TOWARDS MINIMIZING HUMAN FACTORS IN END-USER INFORMATION SECURITY

By

MUHONDE MARY

Reg Num: R096927P

A thesis submitted in partial fulfilment of the requirements for the degree of

Master of Science in Computer Science

SUPERVISOR: Mr. T. Rupere

Department of Computer Science
Faculty of Science
UNIVERSITY OF ZIMBABWE

May 2011

ABSTRACT

Today there are many hardware and software solutions to enhance information security, but there is limited research regarding the human factor in information security. Research has 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. Failure to refer to Information Technology (IT) policy and lack of information security training were 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. 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.

ACKNOWLEDGEMENTS

I have learnt a lot during this research study from the birth of the idea until it was finally handed in. It was a challenging and interesting task. Many people contributed towards the success of this research project and their input is greatly appreciated. I am very thankful for my supervisor Mr. T. Rupere for his guidance which exhibited a high level of academic expertise. Many thanks to students and staff of University of Zimbabwe and Chinhoyi University from who samples were drawn. My sincere gratitude goes to Mrs. D. Musiyandaka for her unwavering encouragement and support. Thank you a million times.

CONTENTS

TABLES

FIGURES

APPENDICES

CHAPTER 1: INTRODUCTION

1.1 BACKGROUND TO THE STUDY

Of late, efforts to improve Information Security have been software-centred or hardware-oriented. So far, there have been limited attempts in addressing the people who use the computers. Recently, it has been discovered that system users, including their interaction with computers are the greatest loophole in Information Systems security. To further highlight that humans are the weakest link in information security, Mitnick and Simon (2002:12) explain that

> A company may have purchased the best security technologies that money can buy, trained their people so well that they lock up all their secrets before going home at night, and hired building guards from the best security firm in the business. The company is still totally vulnerable... The human factor is truly security's weakest link.

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. According to Fléchais (2005:7) findings from early research suggest that:

> Security mechanisms are too difficult to use, and that most users do not maliciously break security policies but do so as a consequence of bad design, complex requirements or an inadequate security culture.

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. In other words, the human factor 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. Examples of insider threats are intentional disclosure of IP addresses, identity theft and phishing to mention a few. Further, human factors in this context, does not refer to any malicious activities by employees of an organization intentionally meant to attack a system, sometimes known as “insider threats”. Examples of the latter include illegally changing sections of code and giving IP addresses of the organization’s servers to competitors. Human factors issue is opposed to intentional malicious activities by unauthorized people who are usually outside a particular organization. Examples of such activities include 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.

The recommended approach to system security is a mixture of technology in conjunction with the people using the computers since computer operation is a combination of these two.
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. The implication is that efforts should be channeled towards getting to understand the reasons behind end-users over-riding rules. This is the reason why this research project sought to address the challenge of human factors in end-user information security by use of non-automated solutions.

Hassel and Wiedenbeck (2004:1) further allude to the inappropriateness of automation by that:

> It seems that there is an implicit assumption that enough technology will solve the problem – that if we can only remove humans from the equation, we can automate our way to information systems security. While technology is certainly important, the assumption that it will solve the security problem has yet to be justified…

Gonzales & Sawicka (2002:6) also highlight the inadequacy of automation as a solution to human errors in end-user information security, that

> … human factors in security systems are treated as "obvious" marginalities or considered unmanageable, hoping that technological solutions should automate security. Such approach is futile: The literature on human error emphasizes the "ironies of automation": Trivial tasks can be technologically addressed, leaving more demanding tasks to people

This is a clear indication that automation is far away from the solution to the human error problem in information security. The solution lies in some strategy that is not automation.

The researcher worked with the Millennium Library Management System at the University of Zimbabwe (UZ), in Harare as well as the Eagle Integrated System at the Chinhoyi University of Technology (CUT), in Chinhoyi in order to ascertain the existence of human errors in information systems

1.2 STATEMENT OF THE PROBLEM

Information systems can be vulnerable to attack even if the best technical security measures such as firewall, IDS and antivirus are in place. The reason is that information security is not limited to the technical aspect but however incorporates the system users. Therefore this research addresses the missing link in information security, that is, the end-user working on

the system. In short, the research is about human errors in regards to accidental exposure of information.

1.3 SUB-PROBLEMS

- What are the causes of human error in end-user information systems security?
- Is lack of training the major cause?
- What strategies can be implemented to minimize human error in end-user information systems security?

1.4 AIM

This research aims to design a model to minimize human factors in information security.

A model works towards portraying the real situation on the ground. Hassel & Wiedenbeck (2004:4) agree that "Creating models is an important part of Information Technology (IT). It permits us to abstract from reality and determine what is important to the domain in which we are working."

1.5 OBJECTIVES

The research was guided by the following objectives:

1) To analyse the causes of human errors among information system users.
2) To assess the relationships among human factors in information systems.
3) To design a model for minimizing human errors in information systems.
4) To test the designed model theoretically

1.6 ASSUMPTIONS

This research study is based on the following assumptions:

- Human error is inevitable

- Non-technical solutions can be implemented to reduce human errors in end-user information security

1.7 DELINEATION OF THE STUDY

The research focused on minimizing human error in end-user information security. Thus, technical human errors such as configuration errors were not part of this study. The study did not cover malicious activities performed by people outside an organization such as ID theft, wire tapping and hacking. The research study did not cover deliberate activities performed by people inside an organisation such as changing program code, commonly known as ***"insider threats".*** Only two organizations were investigated for this research study due to time constraints. Since human factors in information systems security are so numerous, it was impossible to study all of them in one research. Therefore this research study covered the following human factors: carelessness, improper use of passwords, not following procedures, carelessness and social engineering.

1.8 LIMITATIONS

The limitations of the research were

- It was difficult to get permission to work with other university subsystems such as Payroll, Student Records and Accounts
- Findings from these could have increased the scope of the research.
- Such variety could have added the validity of the research

In an attempt to overcome these limitations, the researcher studied a combination of information systems, such as the Millennium Library System at UZ and the Eagle Database system CUT.

1.9 SIGNIFICANCE OF THE STUDY

The "inevitability of human error" is the justification for this research study. Brown (2004:2) alludes that "Regardless of the source, however, psychology tells us that mental-model mismatches, and thus human error, are inevitable in the rapidly changing environments characteristic of IT systems". In addition, Risvold (2010:1)

> Editorials like Schultz (2004 &2005) have asked for more research on the human factor regarding the information security. Researchers are encouraged to publish more papers in this area. So this shows the need for this study to contribute to the research community.

This implies human error in information systems security, has not been thoroughly studied, so far. This call for papers is based on the fact that the majority of research in information security is failing to incorporate the people using the systems. This was part of the researcher's motivation to pursue this study.

To further justify the significance of this research study, Zhang, Reithel & Li (2009:330) propose that;

> While organizations have applied many security technologies, e.g. anti-virus software, firewalls, access control, intrusion detection techniques, encrypted login, biometric techniques, etc. to protect their critical information, humans remain the weakest link in the information security environment and associated security processes.

In addition, the human factor appears to be the major threat in information security, since the majority of all technical flaws (security) are caused by humans. Ironically the human being appears to be the most neglected element of information systems security. There is need therefore, to strike a balance between the human factors in security and the technical issues of information security.

On their own, computers cannot be used to fully administer information security practices. Hence it is important to critically analyse how human errors in system security can be minimized.

(Hassell & Wiedenbeck 2004:1) concur that

> Despite the fact that non-technical computer users are the weak link in information systems security, the study of human factors on security compliance has remained largely ignored in Information Security (INFOSec) and Information Assurance literature.

This research study is intended to benefit universities and other large organizations where human factors are a threat to information security. It is also assumed that the model and IT policy suggested by this research study will provide solutions to the numerous challenges posed by human error in information systems security.

1.10 CHALLENGES

The greatest hurdle encountered by the researcher was finding an organisation to work with. Other researchers in this area of study also faced the similar challenges. Fléchais (2005:13) concurs that

> ...empirical security research is difficult and hampered by the fact that few organisations or projects are willing to open their systems up to scrutiny – generally citing security concerns as the reason.

This explains why the researcher only used systems from institutions of higher learning and not those from private companies or other organizations.

1.11 ETHICAL CONSIDERATIONS

A section on informed consent on the very beginning of each questionnaire served the purpose of informing the survey participants of ethical practices. This section included the purpose of the research and assurance of confidentiality of data collected.

1.12 CONCLUSION

This chapter briefly described the background to the study, and gave the aim of this research project, which is to design a model to minimize human errors in end-user information security. The motivation for this research study emanated from the fact that there appears to be limited research that addresses the human side of information security. The stated objectives and research questions were the vehicle for achieving this aim. The researcher also justified the significance of this research study and defined the scope of the research study. The next chapter will review literature in line with human factors in information systems security.

1.13 DEFINITION OF KEY TERMS

Human factors in security

It refers to human errors while interacting with an information system e.g. forgetting passwords.

Information security

Information security refers to the protection of the confidentiality, integrity and access to information. “Information security involves making information accessible to those who need the information, while maintaining integrity and confidentiality.” (Carstens et al 2004:2)

Human error security incident

"It is defined as any human error-related event that compromises information security as defined by … confidentiality, integrity and availability. (Carstens et al 2004:2)

Security automation

"It is any system or technology that effectively removes the security decision process from the user." Edwards etal (2007:2)

User

Any person who uses Information Technology (IT) equipment such as a computer.

CHAPTER 2: LITERATURE REVIEW

2.1 INTRODUCTION

Chapter two is a discussion of what other researchers and authorities have done and found out with regards to human factors in end-user information security. The section concentrates on the models and solutions implemented elsewhere in an attempt to reduce to a minimum the human factors in information security.

2.2 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 (2009:7) states that "…technology cannot solve the security problems and believing so shows a lack of understanding of the problems and technology."

According to Carstens et al (2004:2)

> Earlier research identified the presence of human error risks to the security of information systems (Wood & Banks 1993, Courtney as cited in NIST, 1992). A survey conducted by these authors, identified password issues as the second most likely human error risk factor to impact an information system. The significance of this is enhanced when realizing that passwords are the primary source of user authentication for the majority of personal and private information systems.

Based on the above research findings, the University of Findlay Centre for Terrorism Preparedness (2003) developed a strategy to assist organizations in identifying their information security shortfalls.

2.3 CONSEQUENCES OF HUMAN ERRORS IN INFORMATION SECURITY

According to Carstens et al (2004:4) below are some of the consequences of human errors in information security.

- distribution of improper, inaccurate, or confidential information
- information system interruption
- a compromise in integrity of information
- significant economic loss
- inability to deliver services

According to Carstens et al (2004:4)

> There were many key human error problems also identified such as a lack of inadequate training, lack of awareness regarding the importance of data and the associated risks for insecure behaviour, time pressures (stress and overload on users and system administrators), lack of responsibility/accountability felt by users (for example, disabling a virus protection program because it slows down their computer),…

The research by Carstens et al (2004) established strategies for combating the consequences of human error. These include automating some system functions and training users.

2.4 COPING WITH HUMAN ERROR

Different authors proposed various strategies of coping with human error.

2.4.1 Automation

This refers to the use of information technologies to make decisions on behalf of the user.

According to Carstens et al (2004:4)

> An example of increasing automated functions within a computer would be to have a pop up menu appear on an employee's computer screen giving notification that it is time to change their password.

Another form of automation is the use of embedded "coping skills" within an IT system. This gives the impression that automation will solve most of these human error problems, but recent research provided an opposite opinion all together. Recent literature emphasizes the ironies of automation.

