skills, whether they received IT training and how far they shared a colleague's logged on computer. UZ faculty of science students responded using their experience in interacting with (TSIME). On the other hand UZ Library end-users based their responses on their experience with the Millennium Library Management System. CUT Database users used their experience of the Eagle Database system to respond to the questionnaire.

4. Data Presentation, Analysis and Discussion of Results

The samples were composed of 160 participants as follows:

- 40 UZ Library end users (any student from UZ is a library end user not considering the science students)
- 40 CUT students (mixed programs)
- 40 UZ science students
- 10 UZ Library Circulation desk staff
- 30 CUT Database users

The sample had an overall return rate of 86% for the questionnaires.

The information systems studied were *The Millennium Library Management* system, *The TSIME e-learning system* (both from UZ) and the *Eagle database system* (CUT). The human errors prevalent on the *Millennium Library Management* system were leaving a logged on computer unattended to, Social engineering (impersonification), failure to follow procedures and carelessness. The human errors prevalent from the database end users who use the *Eagle database system* at CUT were that student marks can be erroneously entered and that a student is assigned an incorrect decision e.g. discontinue instead of proceed carrying a certain course(s) as well as .

4.1 Quantitative Data Amalysis

Data was collected from questionnaires and analysed using PASW v16.0. Results from the data analysis were used to formulate the model for human factors in end-user information security. The analysis was done in terms of descriptive statistics, cross tabs and one-way ANOVA test.

4.1.1 Descriptive statistics

All frequencies were summarized in the table below.

	Password behavior (%)						Social Eng. (%)	Carelessness (%)			IT Security Training %	
Response	Share password s)	Forget password(s)	Write down	Choose good pasword	Change password frequently	Use same password	Open interesting email subject	Leave my logged on comp unattended to	Ignore warnings from browser	Let someone use my logged computer	Receive IT Training	Refer to IT policy
Never	21	32.6	37.0	13.0	19.6	7.2	6.5	5.8	10.9	6.5	*56.5*	*34.1*
Rarely	27.5	25.4	18.8	28.3	34.8	16.7	13.8	24.6	15.2	10.9	*18.8*	*34.1*
Sometimes	*28.3*	36.2	*36.2*	30.4	31.2	29.0	*38.4*	*39.1*	37.7	41.3	16.7	16.7
Regularly	*23.2*	5.1	8.0	18.8	10.1	32.6	*37.0*	*27.5*	31.9	37.7	*4.3*	*6.5*
Always	0.0	0.7	0.0	9.4	4.3	14.5	4.3	2.9	4.3	3.6	*3.6*	*6.7*
Total	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%

Table 1. Frequencies of data collected

From Table 1 above, it can be seen that there is only one parameter under *Social Engineering,* this is because the parameter *Open interesting email subject* was the only one which was common for all groups of respondents. The other parameters under Social Engineering were *I give patrons permission to access library facilities without thoroughly checking their IDs* and for Library staff *I provide my username and password over the telephone to technicians for the purposes of fixing faults* for Database users for example**.** Thus it was going to be impossible to analyse these different parameters in one datasheet.

Results from table1. (in italics and underlined) indicates that the majority of the respondents, never received IT training. 56% never received IT training, 18.8% rarely received IT training. Only 4.3% of respondents regularly received training and only 3.6% always receive IT training. The same applies for referring to IT policy. Close to 70% of the respondents work without referring to the IT policy for guidance. Statistics indicate that 34.1% never refer to policy and another 34.1% rarely referred to policy. Only 6.5% refer to policy and a mere 6.7% always referred to policy. These figures might explain why 28.3% of respondents sometimes shares their passwords and another 23.2% regularly share their passwords. This lack of training in information security could be the reason why 39.1% of respondents sometimes leave their logged on computer s unattended to. In addition 37% regularly open email with an interesting subject even if they are not sure of the sender. All these acts compromise an information system, making it susceptible to unauthorised access or infection by malicious programs such as viruses.

These findings are almost the same as those highlighted by other researchers in the field of human factors in information security.