Automation is not the ultimate solution

Since many security failures are attributed to humans, then it could be wise to use techniques that involve minimum human intervention. The focus of automating systems is on making systems that "just work" without human intervention. The major strength of automation is that it is more predictable and accurate that its' human counterparts. An example of automation is the "old" anti-virus program that required system users to decide on whether to clean, quarantine or ignore a detected virus. With the modern versions of anti-virus programs, the viruses are automatically cleaned upon detection. It is important to remember that, its not every end-user system function that can be automated.

According to Edwards et al (2007) the following are guidelines for automating security

- Automation solution should be reversible.
- Users should perceive the actions of a system
- The system should be able to recover from any automation errors
- Automation is suitable for systems that are less than perfect

- Automation is highly commendable in cases where it is absolutely impossible for the system user to do the work. An example is where packets are checked by intrusion prevention systems at a speed that exceeds that of a human systems administrator.

So far, literature on human error suggests that automation is ironical. According to (Gonzalez & Sawicka 2002:6) "trivial tasks can be technologically addressed, leaving more demanding tasks to people." This implies automation is not going to be the solution to the human error problem, but something else.

One option is implementing embedded "coping skills" into an IT system. Training is one sure way of fighting against human error in information security. According to (Bean 2004), results of a study conducted by Computing Technology Industry Association (CompTIA) established that a company is 20 percent less likely to be a victim of security attacks, only if can train a quarter of its IT staff.

2.4.2 Standard Operating Procedure (SOP)

Challenges resulting from not following procedures can be minimized by introducing Standard Operating Procedures (SOP). A standard operating procedure refers to a series of stages followed by people in order to complete a task. The strength of SOP is that they eliminate the differences in work performance that are as a result of different steps followed by users to complete the same process.

2.4.3 Trust model

Another solution to human factors in information security is the "Trust model".

Schneier (2004:285) defines it as:

> The trust model represents how an organization determines who to trust with its assets or pieces of its assets."

> Using the Trust model, only certain people are given permission to certain rooms, open certain cabinet files, or …sign cheques. In extreme circumstances, additional security comes from segregation of duties, for example, the person who has the physical possession of the cheques does not have the machine that embosses the signatures. .. Someone might be trusted to make changes in the personnel records but not the engineering specifications.

This segregation of duties can also be used to minimise human error. The assumption is that one person can only make an error only in the area they are designated to be working on.

2.5 BROWN'S SOLUTIONS TO HUMAN ERROR

Brown (2004) proposes four categories for coping with human error. namely, *Error prevention, Temporal replication, Spatial replication, and Temporal replication with re-execution.*

The first category (error prevention) is a pre-cautionary approach that tries to stop human errors from taking place. The remaining three categories are targeted at errors that have already happened. However, a combination of any of these approaches usually yields systems that are resistant to human error.

2.5.1 Error Avoidance

Error avoidance can be achieved by ensuring that system users do not commit errors (error avoidance) as well as strategies to prevent the errors from penetrating the system (error interception). In order to accomplish error avoidance, it is should be possible for the errors to be anticipated prior to them occurring. Traditionally error avoidance can be achieved by use of continuous training in collaboration with good user interface design.

2.5.2 Spatial Replication

This strategy deals with errors that have already happened. The backbone of this strategy is the creation of several copies of a system. Each replica of the system has its own duplicates of the system's important information, which is synchronized. The drawback of this approach is that it is most suitable in cases when only the minority of the replicas is affected by human error. Consequently errors affecting the greater proportion of the replicas are accepted as the correct state of system.

2.5.3 Temporal Replication

Temporal replications differ from spatial replication in that it keeps more than one copies of system, with each one having its own replica of state of the system. The major difference is that replicas used in temporal replication are not synchronized. Temporal replication makes use of a current copy that represents the actual state of the system and several replicas (historical) will represent the situation of different states in the system's history. Requests to the system together with human operator input are only effected on the current replica. Figure 1 overleaf illustrates the difference between spatial and temporal replication.

A major drawback is that this approach works well for cases whereby human errors affect the system state. A combination of temporal replication and re-execution, known as "replication with re-execution" can be used to provide protection against operational errors that affect the state of the system.

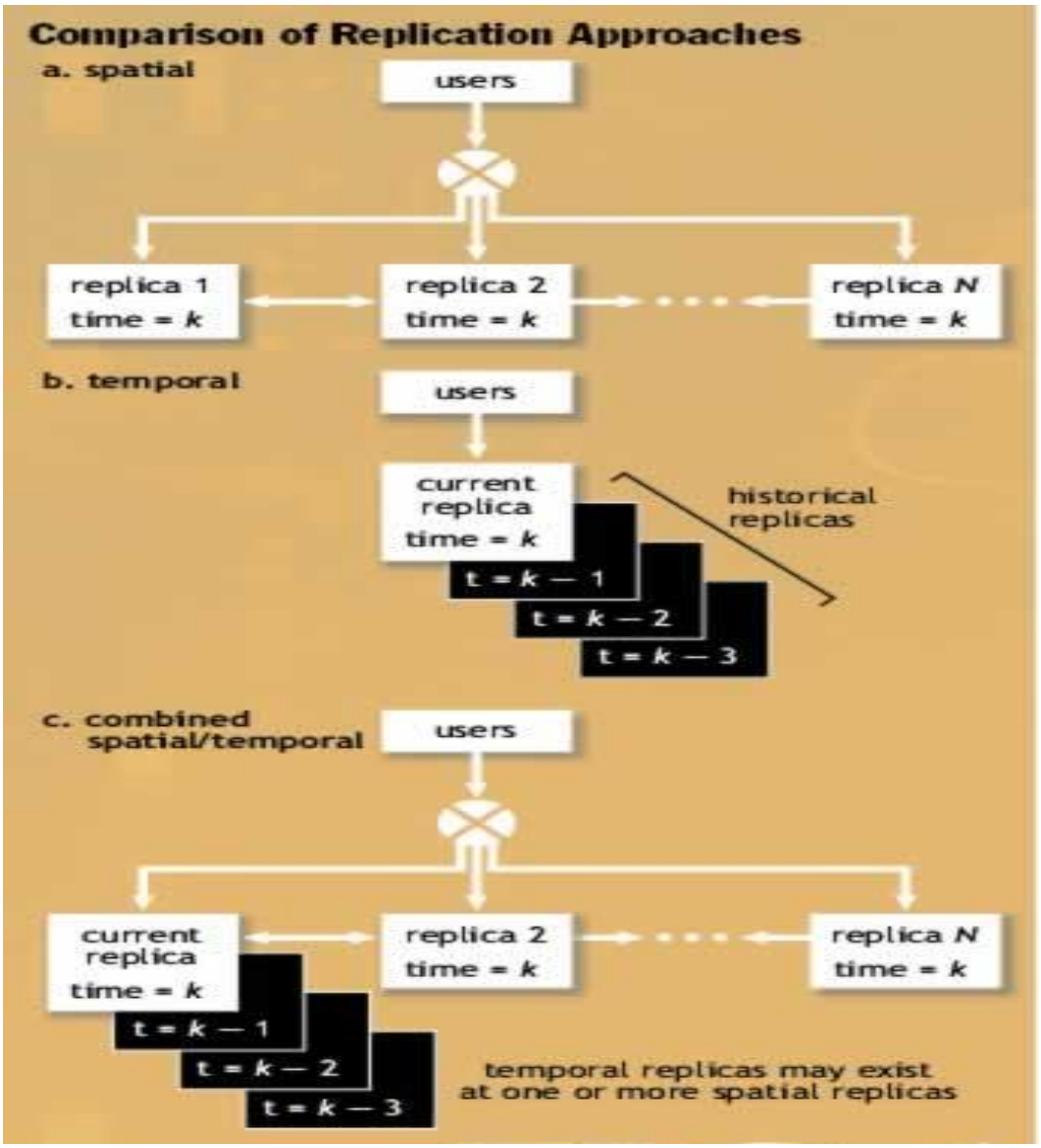

Figure 1: Comparison of replication approaches
(Source: Brown 2004:5)

2.5.4 Temporal replication with re-execution

This approach uses a separate history log that contains a series of all changes from the time the last temporal replica was made. In the event that a human error occurs, the system solves it by switching to the old replica and then re-executes the transactions in the log, so that the replica becomes up to date. This is shown in Figure 2, overleaf.

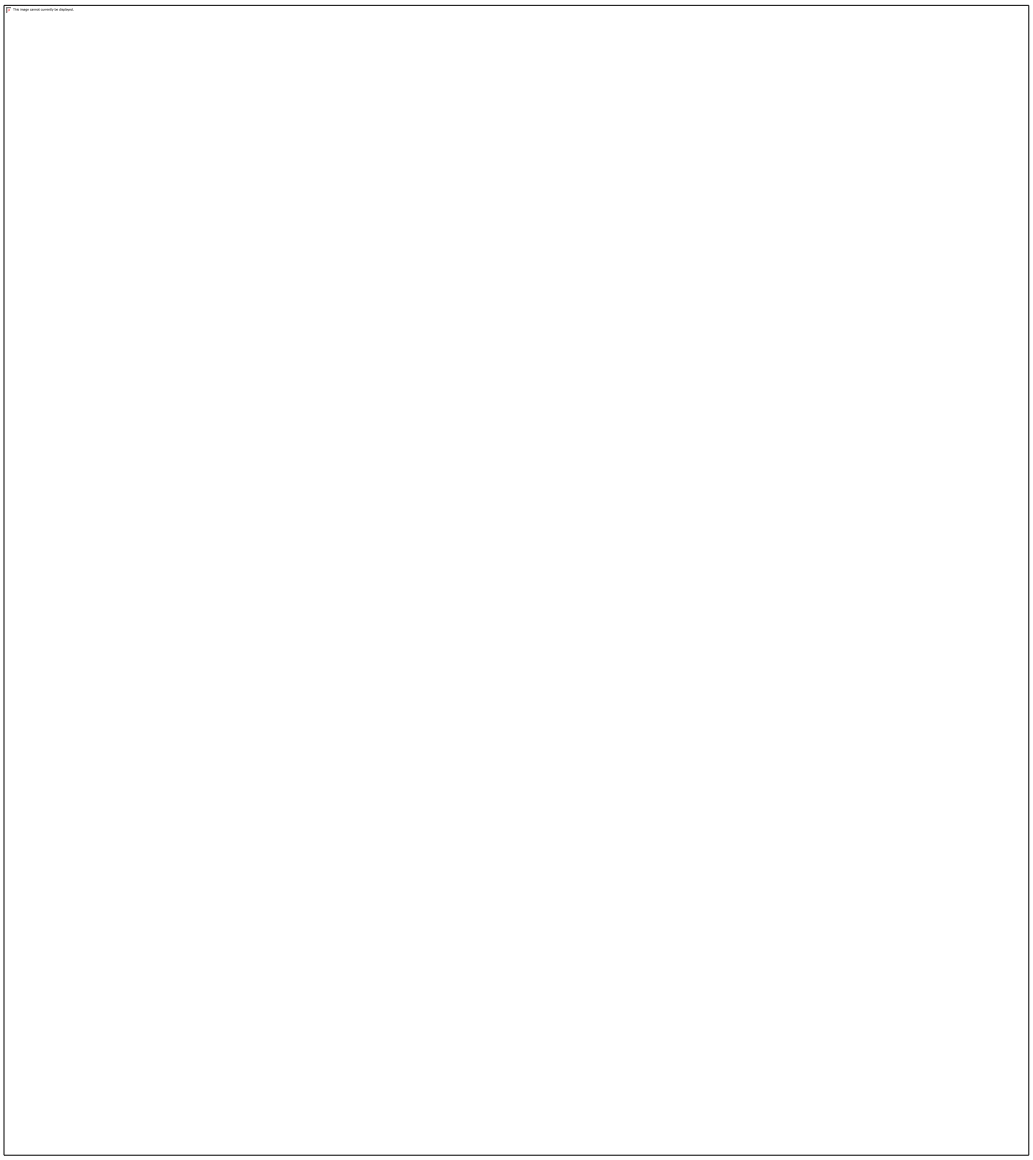

Figure 2: Temporal replication with re-execution
(Source: Brown 2004:6)

One drawback is that it is the most difficult error-recovery strategy to implement. Great care has to be taken when creating and re-executing the history log so that the causal ordering of events is achieved. If the system is heavily-loaded re-execution can be expensive in terms of time and storage requirements.

2.6 GUIDELINES FOR COPING WITH HUMAN ERROR

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 discussed earlier on yields the best solution to the human error problem.

Error avoidance is the first line of defense. This can be accomplished by automation, a sound user interface design as well as continuous training of users. Suppose errors are committed, interception can be achieved by buffering those transactions or executing them on a virtual replica of the system, before their effects are implemented on the live replica. In the event that prevention strategies fail, then those approaches based on replication will have to be implemented.

The unfortunate situation is that all these strategies seem to be challenging to implement. Because human error is inevitable, efforts should be made to develop more effective approaches to solve this problem. According to Bean (2004), continuous training of all computer users appears to be the long-term solution to this human error problem.

A major challenge at the moment is the lack of set standards for measuring information security in an organisation. Bean (2004:2) highlights that

> Currently, there is no clear definition of an information assurance professional and there is a desperate need for common standards and certification moving forward. The first fundamental change that needs to take place is to move security from being seen as a technology issue to be seen as a behavioural one that has profound consequences for both the reputation of the organization with its customers and prospective customers and for its financial health.

Bean (2004:3) further recommends that

> There needs to be shared responsibility at senior management level for the creation, dissemination and enforcing of a robust security policy that every employee has a copy of and familiar with the parts that pertain particularly to them. With proper training, people can become the single most important factor in an organization's security defence strategy.

Thus the issue of ensuring secure systems ceases to be the responsibility of the computer users alone, but an issue of concern to every member of the organization.

2.7 RISK PERCEPTION AND INFORMATION PROCESSING BIASES

When making behavioural decisions, individuals will often decide based on their estimates of the risks associated with the various options.

2.7.1 Optimism Bias

Optimism bias refers to the fact that 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 Parsons etal (2010)). 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 (McIlwraith, 2006).

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. The optimism bias can result in an increase in security related risks, as individuals may underestimate the risk, and may therefore fail to keep up to date with security patches, and may fail to follow other security procedures (Mitnick & Simon, 2005 in Parsons etal (2010)). Essentially, people will underestimate the likelihood that their actions or inactions could result in a security breach.

2.7.2 Cumulative Risk

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 (Fischhoff, 2002 in Parsons etal (2010)). For example, if someone chooses an insecure password, the chance that this non-adherence to procedure will be exploited might be very small on a particular day, but over the weeks and months, this chance builds up.

It is also important to consider the cumulative risk posed by different people all taking small risks. For instance, the risk associated with one person failing to follow one procedure may not be high, but if a number of individuals create different vulnerabilities, the cumulative risk might be substantial. However, individuals are generally quite poor at understanding this cumulative risk ((Slovic (2000) in Parsons etal (2010)), and hence, they might be more likely to take small risks, as they may not appreciate the full consequences.

2.8 THE INFLUENCE OF SOCIAL FACTORS

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 behaviour. For instance, according to (McIlwraith (2006) in Parsons etal (2010)), password sharing can be considered to be a sign of trust in a colleague, and therefore, refusing to share a password could be seen as a sign that people do not trust their colleagues. If such norms are present within an organization, then a great deal of education will be necessary to change these behaviours.

2.9 MODELING IN COMPUTER SCIENCE

Modeling refers to the simplification of a concept so that it can be easily-studied. Modeling is the preliminary step of abstraction. A model exhibits the important features of a phenomenon. The theoretical background enables us to identify the relevant features. A simple model entails that we use symbolic language to describe a phenomenon. This then makes it easy to anticipate measurable effects of given variations in a system.

2.10 MODELS FOR HUMAN FACTORS IN END-USER INFORMATION SECURITY

The fact that research on human factors in information systems security is still in its infancy, explains why this section discusses only three models. Following are models that have been proposed by other experts in this area of study.

2.10.1 Framework for Human Factors in Information Security

Gonzalez and Sawicka (2002) approached the problem from a social sciences point of view. The aim of their research was trying to better understand the role of human factors in information systems security. The researchers based their model on ***The behavioral regulation theory*** which is best explained in terms of **i**nstrumental conditioning. Instrumental conditioning refers to learning through consequences. Of importance in this model is the idea of a subject's or a user's compliance to security practices as well as risk perception. The main idea of instrumental conditioning is that a system user's behavior that produces positive results is reinforced while behaviour that produces negative effects is weakened. These researchers used an imaginary case to demonstrate that designing good security policies can be enhanced by use of system dynamics. Overleaf is a description of the central aspects of the model, which is best explained using the causal structure diagram.

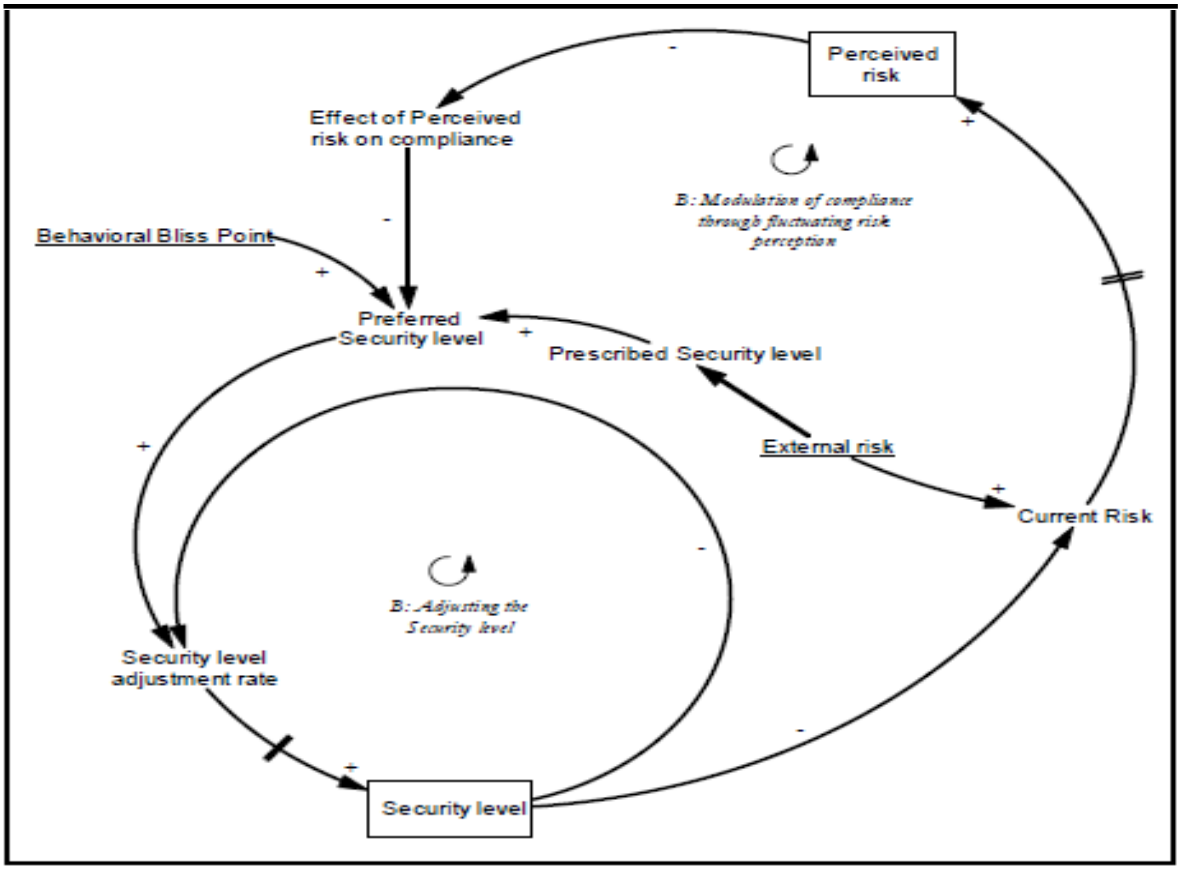

Figure 3: Causal loop diagram of security dynamics under the influence of risk perception
(Source: Gonzalez and Sawicka (2002:3))

The model proposed by Gonzalez and Sawicka (2002) is centered on ccompliance with IT policy in conjunction with risk perception. They believed that factors such throughput pressure can affect compliance with security measures. According to these researchers compliance to security policies can be achieved through alertness to risk. This means that if one perceives a security attack, she tends to be more careful and tries to adhere to the IT policy. Inversely if one is not perceiving a security attack, one tends to relax and rarely or does not refer to the IT policy. Their model revealed that a user tends to comply with policy particularly when one's anticipation of risk is relatively high. A user's anticipation of risk is noted to be "updated" by security attacks. The occurrence of security accidents increases one's perception to risk. On the other hand, risk perception decreases with absence of security attacks. Although the occurrence of security accidents has a positive effect on compliance, it

is not the best way of ensuring compliance to policy. Other methods should be used to ensure appropriate level of risk perception is maintained.

From the researcher's point of view, this model has several weaknesses. Firstly, the model uses an imaginary case of an individual (Kim) to illustrate its major concepts, whereas in proper research samples (more than one person) are used. Secondly, it is not clear on how the individual was selected e.g. computer literacy level. Thirdly, the model cannot be mathematically proven, it is too theoretical. It is because of these drawbacks in the model by Gonzales & Sawicka (2002) that the researcher deemed it necessary to develop a new model.

2.10.2 A Generic Model of Human Factor Management

This model was proposed by Trcˇek & Kandus (2003) and the central issues in their model are real risks (RR) and perceived risks (PR). The rate of adaptation, that is, change in perceived risk (CPR), which is accumulated as PR, is proportional to discrepancy between real risk and perceived risk, and inversely proportional to real adjustment time (RAT). It follows that PR is a level, driven by CPR.

Two components are used to reflect that RAT depends on certain circumstances. The first one is ***initial*** one and the second one is a ***contribution from experiences***. For instance, consider a long period characterized by absence of accidents. In the event that an accident occurs, expectations are grounded on previous experiences, meaning that users perceive this accident more as a rare occasion. On the other hand, if one experiences attacks consecutively for a long period of time, one will expect a similar attack in the near future.

To emphasize this fact explicitly, the model includes length of normal operation (LNO) variable. Change in perceived risk is also driven by the level of security policy - the higher

this level, the faster the rate of adaptation. Of course, security policy level (SPL) is changed with a delay, as RR is always ahead of reported risk and the same holds true for discrepancy and internal accidents frequency (IAF). The basic idea of the model is that one should not violate breaches, if real risk is properly perceived, that is on time and in terms of number of threats. The model is presented in Figure 4 below.