4.1.2 Cross tabs

The Cross tabs analysis compares responses for different groups of respondents without considering mean values. This test gives the responses for each question according to the different groups in the sample.

	Frequently change password(s)					Open interesting email subject					Allow someone to use my logged on computer				
Response	**1**	**2**	**3**	**4**	**5**	**1**	**2**	**3**	**4**	**5**	**1**	**2**	**3**	**4**	**5**
Never	***10***	**5**	**5**	**3**	**4**	**1**	**0**	**2**	**3**	**3**	**2**	**3**	**2**	**2**	**0**
Rarely	***11***	**14**	**12**	**1**	**10**	**1**	**4**	**1**	**2**	***11***	**2**	**2**	**2**	**5**	**1**
Sometimes	**12**	**10**	**15**	***5***	**3**	***10***	***15***	**22**	**2**	**4**	***17***	***13***	***17***	**1**	**14**
Regularly	**4**	**5**	**2**	***1***	**2**	***22***	***16***	**10**	**1**	***2***	***14***	***17***	***14***	**0**	**5**
Always	**2**	**2**	**1**	**0**	**1**	**5**	**1**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**0**
Total	**39**	**36**	**35**	**8**	**20**	**39**	**36**	**35**	**8**	**20**	**39**	**36**	**35**	**8**	**20**

Key (On Response)

1 - CUT **2 - UZ**

3 - Library end-users **4 - Library staff**

5 - Database users

Table 2. Crosstabs analysis

Table 2 shows one parameter from each variable, that is, under Password behavior, there if "*frequently change passwords*", under Social engineering, there is "*open interesting e-mail subject*" and under Carelessness, there is "*allow someone to use my computer*". Based on Table 2 above, it is evident a greater proportion of CUT respondents never or rarely change their passwords. Reasons could be that enforcement of security at CUT is not strict compared to the other samples. This is in contrast to responses from Library staff whose value of 5/8 respondents showed that they sometimes change their passwords, which is a good information security practice. This good behavior can emanate from the fact that the sample (Library staff) consists of professionals who adhere to take information security principles.

Respondents from UZ and CUT could be susceptible to social engineering as indicated in the table. A total of 31 out of 36 respondents have a high tendency of opening interesting email subject. Same applies to CUT respondents with a total of 32 out of 39 respondents who have this same habit. This could be because both samples are composed of students who are mostly concerned with entertainment and not worried about the impact on security. In contrast the majority of database users rarely open email with interesting mail. Professionalism could be the reason for this recommended information security measure.

In terms of "*allow someone to use my logged on computer*" the three samples composed of university students display the same trend. For CUT, 31 out of 39 respondents do this, for UZ, 30 out of 36 respondents do this while for Library end users 31 out of 35respondents do this. These high numbers could be that students allow others to use their logged on computers in the spirit of friendship or wanting to help a colleague. The other reason could be that since the computers are not enough students usually just share, but forget to log off or simply trust the next user could be a colleague.

4.1.3 One-way ANOVA test

The researcher used one independent variable, namely category of respondents. The analysis below shows the significant value between groups of respondents.

Results in Table 3 shows that the two groups are not significantly different. This means the five groups of respondents have almost the same characteristics as far as each of the stated parameters were concerned, for example; share passwords, receive IT training and rate of IT skills. Consequently, it means the same information security model can be implemented on all groups of respondents. In addition the same Information security policy can be applied on all the groups of respondents.

4.2 Human Factors Collaborative Reinforcement Model

We proposed the Human Factors Collaborative Reinforcement Model (HFCRM). This is a non technical solution rather than automation. Findings from the survey led to the development of this model and are centered on collaborative monitoring against policy violations by making use of reinforcement. The fundamental ideas of the proposed human factors model are adopted from [9]; (**A Reinforcement Model for Collaborative Security**) that emphasized a framework that facilitates collaborative monitoring

Parameter	Sig.
Highest qualification	0.001
Time of using information system	0.000
Rate of IT skills	0.000
Sharing password	0.000
Forget my password(s)	0.000
Write down my password(s)	0.000
Choose good password(s)	0.25
Use same password	0.000
Open email with interesting email subject	0.000
Leave logged on computer unattended to	0.000
Ignore warnings from browser	0.000
Allow someone to use my logged on computer	0.001
Receive IT training	0.000
Refer to IT policy	0.000

Table 3. ANOVA analysis summary

for violations of policy. The model also specifies appropriate reward and punishment depending on the reporting of genuine or false violations by the system users. The idea is to make users be actively involved in various aspects of security such as threat perception and monitoring of policy violations.

4.2.1 Assumptions

The human error model has the following assumptions

i. Every organization has a displayed IT policy that is strictly adhered to.

ii. It is only a reported violation accompanied by confirmation from other users and or a monitoring device that is considered as a true violation.

iii. The model assumes that users are informed in terms of access rights and detection and reporting of policy violations.

4.2.2 Implementation Strategy

• Students use computer facilities (in either the library or computer laboratories) in permanent "*manageable*" groups per semester.

• The Systems Administrator allocates each student a group to work in.

• Each student starts with the same number of point for instance 500

• Reinforcement is awarded to an individual and not group(s) though students use the labs in designated groups.

• Reinforcement is in the form of receiving points upon reporting a true IT policy violation. Fewer points imply less privileges / benefits.

4.2.3 Rewards and Punishment

The higher the points an individual has, the more the privileges / benefits such as more internet access time, reduced campus residence fees, half price on meals from university canteen. The justification for these forms of rewards and punishment is that the research was carried out on two local universities and therefore this choice of reinforcement appeared most attractive since most students have challenges in getting enough internet access time, acquiring campus residence and buying food from the university to mention a few. Since there were no differences among all groups of respondents, it made sense to apply the same form of rewards and punishment on all groups.

Punishment is in the form of losing points upon exhibiting evidence of non- adherence to policy (i.e. when you are reported for IT policy violation) and is applied on individuals and not the whole group. This could be in the form of reduced internet access time.

This model appeared to face challenges in the event that some students might offer fellow students bribes which are more valuable compared to benefits being offered.

The model considers a situation whereby subjects (users) have access to shared resources that is governed by (security) policies. The policies may be composed of some access restrictions, such as that a copy operation on a specific file is prohibited. The policies may also expect specific behavior from subjects like a user not sharing her password. It also assumes a set of subjects to be $S = \{s1, s2, \ldots, sn\}$ and infinite ways to violate a security policy leading to a collection of violations, $Vio = \{vio_1, vio_2, \ldots, vio_m\}$

Primary payoff	True violation	False violation
Reported	R_{ij}	$-P_{ij}$
Not reported + Undetected by user	$-CP_j$	#
Detected +Not Reported	$-P'_{ij}$	#
Threat reporting	Θ_{ij}	#

Table 4. Primary pay-off table

The **notations** below were adapted from [9]

$\boldsymbol{R_{ij}}$ **:** Reward for player $\boldsymbol{s_i}$ on reporting true primary violation $\boldsymbol{vio_j}$.

$\boldsymbol{-CP_j}$**:** Community price associated with true primary violation $\boldsymbol{vio_j}$

$\boldsymbol{-P'_{ij}}$**:** The punishment for player $\boldsymbol{s_i}$ for not reporting true primary violation $\boldsymbol{vio_j}$.

Θ_{ij}**:** Reward for player $\boldsymbol{s_i}$ on reporting potential violation

$\boldsymbol{P_{ij}}$**:** The payoff for player $\boldsymbol{s_i}$ for false reporting on violation $\boldsymbol{vio_j}$

 # : Undefined value.

However, the rewards and punishment model has challenges associated with. Behaviour based on motivation from rewards has a tendency to cease the moment rewards are eliminated. This makes choice of rewards very difficult. It is also only an attractive reward that is higher than their current socio-economic status that is likely to motivate users to report a policy violation. Thus in order for rewards to be effective, they should meet the user's satisfaction.

4.2.4 Likelihood model for reporting estimation

This parameter enables the researcher to estimate how likely a policy violation is to be reported. This is important since it is not every policy violation that will be detected and reported. It is also important to consider that there could be some hidden benefit for not reporting a policy violation.