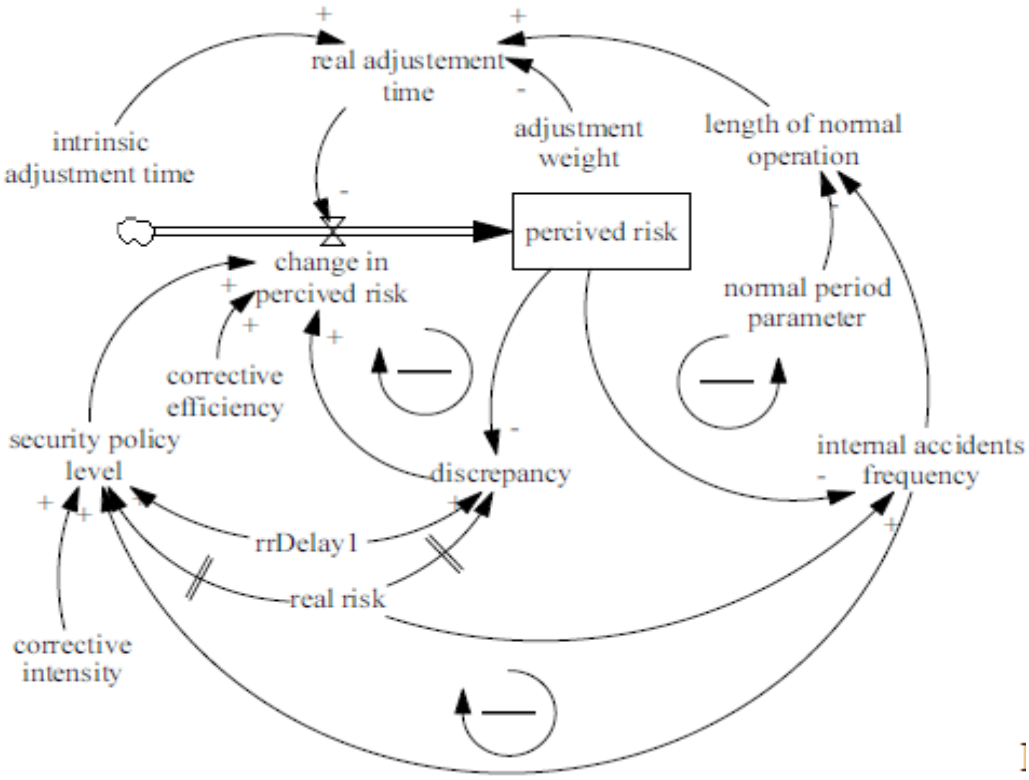

Figure 4: **A generic model of human factor management for security policy**
(Source: Trcˇek & Kandus (2003:3))

A contribution from experiences is used to reflect the fact that RAT is determined by certain circumstances. For instance if one is a victim of serial attacks, for a long time, he / she will be anticipating the next attack. Consequently such a person becomes more careful and is cautious with the security measures. On the other hand, if one experiences long periods of time without being attacked, one tends to relax and may not practice any security strategies. Change in perceived risk is also driven by the level of security policy - the higher this level, the faster the rate of adaptation.

The system consists of three balancing loops. The loop of perceived risk (PR, RPR, discrepancy, CPR) is represented by the upper left loop. Similarly, the trust of employees in the system, in the light of experienced normal operation, which influences R.A.T., is captured by trust loop in the upper right corner. Finally, at the bottom, is the adjustment loop which models adjustment of anticipated risk which is a result of the management via SPL.

Just like the previous model, "A framework for human factors in information security" by Gonzalez and Sawicka (2002), this model is silent on a number of issues that are of importance. First, the model is too narrative and lacks scientific soundness. Second, it does not use specific variables of information security such as social engineering, insider attacks etc. Third, the model cannot be mathematically proven, it is too theoretical. These shortfalls motivated the researcher to develop a new model

2.10.3 Collaborative Reinforcement Model

Saha and Misra (2009) proposed a reinforcement framework that enables collective monitoring of policy breaches by system users. They defined a "rewards" model to implement the framework. The model specifies appropriate reward, punishment, as well as community price depending on the reporting of a genuine or false violation. Non-reporting of detected violations, together with prior reporting of vulnerabilities by the users was also considered.
The idea is to make users responsible for information security by actively involving them in different aspects of security such as threat perception and the monitoring of policy violations.
An example of how the Reinforcement model for collaborative security works is,

> … a malicious user making destabilizing changes in a code base could be better monitored and reported for doing so by the associated team members, who have probably better knowledge of it or can better detect it than the centrally administered monitoring mechanisms.
> Saha and Misra (2009:1).

The human error model suggested by this research paper has the following assumptions

i) A violation is assumed to exhibit observable impact in order to eliminate cases of false reports falsity

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

iii) A violation is said to be detected only when it is reported to have occurred. The detection is done by other users or monitoring equipment. That means, suppose a violation occurs but is not reported by any of the witnesses (or captured by the monitoring device), it would be regarded as not detected.

iv) Users have accesses to security policies and are able to detect and report real violations

A number of social psychology studies based on the role of extrinsic motivation in influencing individual and group behaviors formed the justification for this model. Below are conclusions from some of these studies:

- Group punishment contributes towards prolonged community behaviors. Individuals in groups have a tendency to influence others so that they evade collective punishments that is caused by other group members.
- New (community) behaviors in individuals can be fueled by extrinsic rewards
- Punishments, in addition to rewards, are also used as negative reinforcement strategies for individuals, who attempt to escape punishments. Individuals however tend to go back to their old habits if they do not internalize expected behaviours.
- Sociological studies centred on *locus of control* show that individuals are better motivated when they perceive more control over their environment. Generally, collaborative security allows users to contribute towards policy design. The ability to monitor their violations gives them a sense of control over the assets and policies they are using as compared to situations where they have limited or no contribution to these aspects.

The use of reinforcement to achieve information security is an approach that has been implemented by several researchers. In addition to Saha and Misra (2009) who proposed ***A Reinforcement Model for Collaborative Security***, Kabay (2002) in Saha and Misra (2009) also highlighted that when designing security policies, it is crucial to apply socio-psychological understanding of individual and group behavior. He emphasized the need for the creation of policies and environments that reward employees for reporting security violations.

- **The Payoff Matrix Model**

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, $Vio = \{vio1, vio2, \ldots, viom\}$

Table 1: The payoff matrix table for the reporting behaviour of primary violations
(Source: Saha & Misra (2009:4))

Primary Payoffs	True Violations	False Violations
Reported	$R_{ij}(t)$	$-P_{ij}(t)$
Non Reported + Undetected	$-CP_j(t)$	#
Detected + Not Reported	$-P`_{ij}(t)$	#
Threat Reporting	$\Theta_{ij}(t)$	#

Table 1 above shows the variables for a primary security policy violation. In the context of this model, a primary violation is a case whereby a user s_i detects a policy violation and reports it. On the other hand a secondary violation is whereby a user s_i detects a policy

violation and does not report it, instead, some other subject s_n (who also witnessed the same violation) reports against her for doing so.

Table 2: The payoff matrix table for the reporting behaviour of secondary violations (Source: Saha & Misra (2009:4))

Secondary Payoffs	True Violations	False Violations
Reported	$r_{ij}(t)$	$- p_{ij}(t)$
Non Reported + Undetected	0	#
Detected + Not Reported	$-p`_{ij}(t)$	#
Threat Reporting	$\partial_{ij}(t)$	#

Notations: All the entries in the tables (Table 1 and table 2) are dependent on time. This means the value of each is determined by the subject's previous events. *t* is the variable for time. Further, (Saha & Misra 2009:3) define the list of variables below

Rij(*t*): Reward for player *si* on reporting true primary violation *vioj* .
CPj (*t*): (absolute value) Community price associated with true primary violation *vioj* .
P_ ij(*t*): (absolute value) The payoff for player *si* for not reporting true primary violation *vioj* .
Θ*ij*(*t*): Reward for player *si* on reporting potential violation (or threat) on *vioj* .
Pij(*t*): (absolute value) The payoff for player *si* for false reporting on violation *vioj* .
rij(*t*): Reward for player *si* on reporting true secondary violation on *vioj* .
cpj(*t*): (absolute value) Community price associated with true secondary violation on *vioj* .
p_ij(*t*): (absolute value) The payoff for player *si* for not reporting true secondary violation on *vioj* .
∂ij(*t*): Reward for player *si* on reporting potential secondary violation on *vioj* .
pij(*t*): (absolute value) The payoff for player *si* for false reporting of a secondary violation on *vioj* .
#: Undefined value.

For ease of implementation, Saha and Misra (2009:8) introduced a "***Motivation index".*** This is a control variable 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

According to Saha and Misra (2009:8), the motivational index ($\boldsymbol{m_{ij}}$) is determined by the formula

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

T_{ij} [1 1] is the reward *si* would gain for reporting true violation vio_j

T_{ij} [2,1] is the corresponding community price if none of the subjects detecting the violation report

T_{ij}[3,1] is the punishment for the secondary violation, that is, the loss s_i would have in case she does not report the violation but in turn some other subject reports against him for doing so.

Ω_j indicates the effect of the factors that collectively can act as a deterrent for reporting the violation.

In addition, Saha and Misra (2009:8) proposed the probability of violation vio_j being reported as

$$1 - \prod_{s_l \in S_j} (1\text{-P}l_j)$$

For each player $s_l \in S_j$, there exists a subset of users who notice *sl* detecting *vioj*. This is denoted by $Y_l = \{sl_1, sl_2 \ldots sl_r\} \subseteq S_j$.

In summary, the main idea of this model is that users work collaboratively to ensure that information security policy is adhered to by every member in the group. Certain rewards and punishments are then awarded to individuals, depending on their actions. The probability of a policy violation being reported is then calculated using the given formula.

2.10.3.1 Challenges of the Collaborative Reinforcement Model

The drawbacks of this Reinforcement model are:

- If a member of a group has strong personal relationships with other group members, one may not report a violation, in attempt to protect good reputation and for fear of isolation.
- Determining the actual is a major challenge since individuals vary in their choices of preferred rewards. One may be motivated by special recognition while another may be motivated money.
- The need for establishing adequate regulations and controls aimed at preserving the privacy of group members.

In addition the model does not specify the exact security issues that the study covered. Furthermore, the model is silent on the kind (e.g. computer literacy levels) of subjects who participated in the study.

Regardless of its drawbacks, the *Collaborative Reinforcement model*, appeared to be more applicable in the scenario for this research project. As a result the *Human factors model* proposed by this research project is heavily dependent on some aspects of the *Collaborative Reinforcement Model*.

2.11 CONCLUSION

This chapter discussed a paradigm shift of IT security where information security is regarded more as a behavioural issue and not only as a purely technological issue. According to the researches done so far, information security has been focused on improving hardware and software solutions. Interestingly, of late, emphasis is on the people who use computers.

Statistical evidence reveal that 80 percent of known information security breaches are as a result of human error caused by failure to follow security procedures and lack of proper training.

Models aimed at minimizing human factors in information security include;
A Framework for Human Factors in Information Security by Gonzalez & Sawicka (2002), ***A Generic Model of Human Factor Management*** proposed by Trcˇek & Kandus (2003) and ***A Collaborative Reinforcement model*** by Saha & Misra (2009).

Human errors have adverse effects on information systems security. Some consequences of human factors in information security are a distribution of improper, information system interruption, inaccuracy and economic loss.

The next chapter focuses on the methodology used. This includes the research design, choice of sample and data collection method the researcher used.

CHAPTER 3: METHODOLOGY

3.1 INTRODUCTION

This chapter gives a detailed procedure used to carry out this research. Since the research is on human factors in information security, there was need to determine the human factors prevalent in end-user information security. To accomplish this; a survey was conducted at University of Zimbabwe (UZ) and Chinhoyi University of Technology (CUT). The data collected was analysed using a statistical package, PASW v 16.0. Consequently, results from this analysis were used to design a model that aims at reducing the number of human factors in end-user information security. Finally, the "Human Factors Information Security Policy" was designed to facilitate the implementation of the model, since the latter is based on security policy violation.

3.2 PRELIMINARY SURVEY

A preliminary survey was carried out at the UZ in order to verify the existence of human errors in information security, using the Millennium Library Management System.

The "Millennium Library Management System which consists of four modules namely the Circulation sub-system, Reserve, Acquisitions and Cataloguing subsystems. The Millennium Library Management System operates in the main library, and four other sub-libraries namely; Veterinary Library, Education Library, Law Library, Map Library, Institute of Development Studies Library and Medical School Library, situated at Parirenyatwa Hospital.