4.2.4. 1 Motivation index

Motivation index $\boldsymbol{m_{ij}}$ is a measure for motivating a user to report a policy violation. The motivation index can be decided by considering the factors below:

- The reward a user gains for reporting.
- The punishment for committing secondary violation.
- Other factors that can deter a user from reporting a violation, such as the need to maintain good reputation with friends
- Fear of community price

Similar to [9] Motivation index m_{ij} will be calculated as:

$$m_{ij} = |T_{ij}[1, 2]| + \max\{|T_{ij}[1, 3]|, |T_{ij}[1, 4]|\} - \Omega_j$$

$T_{ij}[1, 2]$ is the reward; a user gains for reporting a genuine violation vio_j.

$T_{ij}[1, 3]$ is the community price suffered by the whole group for failure to report a policy violation.

$T_{ij}[1, 4]$ is the punishment for the secondary violation, that is, the loss s_i would incur in case she does not report the violation but in turn some other subject reports against him for doing so.

Ω_j represents any factor that may hinder one from reporting a violation. Ω is a constant set to 1.

NB: Values for $T_{ij}[1, 2]|$, $T_{ij}[1, 3]$ and $T_{ij}[1, 4]$ are found in Table 8 (Determining actual rewards for violations) in the form [row, column]

Since the model is a collaborative reinforcement model, the type of reward will be used as a means to ensure users report any policy violation. Table: 5 show the classification of policy violations.

Type of violation (P_{vio})	Rank / Sensitivity level (R_{vio})	Device used to confirm occurrence of violation
Social Engineering	**1**	CCTV + person (observable)
-Use somebody's ID		
-Open email with interesting subject		
Password behaviour	**2**	System admin + partly observable
-Forget my password		
-Write down my password		
-Choose good password		
Change password frequently		
Carelessness	**3**	CCTV + person (observable)
-Ignore warnings from a web browser		
-Let other people use my logged on computer		

Table 5. Classification of policy violations

Since this model assumes observability and detectability, the last column in the table above, "*Device used …*" serves to confirm whether a report of a security violation is true or not, thus checking against false reporting. From the table above, it can be noted that type of reward T_{rew} or type of punishment is directly proportional to the rank of violation, R_{vio}. $T_{rew} \propto R_{vio}$ thus, $T_{rew} = k R_{vio}$. Table 8 below is for determining the type of rewards / punishment for each type of policy violation.

Since the model is based on likelihood (chance), we will consider the variables and assumptions below in order to come up with a mathematical expression for the model

• The rate of reporting $rrep_{ij}$ denotes that the subject s_i will report a primary violation vio_j .

• Motivational index for reporting is

$$m_{ij} = |T_{ij}[1, 2]| + \max\{|T_{ij}[1, 3]|, |T_{ij}[1, 4]|\} - \Omega_j$$

4.2.5 Likelihood for reporting a policy violation

The likelihood value l_{ij} will be used as measure to determine whether a user s_i will report or not report a policy violation vio_j.

Rank of violation R_{vio}	Reported R_{ij}	Not reported + Undetected by user - CP_j	Detected + Not Reported - P_{ij}	Threat reporting Θ_{ij}	False reporting-P_{ij}
1	14	-10	-6	5	-5
2	12	-6	-4	4	-4
3	10	-5	-4	3	-3

Table 6. Determining actual rewards for violations

Using policy violation R_{vio} **= 1, that is, Social Engineering,** as an example,

- Calculating m_{ij} first, we get
- m_{ij} $= (| T_{ij}[1, 2]| + \max\{| T_{ij}[1, 3]|, | T_{ij}[1, 4]|\} - \Omega_j)$
  $= (R_{ij} + \max\{- CP_j, - P_{ij}\} - \Omega_j))$
  $= (14 + \max\{-10, - 6\} - 1)$
  $= 14 - 6 - 1$
  $= 7$