- **Circulation sub-system**

  Consists of Borrowing section, Returns and Reserve sections which are operated by different people at different positions.

- **Reserve and Fines**

  This section services those people who would want to borrow books from the "Reserve" section as well as pay fines for either overdue accounts of improper behaviour in library.

- **Acquisition**

  This sub-system is for buying (acquiring) books for the university library and all its sub-branches. This section liases with Faculty Librarians, Deans and Lecturers who then submit lists of books to purchase. This seems not to be busy as was evidenced by two members of staff designated for the job

- **Cataloguing**

  The main area of focus here is verifying that the barcode attached on books in the Acquisition section is very correct. Just like the Acquisition section, this section is not so busy that two members of staff are sufficient for the job.

Another preliminary survey was also carried out at CUT using the Eagle Integrated System, specifically the database subsystem. The researcher was granted limited access to the database, with authorities citing security concerns. The subsystem used for this preliminary survey was that used by departmental secretaries for capturing students' exam marks.

3.3 RESEARCH PARADIGM

This research study belongs to the Information Systems category which is a branch of Computer Science; therefore the mixed research approach was used. Mixed methodology is simply a methodology that is an integration of qualitative and quantitative research methods. According to Jones (2004) in Moon and Moon (2004), qualitative data is essentially descriptive data from unstructured interviews or observations. Contrarily, quantitative data is basically data in numerical form, often derived from questionnaires or structured interviews.

Mixed research is simply research in which quantitative and qualitative techniques are used in parallel in the same study. Mixed research is considered third among other major research paradigms. The main strength of this approach is that qualitative methods and quantitative methods are compatible, that is, they can both be used in a single research study.

Below is a diagram illustrating the integrated research design. The steps for the quantitative method are sequential while those for the qualitative part are evolving. During the research process the researcher followed all the steps of the integrated research approach.

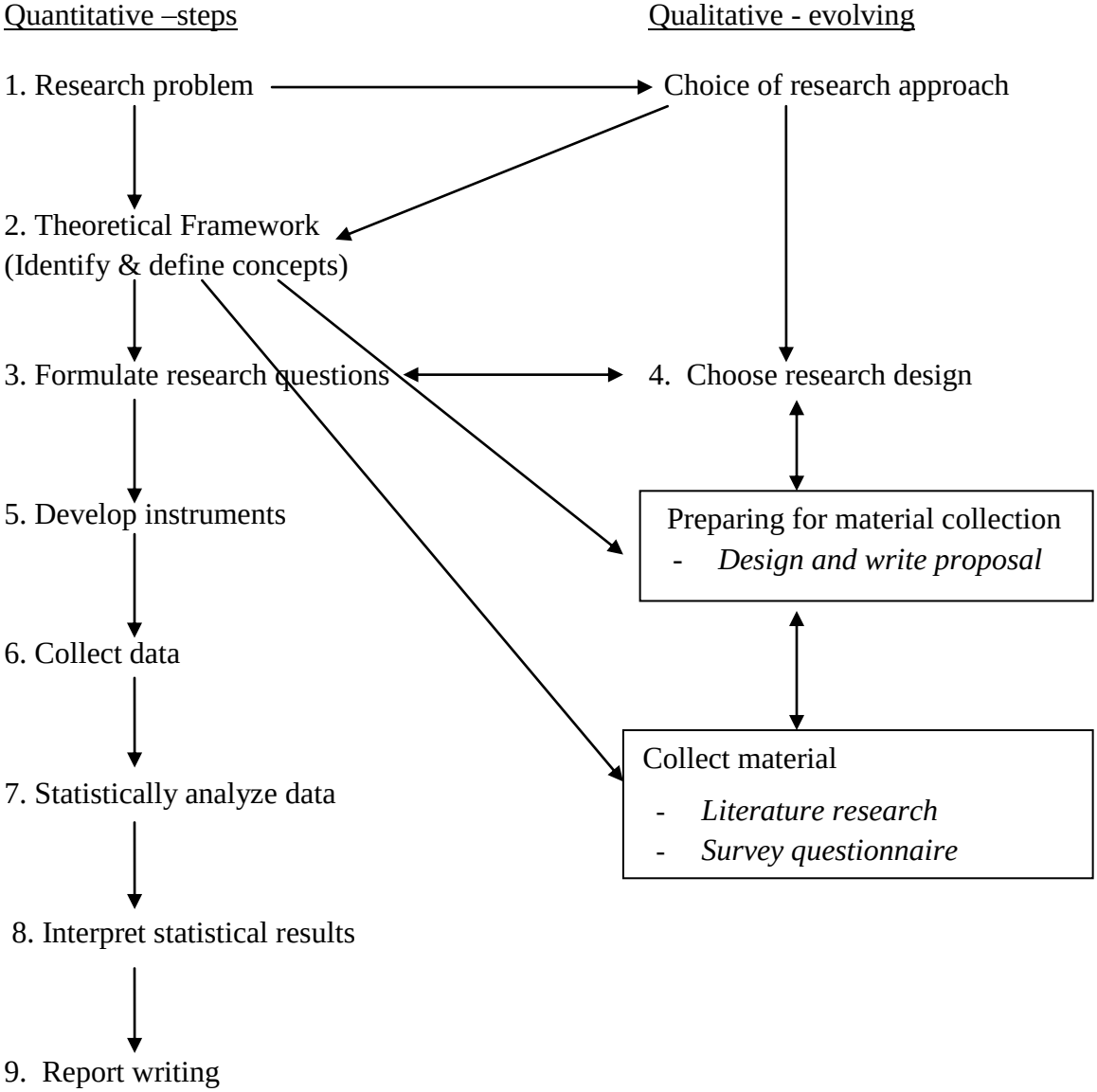

Figure 5: Integrated research design (adapted from Du Plessis (2004)**)**

3.4 RESEARCH METHODOLOGY

The case study research methodology was used. This methodology was used since it is the one recommended for research that is being conducted in an area where limited research already exists. Human factors in information security is not an area that is widely or commonly studied, thus the researcher found the case study methodology as the most appropriate one to use.

3.4.1 Case study methodology

A case study is characterized by an in-depth study of a single case, situation or place. Case studies typically, focus on a couple of selected issues that are crucial to the case under investigation. The main characteristic of a case study is that we learn it enables an in-depth examination of a particular case. Unfortunately, the findings cannot be generalized. Since human factors in information security are greatly influenced by organizational culture, case study methodology was the most suitable to use following the fact that organizational culture is not universal, but unique to an organization. The purpose of this research is not worried with generalizations, but is interested in a particular case, hence the research was carried out only at UZ and CUT. This is the justification for using of the case study methodology for this research study.

3.4.2 Strengths of a case study

- It is possible to develop new hypotheses for later testing. This is a major strength of case studies. In this context, the researcher developed a model for combating human factors in information security, which can be tested by other researcher in future research work.

- A case study can provide detailed descriptions of cases. Following this advantage, the research provided end-user security behaviours for users in two institutions of higher learning.
- It provides a vast amounts detail. Researchers can be immensely informed using one case. Such detail is indicative of numerous future research questions necessary for follow up studies, in the future. The findings from this research study provide an opportunity for further researcher as a follow up to some of the issues that emanated from the study.

3.4.3 Drawbacks of a case study

A major shortfall of the case study methodology is that it is only dependent on a specific case making it incapable to provide generalizations of conclusions to a wider population**.** To minimize this weakness, the researcher worked with samples from two institutions (i.e. CUT and UZ) instead of carrying out the study in a single organization, as the phrase "case study" implies.

3.5 SAMPLING

Sampling refers to the selection of a suitable group that is representative of a population, so that characteristics of the whole population can be determined. Conclusions about populations can be drawn from samples. Direct observations of a sample by a researcher can be used in inferential statistics to determine the characteristics of a population.

Reasons for sampling

The major reasons for sampling over a census are that; it is cheap, it is less time-consuming and that it makes it feasible to study large populations.

Problems with sampling

Sampling error and sampling bias are the major challenges of sampling. A sample is expected to represent the population from which it was drawn. Unfortunately, it is not guaranteed that a sample will always perfectly represent the population from which it comes.

- **Sampling bias**

Sampling bias is the tendency to prioritize the selection of subjects exhibiting certain features. A poor sampling plan is the major reason for sampling bias. The bias of non-response is the most common one where by some individuals fail to have a chance of being selected in the sample. For instance, suppose a researcher wanted to find out the average income of a certain community and then chooses to select the sample based on telephone numbers. There is greater probability that this sample will be composed of high average income people only, since they are those most likely have home telephones, leading to a biased sample. Sampling bias leads to biased results therefore researcher made an effort to guard against it, as much as possible.

To avoid sampling bias the researcher used a sample of students from different faculties such as faculty of Business Studies and Tourism and Hospitality who are assumed to have low IT competency skills together with a sample of students from the Computer Science department who are assumed to have high competency in IT skills. In addition, the researcher also used varied information systems; that is a library management system, a database management system and E-Learning systems. The fact that the research study was carried out in two universities also worked out to reduce sampling bias as well.

- **Sampling error**

Sampling error is the difference between the true characteristics, and behaviors, of the entire population from those gathered from the sample. (Castillo 2009)

Sampling error arises from a situation whereby researchers select different subjects from the same population but still, the subjects show differences. Sampling error is usually as a result of a biased sampling procedure. Chance is another possible cause of sampling error. In order to minimize sampling error, random sampling was done, but chances are that the selected sample was still not representative of the whole population. To eliminate this error the solution is to test the entire population. However, this is not feasible in most cases.

(Castillo 2009)

3.6 SAMPLING TECHNIQUES

Random sampling and census are the sampling techniques that were used in this research study.

- **Census**

Respondents who provided information about the daily operation of the Millennium main library system were chosen using the census method. The census strategy uses

a complete enumeration (that is every member in the target group) as opposed to other sampling methods that deal with a selected group of respondents. The justification for census sampling was that there were only ***ten*** people who worked at the Circulation desk. This number is small and manageable, resulting in everyone in the target group (main library – Circulation desk staff) being part of the research study.

- **Random sampling**

This was used to select three groups of respondents. The ***first*** one is the group of students who use the UZ 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 (UZ). 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 Chinhoyi University.

The Observation schedule was used to observe security habits of the UZ main library staff, who work on the Circulation desk. The researcher recorded her findings from observations made during the processes of issuing out books, returning borrowed books, paying of fines and registration of new library patrons. The findings are discussed in Chapter 4.

3.7 POPULATION AND SAMPLE SIZE

Questionnaires were issued to five different groups of respondents. The population was about 4000 people. A sample of 160 was chosen for this study. The samples were composed of:

- 40 UZ Library end users (any student from UZ is a library end user)
- 40 CUT students (mixed programs)
- 40 UZ science students
- 10 UZ Library Circulation desk staff
- 30 CUT Database users

The return rate of questionnaires for each sample group is indicated in brackets

- 35 UZ Library end users (88%)
- 39 CUT students (98%)
- 36 UZ science students (90%)
- 8 UZ Library Circulation desk staff (80%)
- 20 CUT Database users (67%)

The overall return rate for all the questionnaires was 138/160 *100 = 86%

3.8 INSTRUMENTS

An observation schedule and questionnaires were used to collect data about human factors in information security, since a case study requires multiple data collection methods. It is hoped that these results would work together to achieve construct validity, See Appendix A for Observation schedule and Appendices B to E for questionnaires.

The observation schedule was used for the UZ main library 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.

The questionnaires issued to Library end users, CUT students and UZ Science students were the same. 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 Science respondents answered these questions using their experience of interacting with the TSIME e-learning system. On the other hand UZ Library end-users based their responses on their experience with the Millennium Library Management System.