Calculating the likelihood for reporting policy violation R_{vio} **= 1,** we get

li_{ij} $= [m_{ij} * R_{ij} - CP_j - P_{ij}] / 100)$ **(expressed as a percentage)**
$= [(7 * 14 - 10 - 6) / 100]$
$= (98 - 16) / 100$
$= 82 / 100$
$= \underline{82\%}$

Using policy violation R_{vio} **= 2, that is, Password behaviour**

- Calculating m_{ij} first, we get
- m_{ij} $= (| T_{ij}[2, 2]| + \max\{| T_{ij}[2, 3]|, | T_{ij}[2, 4]|\} - \Omega_j)$
  $= (R_{ij} + \max\{- CP_j, - P_{ij}\} - \Omega_j)$
  $= (12 + \max\{- 6, -4\} - 1)$
  $= 12 - 4 - 1$
  $= 7$

Calculating likelihood for reporting policy violation R_{vio} **= 2,** we get

l_{ij} $= [m_{ij} * R_{ij} - CP_j - P_{ij}] / 100)$ **(expressed as a percentage)**
$= [(7 * 12 - 6 - 4) / 100]$
$= (84-10) / 100$
$= 74 / 100$
$= \underline{74\%}$

Using policy violation R_{vio} **= 3, that is, Carelessness,** as an example,

- Calculating m_{ij} first, we get
- m_{ij} $= (| T_{ij}[3, 2]| + \max\{| T_{ij}[3, 3]|, | T_{ij}[3, 4]|\} - \Omega_j)$
  $= (R_{ij} + \max\{- CP_j, - P_{ij}\} - \Omega_j))$
  $= (10 + \max\{- 4, - 5\} - 1)$
  $= 10 - 4 - 1$
  $= 5.$

Calculating the probability for reporting policy violation R_{vio} **= 3,** we get

l_{ij} $= [m_{ij} * R_{ij} - CP_j - P_{ij}] / 100)$ **(expressed as a percentage)**
$= [(8* 10 - 4 - 5) / 100]$
$= (80-9) / 100$
$= 71 / 100$
$= \underline{71\%}$

Thus, with regard to Carelessness, the likelihood that s_i will report a policy violation vio_j that she witnessed is 71%. For this action s_i will gain a reward of 10 points. Failure to report this violation will attract a penalty of -4 points on that particular individual i.e. the subject s_i will lose 4 points if user does not report the violation, since it will be detected by some device. In addition failure to report a violation that will be reported by another subject will attract a penalty of -5 on the whole group, that is each individual in the group will lose 5 marks. Thus, in conclusion, a user who violates policy receives double penalty, one that is applied on him as an individual and another that is applied to the whole group. This collaborative reinforcement model works, since groups will work together in closely adhering to policy in order to avoid negative reinforcement (penalty). In addition a user who observes a policy violation is motivated to report of such a case since the reward is quite attractive and the penalty quite deterring.

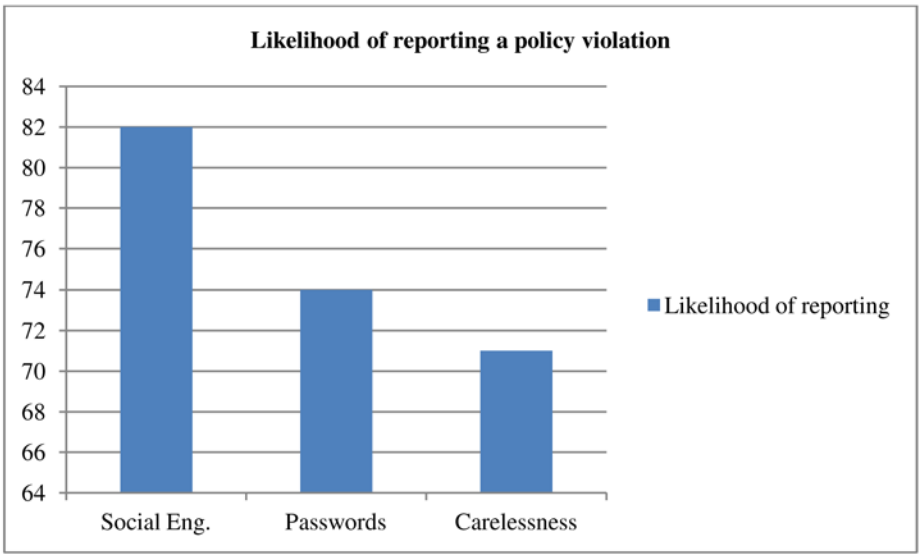

Figure 1. Likelihood of reporting a policy violation

Figure 1 shows that the policy violation whose consequences on security are highest has the highest likelihood of being reported. The policy violation with the least impact, in this case, Carelessness has the least likelihood of being reported.

Conclusions from these socio-psychological studies[9] are:

• New behavior in individuals can emanate from extrinsic rewards

• Due to fear of group punishment, individuals tend to encourage each other to adhere to policy and avoid violations mechanisms

• Punishments can be indirectly used as negative reinforcement so as to foster expected behaviors. However, if negative reinforcement is withdrawn, individuals are at risk of going back to their old habits.

The use of reinforcement to achieve information security is an approach that has been implemented by several researchers. Kabay (2002) in [9]a good understanding of individuals is vital when designing security policies. He also emphasized the importance of rewarding individuals who report violations of security policy.

4.3 Information Security Policy

The human factors model we proposed, **Human Factors Collaborative Reinforcement Security Model** is centered on collaborative monitoring of information security policy; hence an information security policy was designed to facilitate the implementation of this model (see appendix 1). The policy addresses the human factors gathered from the survey and is meant to guide system end-users as they interact with the system. The purpose of this policy is to give users guidelines so human errors in end-user information security for university students and staff can be minimized, see section 1.0 of policy.

Section 3.1 of the policy explicitly states that users should report any form of suspected violation to security policy, such as evidence of leaving a logged on computer unattended to. This is the main focus of the proposed model. The policy also describes the appropriate measures to follow so that information is kept secure. Section 3.2 gives these details in terms of

password behavior, carelessness and social engineering. Section 4.0 is on training users and requires the systems administrator to regularly offer IT security training to system end-users. Section 5.0 states that constant reference must be made to this policy in order to minimize the frequency of policy violations. Finally section 6.0 is on enforcement, that disciplinary measures in the form of negative reinforcement may be implemented on any user found to have violated the security policy.5

5. Conclusion

The scope of this study was specifically; human factors in end-user information security. The general finding was that the five groups of respondents were similar. They all had the same characteristics in terms of password behavior, carelessness, social engineering and IT security training. Findings established that all groups had bad password behavior, they were careless with securing information, rarely receive IT training and they were all at one time victims of social engineering. These human errors were classified into three major categories, namely Carelessness, Social Engineering and Password Behaviour. It was also discovered that the majority of these human errors were as a result of lack of IT security training.

A **Human Factors Collaborative Reinforcement Security Model** was then designed, based on these findings. Since the model is based on collaborative monitoring against policy violation, an Information Security Policy was consequently developed to facilitate the implementation of this model. This policy addresses the various issues covered in the model. The model was also tested theoretically. The model's effectiveness is commendable since the use of rewards is known to reinforce good information security behaviour while the use of punishment (negative reinforcement) is known to deter bad security behaviour.

Findings from this research revealed that even if the best technological solutions to information security were in place, human behavior will somehow contribute to information insecurity.

6. Recommedations & Future Work

Simulations based on the Human factors model will need to be carried out. Furthermore technological solutions need to be pursued with the social solutions. In addition there is need to include more human errors, since this research work only looked at three, which are Social engineering, Password Behaviour and Carelessness.

References

[1] Bean, M. (2004). Human error at the center of IT Security breaches, New Horizons Computer Learning Centers

[2] Brown, A. B. (2004). Coping with Human Error in IT. *Queue,* 2 (8) — ACM Digital Library

[3] Carstens, D. S., McCauley-Bell, P. R., Malone L. C., DeMara, R. F. (2004). Evaluation of the Human Impact of Password Authentication Practices on Information Security, *Informing Science Journal*, 7, 68-85

[4] Edwards, W. K., Shehan, E., Stoll, P. J. (2007). Security Automation Considered Harmful?. North Conway, NH. 85 Fifth Street NW, Atlanta, USA.