The questionnaires administered to Database users and UZ main Library circulation desk staff was almost the same. The questionnaires were designed to collect data on password behaviour, whether they locked their offices for short periods of going out, rate of IT skills and whether they received IT training or not. CUT Database users used their experience of the Eagle Database to respond to the questionnaire. The Millennium Library Management System was used by the UZ main library Circulation desk staff.

3.8.1 Advantages of questionnaires

Administering questionnaires on random samples is a reliable way of gathering characteristics of a large group of people. These findings can then be generalized since they emanate from a random sample. In addition it makes it cost effective to collect data from a large population under study.

3.8.2 Disadvantages of questionnaires

- The wording of a question can influence how respondents answer questions. Questions seeking the respondents' opinion yield better results than those which sound accusatory. In this regard, accusatory type of questions were avoided in the questionnaires. See Appendices B to E.
- Some people may not return questionnaires. To overcome this challenge, the researcher let the respondents fill in the questionnaire while she waited.

3.8.3 Instrument validity and reliability

Instrument validity emanates from how way the instrument is administered. Some authors are of the opinion that reliability is simply a trait of the instrument itself.

3.8.4 Questionnaire validity

Validity refers to whether the survey or questionnaire measures what it is supposed to measure. In other words, validity refers to the extent to which a measuring device e.g. questionnaire is truly measuring what we designed it to measure. This was achieved by asking only those questions which are closely related to human factors in end-user information security.

3.8.5 Questionnaire reliability

Reliability is more to do with the consistency of a test, survey, observation, or other measuring device. A reliable questionnaire produces similar results even when administered to different groups of respondents. In short, a reliable questionnaire will always produce the same results regardless of the respondents and time and place.

To achieve reliability, a number of the same questions were asked to different groups of respondents. For instance, questions to do with password behavior, carelessness, I.T. security and training appeared on all the questionnaires given to Library staff, Library end-users, database users and students from different faculties. In addition the questionnaires were administered to students from different universities that is University of Zimbabwe and Chinhoyi University.

3.8.6 Cranach's alpha test for reliability (as per group of variables)

Internal consistency is vital whenever variables / items are used to form a scale. The items/ variables should have a correlation since they are meant measure the same thing. The Cronbach's alpha test is a good coefficient for assessing internal consistency. The Cronbach's alpha test was done for each group of questions to test for internal consistency. The four major human factors on the questionnaire were; Password behavior, Carelessness, Social Engineering and IT Security Training. The reliability test for each of these are attached in the appendices.

The variable "Carelessness" had three parameters under it namely*; Leave a logged on computer unattended to, Ignore warning from a browser and Allow someone to use my logged on computer*. The Cronbach's alpha value for these variables was 0.868. See Appendix G. The variable IT Security training had two parameters under it namely; *Receive IT Training and Refer to IT policy*. The Cronbach's alpha value for these variables was 0.727. See

Appendix H. Finally the variable Password behavior, had a total of six parameters under it, but two of them namely, *Choose good passwords and Change passwords frequency* required answers in the opposite of the other four. As a result a reliability test could not be performed at once using the entire six variables because it resulted in a Cronbach's alpha with a negative value which was caused by different scoring scales on the questionnaires. Thus the variable Password behavior was tested in two groups that is group 1 with variables; *Share passwords, Forget password, write down password and re-use the same password.* The Cronbach's alpha value for these four parameters was 0.816. The last group of parameters under Password behavior consisted of *Choose good password and Change password frequently*. The Cronbach's alpha value for these two parameters was 0.764. These Cronbach's alpha values for all the variables are high and this imply a high reliability among the parameters. Literature states that the closer the Cronbach's alpha coefficient is to 1.0 the greater the internal consistency of the items in the scale. George and Mallery (2003) in Gliem and Gliem (2003:87) provided the following rules of thumb:

> _ > .9 – Excellent, _ > .8 – Good, _ > .7 – Acceptable, _ > .6 – Questionable, _ > .5 – Poor, and _ < .5 – Unacceptable"

This means when testing for reliability the Cronbach's alpha value must be at least 0.7 and that a recommended goal is an alpha of 0.8.

3.9 DATA COLLECTION PROCESS

Data was collected by means of a survey. Questionnaires were in paper form and were distributed to respondents. For respondents made up of library end-users (UZ), Computer Science students (UZ) and CUT students, they were requested to fill in the questionnaire as the researcher waited for collection. This was done to ensure a high return rate since it was going to be difficult to follow up on respondents, in case they did not return the questionnaires. However the researcher failed to get back all questionnaires issued to Library

end users because students constantly moved in and out, making it difficult for the researcher to identify those to whom questionnaire were given.

For respondents who were members of staff, namely library staff (UZ) and departmental secretaries (CUT), a different approach was used. These were left to fill in the questionnaires within three days. This is because these people are professionals who could be busy with some other work, making it difficult to hurry them to complete the questionnaires. In addition, they are people who work in fixed / known offices, making it easy to make a follow up, in the event of questionnaires not returned. Unfortunately, this approach resulted in a lower return rate as the researcher could not find some of the respondents on the day of collecting the questionnaires.

3.10 SOFTWARE TOOLS

The statistical package PASW v 16.0 is the package used for data analysis. Findings from the research were analysed in terms of frequencies, crosstabs and one-way ANOVA (Analysis Of Variance) test.

3.11 CONCLUSION

The chapter discussed the research paradigm used, that is, mixed methods research approach. The research methodology used was “case study” and its applicability was justified. The strengths and drawbacks of this methodology were also discussed. Questionnaires and observation schedules were used for data collection. The advantages and disadvantages of questionnaires were also discussed. The data collection procedure was also discussed. The researcher also highlighted how she overcame these challenges. Instrument reliability and validity were also discussed. The next chapter is on the presentation, analysis and discussion of results.

CHAPTER 4: DATA PRESENTATION

4.1 INTRODUCTION

This chapter discusses the findings from the survey. The data analysis shows the data collected for each objective the, and draws general conclusions based on users' responses. The chapter also discusses the relationships between literature and findings of this particular research.

4.2 VALIDITY OF DATA COLLECTED

A comparison of samples that were drawn from two different institutions enhanced the results' validity. Therefore, other than analyzing the results individually, a comparison was done as well.

4.3 RESULTS EVALUATION

Observations and questionnaires were used to collect data during the research project.

The researcher worked with three (groups of respondents) information systems namely: The Millennium Library Management System at the University of Zimbabwe (UZ) main library, the E-Learning Management System (TSIME) at UZ and the Integrated Database System at Chinhoyi University. The research questions were used to discuss findings from the observations made.

4.4 QUALITATIVE ANALYSIS OF DATA

The analysis is based on what the researcher observed while the Circulation desk staff interacted with the Millennium Library Information System. This observation was meant to ascertain the kind of human errors to use for the research study. The researcher also observed UZ students as they worked in the Computer Science laboratory. Findings from these observations provided clues as to the kind of questions to use in the questionnaires. Below is a qualitative analysis of the observations made by the researcher.

4.4.1 The Millennium Library Management System

This system is used for managing the borrowing of books to patrons, the returning of borrowed books to the library, registration of patrons to the system and the paying of fines pertaining to library usage. The researcher observed only the Circulation desk staff as well as students' interaction with the system. The researcher observed the findings below:

a) **Leaving a logged on computer unattended to**

Library Circulation desk staff had a tendency of not logging off when attending to phone calls or when going to the toilet. Others leave their computers logged on when going for tea. Circulation desk can use each other's account to do work. Library patrons, (end-users) especially students were also observed leaving their logged on computers unattended to, or completely going out of the library without logging off.

b) Social Engineering (impersonification)

A student can use another student's college ID for borrowing books, for instance. In addition if a student commits an offence of "improper library behaviour" such as use of cell-phone or mis-use of a computer, the student can produce another student's ID for purposes of being charged. This means a wrong student's account is charged.

c) **Failure to follow procedures**

An example of this is when a Circulation staff member gets a book without following the correct procedure (that is using the book inside the library but without having borrowed it out using the system). This means when a student uses the online catalogue to check the availability of a desired book, the system reports that the book is available, but in actual fact, some staff member is using it unofficially. This creates unnecessary inconvenience for the student who is informed (by the system) that a particular book is available, but cannot get it.

d) **Library patrons may be erroneously assigned to the wrong grade during registration**. Grade or Patron Type determines the number of books one can borrow and the period for which one can borrow a book. In order for patrons to use the library, they have to register with the library first. For registration purposes, University employees only take their staff ID cards for registration in the library. For instance, PatronType5=Senior non-academic staff who have a priviledge of borrowing at most ten books and return them after three months, while PatronType6=Junior non-academic staff who can borrow up to four books and return them after two weeks. Chances of human error in this case are very prevalent since the staff ID card does not specify an employee's grade. It only states the job title e.g. Clerk, Driver etc without indicating the grade. This means if a patron is registered using a wrong grade, especially one that disadvantages them; they will not enjoy their rightful benefits.

e) Carelessness e.g. Failure to cross-check screen messages when using scanner during the process of returning (checking-in) books.

When one returns a book to the library, the Library staff member scans the book so that the system captures it as having been returned. The scanner makes a beep

sound after reading the bar code. The human error here is that in most cases, the Library person assumes that the beep sound is a sign that the book has been captured as a returned book. In some cases the beep sound may be a warning message that the Librarian has to attend to before proceeding. An example of such warning messages is the one below:

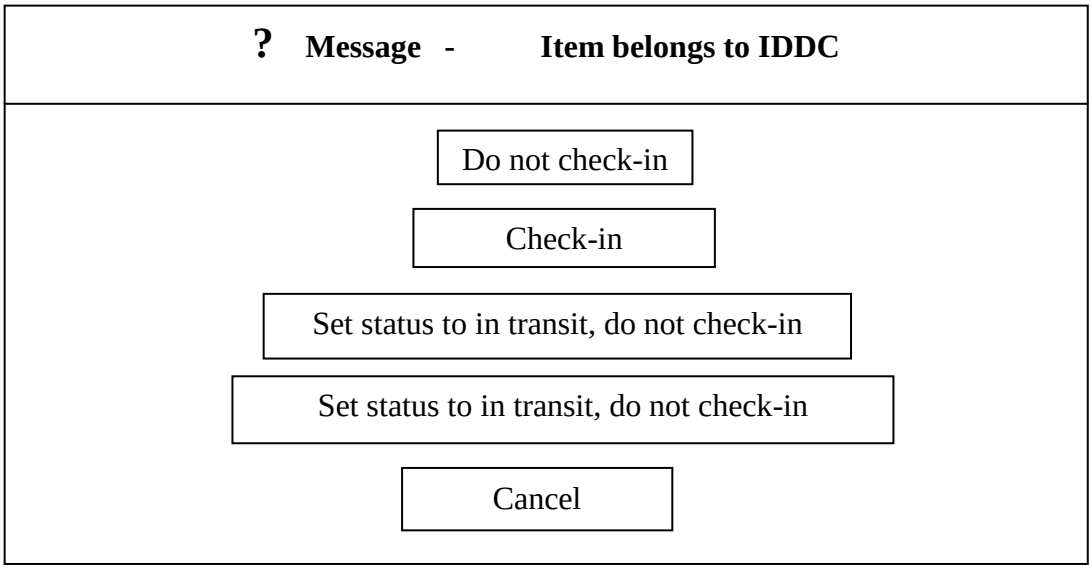

Figure 6: Warning message during the check in process

The warning message above informs the Librarian that the book scanned does not belong to the main library, but belongs to the Institute of Development Studies Library, which is a sub-library of the main library. If the Librarian clicks on "Check-In" by mistake, then it means the IDDC sub-library stock will show that this particular book was returned, but in fact it will not be physically present in that library. To avoid this error a student is supposed to return a book to the specific sub-library where he or she borrowed it.