[5] Fléchais, I. (2005). Designing Secure and Usable Systems, University College London Gonzales, J. J., Sawicka, A. (2002) A Framework for Human Factors in Information Security, *In*: Proceedings of the WEAS International Conference on Information Security, Rio de Janeiro, Brazil.

[6] Hassell, L., Wiedenbeck, S. (2004). Human Factors and Information Security, Drexel University College of Information Science and Technology

[7] Jones, A., Martin,T. (2010). Making Information Security Acceptable to the User. *International Cyber Resilience conference Security Research Centre Conferences*, Edith Cowan University Perth Western Australia

[8] McIlwraith, A. (2006). Information Security and Employee Behaviour: How to Reduce Risk through Employee Education, Training and Awareness. Aldershot, UK: Gower Publishing Limited.

[9] Misra, J., Saha , I. (2009). A Reinforcement Model for Collaboration Security and its Formal Analysis, NSPW'09 ACM, United Kingdom.

[10] Mitnick, K.D., Simon, W.L. (2002). The Art of Deception: Controlling the Human Element of Security. Indianapolis, ID: Wiley Publishing, Inc.

[11] Nikolakopoulos, T. (2009) Evaluating the Human Factor in Information Security. Oslo University College

[12] Parsons, K. McCormac, A. Butavicius, M., Ferguson, L.(2010). Human Factors and Information Security: Individual, Culture and Security Environment DSTO-TR-2484, Command, Control, Communications and Intelligence Division, *Defence Science and Technology Organization*, Edinburgh, Australia.

APPENDIX 1

HUMAN FACTORS INFORMATION SECURITY POLICY

VERSION 1.0

1.0 Purpose
The purpose of this policy is to provide guidance for users in order to minimize human error in information security for university students and staff.

2.0 Scope
This policy applies to students and staff in local universities.

3.0 Policy
Appropriate measures must be taken when using computers to ensure the confidentiality, integrity and availability of personal and sensitive information.

3.1 Users are to report suspected computer security violations, such as evidence of "*ignoring warnings from browser*", "*leaving a logged on computer unattended to*" and other forms of compromise, to the proper IT personnel, immediately.

3.2 Appropriate measures include:
3.2.1 Restricting physical access to workstations to only authorized persons
3.2.2 Complying with all applicable password policies and procedures that is,
3.2.3 Passwords will be established and maintained to provide system security.
3.2.3.1 Passwords must be a minimum of eight characters, utilizing a combination of capital letters, lower case letters, and numbers.
3.2.3.2 Passwords will be changed periodically as part of system security.
3.2.3.3 Passwords should never be written down, stored on-line, or allowed to be used by other persons.
3.2.4 Ensuring that monitors are positioned away from public view. If necessary, install privacy screen filters or other physical barriers to public viewing.
3.2.5 Never ignoring warnings from a browser, these may alert you of potential infection
3.2.6 Never opening email from an unfamiliar sender, most of such email is malicious
3.2.7 Ensuring workstations are logged off after a user is through
3.2.8 Never allowing someone (including your friends) to use your logged on computer

4.0 User awareness and training
The IT Security Officer is to implement a university-wide information security program, including policy, procedure and best practice development, user education and training

5.0 Reference to IT policy
Constant reference must be made to this policy in order to minimize the frequency of policy violations.

6.0 Enforcement
Any user found to have violated this policy may be subject to disciplinary in the form of negative reinforcement.

7.0 Definitions

7.1 Violations in this context generally refer to
• Any action that is contrary to what is laid down in policy e.g. letting somebody use another user1s logged on computer
• Any action / human factor that makes a computer‘s system vulnerable to attack
• Any action that scans, sniffs or logs systems or networks without authorization from the IT Security Office;

7.2 Negative reinforcement is any form of disciplinary measure intended to minimize human error

8.0 Revision History
This is version 1.0 and will be revised in due course.