However, there are situations whereby a student has no choice but just to have a book borrowed from a sub-library, returned to the main library. This is because all sub-libraries do not open on Saturdays and Sundays. This means all books due on

Saturdays and Sundays have to be returned to main library so that students do not accrue over-due fines.

The human error here is that library staff can arrange all returned books to shelves of the main library without separating those from sub-libraries. The proper thing for the librarian to do is to separately arrange all books according to their sub-libraries so that they can be transported to the appropriate sub-libraries. If the librarian makes this mistake, of not separating books, then systems in these sub-libraries will indicate that the books have been returned, and yet the books will not be physically present.

f) Carelessness - Wrong date stamp

Books are lent to patrons on either short-term (3 days) or long-term (fourteen days) basis. If a Librarian has been issuing out books on long-term basis, tendency is that the Librarian continues stamping the same date even for short term books. Suppose the Librarian erroneously loans (by stamping) a short-term book on long-term basis, then it means that the student suffers consequences of over-due fine. This is because that all short term books are programmed to be returned 3 days after the day of borrowing. The same applies for all long-term books. This means fines are calculated automatically, and this is not negotiable. As a result the student (borrower) is unfairly charged, while the library enjoys an unfair economic gain.

4.4.2 The Eagle Integrated Database System

Chinhoyi University uses a database management system called Eagle. The system stores all the details about each student, such as personal details, programme being studied and results for each semester. This system is basically used by *Admissions* department for student

admissions purposes, Departmental *secretaries* for capturing exam marks, and the *Systems analyst* for calculating grades for courses and *Exams* department for preparing transcripts.

This research study only covers the activities of Departmental secretaries on the integrated system. Permission to include the rest of the database users was not granted by the relevant authorities. There are human errors that arise especially when departmental secretaries capture results of students. The researcher made several observations during the time of capturing students' results. The researcher made the following observations as secretaries captured results for students:

a) Student marks erroneously entered
b) Student is assigned an incorrect decision e.g. discontinue instead of proceed carrying a certain course(s).

The system is designed such that once a mark is entered and the Enter key is pressed, it is impossible to alter the mark. If a secretary captures an incorrect mark for a student, then the department writes a letter to the Database Manager to seek permission to change (correct) that mark. This process proves to be tedious as one has to physically take the letter to the Database Manager and Senior Assistant Registrar (Academic) for signing. Once authorized the option for changing / editing marks is then activated for that particular secretary.

4.5 QUANTITATIVE DATA ANALYSIS

This was done using data from questionnaires. The statistical analysis of the data collected. was done using statistical package, PASW v16.0. This data analysis was used to formulate the model for human factors in end-user information security. The analysis was done in terms of frequencies, cross tabs and one-way ANOVA test.

4.5.1 Frequencies

All frequencies were summarized in the table below.

Table 3: Frequencies of data collected

	Password behavior (%)						Social Eng. (%)	Carelessness (%)			IT Security Training %	
Response	Share password s)	Forget password(s)	Write down	Choose good paswrd	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 %

From Table 3 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 and *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. Refer to Appendix L, Frequencies1.sav, for the detailed frequencies.

Only the figures in italics and underlined are discussed. Results indicated 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.

4.5.2 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.

Table 4: Crosstabs analysis

	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**
Somtimes	**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

1 - CUT **2 - UZ**

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

5 - Database users

The table 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". Only three parameters are discussed here due to space limitations. Only the figures in italics and underlined are discussed. The rest of the parameters on Crosstabs are in Appendix M, crosstabs1.sav. Based on Table 4 above, it is evident a greater proportion of CUT respondents never or rarely change their passwords, indicated by the figures 10 and 11 respectively. Only two out of 39 respondents from CUT always 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 five out of eight 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, that is, 15 for sometimes and 16 for regularly. Same applies to CUT respondents with a total of 32 out of 39 respondents who have this same habit, with 10 for sometimes and 22 for regularly. 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 (that is 11 out of 20) and only 2 out of 20 regularly do this. 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, (that is 17 sometimes and 14 regularly). For UZ, 30 out of 36 respondents do this, (that is 13 sometimes and 17 regularly). For Library end users 31 out of 35respondents do this, (that is 17 sometimes and 14 regularly). 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.

4.5.3 One-way ANOVA test

ANOVA stands for analysis of variance. It is a statistical analysis for determining how each sample group differs from the other using, the mean. In this case (One-way ANOVA) the researcher used one independent variable, namely category of respondents. The analysis below shows the significant value between groups of respondents.

Table 5: ANOVA analysis summary

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

Based on Table 5 above, the two groups are not significantly different. For instance, in terms of leaving a logged on computer unattended to the mean significance between all the groups is 0.000. This mean difference is insignificant, implying that the groups are the same. This means the five groups of respondents have almost the same characteristics as far as each of the stated parameters are 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. Refer to Appendix N, ANOVA one-way.sav for a detailed ANOVA analysis.

4.6 HUMAN FACTORS COLLABORATIVE REINFORCEMENT MODEL

The Human Factors Collaborative Reinforcement Model is the model proposed by this research study. Since literature earlier on, highlighted that automation is not going to solve this problem, a non-technical solution was therefore proposed. Findings from the survey led to the development of this model.

The greatest challenge concerning human factors in end-user information security is that, it is an area for which limited research has been done, so far. As a result very few models exist, from which the researcher could borrow ideas. Thus, this research project proposed a human factors model that is centered on collaborative monitoring against policy violations by making use of reinforcement. The fundamental ideas of the proposed human factors model are heavily borrowed from Saha and Misra (2009); **A Reinforcement Model for Collaborative Security.** Their model emphasizes a framework that facilitates collaborative monitoring for violations of policy. Their model 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. A case that can be used to better understand the Reinforcement model for collaborative security works is when a user shares a logged on computer with somebody else who may have lower access right s to a particular system

4.6.1 Assumptions

The human error model suggested by this research study 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.

4.6.2 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.

4.6.3 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.

4.6.4 What makes this model different from the one by Saha and Misra (2009)?

- It specifies the form of rewards and punishment i.e. points gained or lost that consequently determine tangible benefits e.g. increased or reduced internet access time depending on violation type
- It uses actual variables namely, carelessness, impersonification (social engineering) and password behaviour.

  The justification for using these variables comes from the survey that was carried out on two different local universities. These variables mentioned above were found to be the most prevalent.
- It is limited only to primary violations and not concerned with secondary violations
  - A primary violation is whereby a user s_i detects and reports a policy violation.
  - A secondary violation is whereby a user s_i detects a policy violation and does not report it, instead, some other subject s_n (who also witnessed the same violation) reports against her for doing so.
  - This model considers the person who committed the violation, unlike the original one which only considers the violation and not the person who committed it and yet these two are strongly linked and are difficult to separate

The rewards / punishment model

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, $Vio = \{vio1, vio2, \ldots, viom\}$

Table 6: Primary pay-off table

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}	#

The **notations** below are adapted from Saha and Misra (2009)

$\boldsymbol{R_{ij}}$ **:** 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 $\boldsymbol{vio_j}$.

$\boldsymbol{\Theta_{ij}}$**:** 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.

4.6.5 Challenges associated with models based on rewards and punishments

- 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 an 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.

4.6.6 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. As mentioned earlier on, it is the type of reward due them that will motivate users to make a report. It is also important to consider that there could be some hidden benefit for not reporting a policy violation.

4.6.7 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 Saha and Misra (2009) 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: 7 shows the classification of policy violations.

Table 7: 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		

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 $\mathbf{T_{rew}}$ or type of punishment is directly proportional to the rank of violation, $\mathbf{R_{vio}}$. $\mathbf{T_{rew}} \propto \mathbf{R_{vio}}$ thus, $\mathbf{T_{rew} = k\ R_{vio}}$. Table 8 below is for determining the type of rewards / punishment for each type of policy violation.

Table 8: Determining actual rewards for violations

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

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 $\boldsymbol{rrep_{ij}}$ denotes that the subject $\boldsymbol{s_i}$ will report a primary violation $\boldsymbol{vio_j}$.
- Motivational index for reporting is

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

4.6.8 Likelihood for reporting a policy violation

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

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

- Calculating $\boldsymbol{m_{ij}}$ first, we get
- $\boldsymbol{m_{ij}}$ $\mathbf{= (\ |\ T_{ij}\ [1,\ 2]| + \max\{|\ T_{ij}\ [1,3]|, |\ T_{ij}\ [1,4]|\} - \Omega_j\ )}$

  $\mathbf{= (\ R_{ij} + \max\{- CP_j, - P_{ij}\} - \Omega_{jj}\ )}$

  $\mathbf{=(\ 14 + \max\{-10,-6\}\ -1)}$

=14-6 -1

=7

Calculating the likelihood for reporting policy violation $\mathbf{R_{vio}}$ **=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

= <u>82%</u>

Using policy violation $\mathbf{R_{vio}}$ **=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]|} − Ω_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 $\mathbf{R_{vio}}$ **= 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

= <u>74%</u>

Using policy violation $\mathbf{R_{vio}}$ **=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]|} − Ω_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 $\mathbf{R_{vio} = 3,}$ we get

$$l_{ij} = [\, m_{ij} * R_{ij} - CP_j - P_{ij}] / 100) \text{ (expressed as a percentage)}$$

$$= [(8* 10 -4 -5) / 100]$$

$$= (80-9)/100$$

$$= 71/ 100$$

$$\underline{= 71\%}$$

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 she 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.

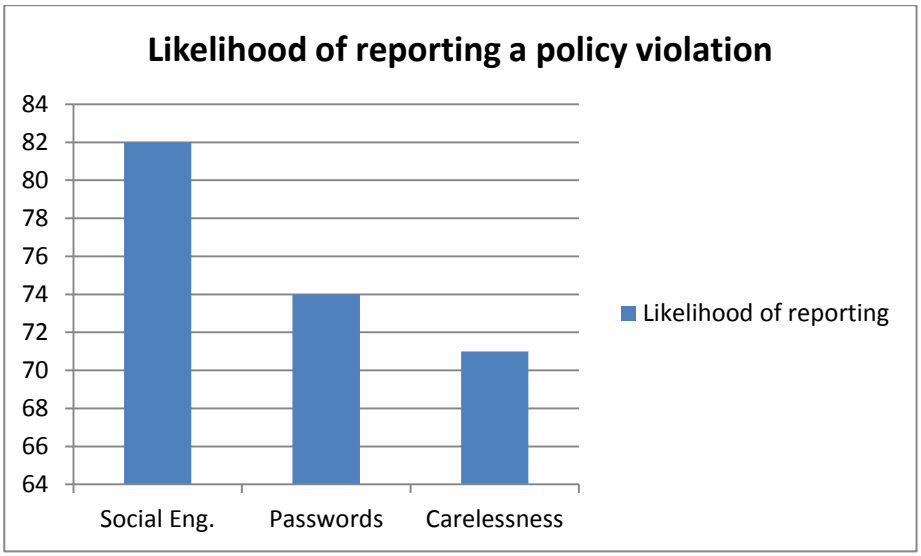

Figure 7: Likelihood of reporting a policy violation

Figure 7 above 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.

4.6.9 Justification for this model

Jones and Martin (2010:8)

> Security is currently seen as an activity that only has penalties for poor behaviours and that has no obvious positive impact on the user. An approach that might be considered for improving ICT security would be to offer incentives for acting in a positive manner with regard to security. This might be implemented in a number of ways, depending on the organization, but the effect that could be achieved is to attract attention to ICT security within the organization and change the way in which it is viewed by staff. One example of this is the Massachusetts Department of Environmental Protection 2010 Small System Security Award.

According to Saha and Misra (2009:3), some of the conclusions from these socio-psychological studies 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 Saha and Misra (2009) 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.

4.7 INFORMATION SECURITY POLICY

The human factors model proposed by the researcher, **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 F for the security policy. 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 Appendix F.

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.

4.8 CONCLUSION

The chapter discussed the results of the findings using frequencies, one-way ANOVA and crosstabs. Crosstabs were used to establish relationships among groups of respondents. 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.

CHAPTER 5: CONCLUSION, RECOMMENDATIONS AND FUTURE WORK

5.1 INTRODUCTION

Human factors influence how individuals interact with information security technology; it is this interaction that is often detrimental to security. It is evident that purely technical solutions are unlikely to prevent security breaches. Organizations need to enforce and maintain a culture where positive security behaviours are valued. Technology on its own cannot be used to solve numerous violations of security emanating from human behavior. Therefore a combination of technical and non-technical solutions should be used to solve this human error problem.

5.2 CONCLUSION

This thesis' aim was to come up with a model to minimize human error in information security. The scope of this study was specifically; human factors in end-user information security. A case study was carried out at University of Zimbabwe and Chinhoyi University. A survey was carried out to determine the human factors to use for the study. Three major causes of human errors were identified, 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. The relationships between human errors were illustrated using Crosstabs and one-way ANOVA analysis. In this study, all the groups of respondents did not prove to be significantly different, that is, they all exhibited the same characteristics as far as human error is concerned. 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. See Appendix F. 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. Zelonis (2004:3) concludes the matter by that

> … technology solutions should still be pursued but with the intent of working in combination with user behavioral strategies.

Furthermore, the case study methodology used, makes it difficult to generalize findings. Thus, the model developed by the researcher in this study is with regard to the systems that were studied and the organizations from which samples were drawn.

5.3 CRITIQUE OF OWN WORK

Allocation of rewards in the form of points in Table 8 (Determining actual rewards for violations), is subjective. In addition, the model is applicable only to users who work in groups such as students and may not be applicable to users who work as individuals and may not share an office such as secretaries.

5.4 RECOMMENDATIONS & FUTURE WORK

Simulations based on the Human factors model will need to be carried out. In addition there could be need to include more human errors, since this research work only looked at three, which are Social engineering, Password Behaviour and Carelessness. The researcher's recommendation is that organizations should be more co-operative in order to enable better research on security to take place.

REFERENCES

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

Brown, A. B. (2004) **Coping with Human Error in IT.** *Queue vol. 2, no. 8*— ACM Digital Library

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

Castillo, J. J. (2009) **Sampling Error in Research,** Experiment Resources: http://www.experiment-resources.com/sampling-error.html

Cranor L. F. **A Framework for Reasoning about the Human in the Loop**, Carnegie Mellon University

Du Plessiss, Y. (2004) **Research methodology and Method** University of Pretoria etd, South Africa

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

Fléchais, I. (2005) **Designing Secure and Usable Systems**, University College London

Furnell, S. (2005). **Why users cannot use security**. *Computers & Security*, page 249-279

Gliem, J. A. & Gliem, R. R. (2003) **Calculating, Interpreting, and Reporting Cronbach's Alpha Reliability Coefficient for Likert-Type Scales,** Midwest Research to Practice Conference in Adult, Continuing, and Community Education, Ohio State University, Columbus

Gonzales, J. J. & Sawicka, A. (2002**) A Framework for Human Factors in Information Security**, Proceedings of the WEAS International Conference on Information Security, Rio de Janeiro, Brazil

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

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

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

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

Moon, J and Moon, S. (2004) **The Case for Mixed Methodology Research: A review of literature and methods**

Norman, D. A. (1981) **Categorization of action slips.** ***Psychological Review****, 88(1),* 1-15.

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

O'Brien, J.A. (2000). **Introduction to Information Systems: Essentials for the Internetworked Enterprise.** United States of America. McGraw-Hill Companies, Inc..

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

Patrick, A. (2002) **Human Factors of Security Systems: A Brief Review (Draft),** National Research Council of Canada, Version 1.5, Canada

Rice University Information Security Policy Document ID 1.0 Version 1.0.5

Risvold, M. O. (2010) **Organizational Issues related to information security behaviour**" A Master's Thesis for the Department of Business Administration and Social Sciences, Lulea University of Technology

Sapronov, K. (2005) **The human factor and information security** from www.securelist.com 01 525026 ch01.qxd 4/7/03 9:31 AM Page 1-12

Sasser, P. (2010) **Human Error and Information Security**, Articles Base Free Online Articles Directory

Schneier, B. (2004) **Secrets and Lies: Digital Security in a Networked World**. Wiley Publishing, Inc, Indianapolis, Indiana

Trc˘ek, D. and Kandus, G. (2003) **Information Systems Security Policy - Human Factor Modelling and Simulation** "Jo˘zef Stefan" Institute Jamova 39, 1001 Ljubljana, Slovenia

Weir, C. S., Douglas, G., Carruthers, M., & Jack, M. (2009**). User perceptions of security, convenience and usability for e-banking authentication tokens**. *Computers & Security*, *28*(1-2), 47-62.

Zelonis, K. (2004) **Avoiding the Cyber Pandemic: A Public Health Approach to Preventing Malware Propagation,** Carnegie Mellon University

Zhang, Reithel & Li (2009) **Impact of perceived technical protection on security behaviors,** USA

APPENDICES

APPENDIX A

OBSERVATION SCHEDULE
Human Factors in Information System Security

Observation schedule on how library staff works with the Millennium Library System

1. Log on procedures

……

……

……

2. Share password,

……

……

……

3. Write down password

……

……

……

……

4. Leaving a logged in computer unattended to

……

……

……

……

5. Allowing a colleague to one's logged on computer

……

……

……

6. Locking of offices for short periods e.g. when going to a nearby office

……

……

……

……..

7. Not following procedures

……..

……..

……..

8. Any other human error(s)

……..

……..

……..

……..

……..

……..

The End.

APPENDIX B

QUESTIONNAIRE - HUMAN FACTORS IN INFORMATION SECURITY
Questionnaires for Library staff

Introduction
I am Mary Muhonde. I am carrying out a research study entitled "**Towards minimizing Human Factors in Information Systems Security".** Data collected from this research study will be treated with utmost confidentiality and will be used strictly for academic reasons.

Instructions

- **Please do not write or any form of your identification details e.g. your name**
- **Fill in the questionnaire as honestly as possible, making sure you follow the given instructions in each question.**

SECTION A - Personal details **Please tick in the appropriate box**

1. What is your highest academic qualification?

☐	Ordinary Level	☐	Advanced Level
☐	Certificate	☐	Diploma
☐	Degree	☐	Masters Degree
☐	Other. Specify ……		

2. How experienced are you with Information Systems?

☐	Less than one year	☐	One-Two years
☐	More than two years	☐	More than five years

3. Period you have been using this particular Library Management System?

☐	Less than one year	☐	One-Two years
☐	More than two years	☐	More than five years

4. How do you rate your IT skills?

☐ Struggle a lot (Have problems handling files/folders and programs. Have lost data at times)

☐ Below average (Often need help and should learn more)

☐ Average (Can do what is expected but should learn more)

☐ Good (Manage fine and sometimes help other users)

☐ Very good (Have no problems at all. Often help other users)

☐ Others (Specify)

……..

……

Please use the following ratings from 0 to 4 as follows

Rate	Meaning
4	Always
3	Regularly
2	Sometimes
1	Rarely
0	Never

SECTION B - Password behaviour

Score

1. I share my passwords with colleagues. …….
2. I have a tendency to forget my password(s). ……..……
3. I write my password(s) on pieces of paper. …….
4. I choose good passwords. (i.e. not easily guessed ones). ……..
5. How often do you change your password(s)? ……....
6. Some of my user accounts share the same password. ……..

SECTION C - Impersonification / Social Engineering

1. I give patrons permission to access library facilities without thoroughly checking their IDs ……
2. If I receive email with an interesting subject e.g. "critical security updates", I open it. …….
3. I provide my username and password over the telephone to technicians for the purposes of fixing faults. …….

SECTION D - Input / Output Screen Design

1. The screen design of the program I use results in human errors ……..

SECTION E - Carelessness

1. During checking in or checking out books, I assume that the beep sound from the scanner means that everything is OK. …….
2. I leave my logged on computer unattended to …….
3. I ignore warnings from a web browser e.g. warning of a potentially harmful website. ……..
4. I let other people use my logged on computer. ……

5. I lock my office whenever I leave it, even if it is for a short while like going to the toilet? …….
6. I use my organization's e-mail address on the Internet even for competitions, chain letters, etc ……..

SECTION F - IT security training

1. I receive training on IT security practices ……..
2. I refer to the IT policy / rules for guidance. ……..

SECTION G - Impact of human errors in information systems security

1. Human error problems may result in the following
(Use **the rating overleaf: 0 to 4)**

a) Compromising information integrity …….

b) distribution of private information …….

c) availability of incorrect / inaccurate information ……

d) unfair economic loss / gain …….

e) information system interruption …….

Thank you for your co-operation.

APPENDIX C

QUESTIONNAIRE - HUMAN FACTORS IN INFORMATION SECURITY
Questionnaires for Library End-users

Introduction

I am Mary Muhonde and I am carrying out a research study entitled "**Towards minimizing Human Factors in Information Systems Security".** Data collected from this research study will be treated with utmost confidentiality and will be used strictly for academic reasons.

Instructions

- **Please do not write your identification details e.g. your name**
- **Fill in the questionnaire as honestly as possible, making sure you follow the given instructions in each question.**

SECTION A - Personal details **Please tick in the appropriate box**

1. What is your highest academic qualification?

☐ Ordinary Level ☐ Advanced Level

☐ Certificate ☐ Diploma

☐ Degree ☐ Masters Degree

☐ Other. Specify ……

2. For how long have you been using this particular Information System?

☐ Less than two years ☐ One-Two years

☐ More than two years ☐ More than five years

3. Programme under study …….

4. How do you rate your IT skills?

☐ Struggle a lot (Have problems handling files/folders and programs. Have lost data at times)

☐ Below average (Often need help and should learn more)

☐ Average (Can do what is expected but should learn more)

☐ Good (Manage fine and sometimes help other users)

☐ Very good (Have no problems at all. Often help other users)

☐ Others (Specify) …….

Please use the following ratings from 0 to 4 as follows

Rate	**Meaning**
4	Always
3	Regularly
2	Sometimes
1	Rarely
0	Never

SECTION B - Password behaviour

Score

1. I share my passwords with colleagues. …….
2. I have a tendency to forget my password(s). ……..……...
3. I write my password(s) on pieces of paper. ……..…
4. I choose good passwords. (i.e. not easily guessed ones). ……
5. How often do you change your password(s)? ……..
6. Some of my l user accounts share the same password . (e.g. library account, personal email account,) ……

SECTION C - Impersonification / Social Engineering

1. I either use somebody's student ID or let somebody use my student ID to gain access to the computer lab / library ……..…

2.If I receive email with an interesting subject e.g. "new computer games", I open it. ……

SECTION D - Input / Output Screen Design

1. The screen design of the program(s) I use results in human errors ……..

SECTION E - Carelessness

1. I leave my logged on computer unattended to. …….
2. Ignore warnings from a web browser e.g. warning of a potentially harmful website ……..

3.I let other people use my logged on computer. ……

SECTION F - IT security training

1. I receive training on IT security practices ……..
2. I refer to the IT policy / rules for guidance. ……..

Thank you for your co-operation.

APPENDIX D

QUESTIONNAIRE - HUMAN FACTORS IN END-USER INFORMATION SECURITY
Questionnaires for Students

Introduction

I am Mary Muhonde and I am carrying out a research study entitled "**Towards minimizing Human Factors in Information Systems Security".** Data collected from this research study will be treated with utmost confidentiality and will be used strictly for academic reasons.

Instructions

- **Please do not write your name or any form of your identification details.**
- **Fill in the questionnaire as honestly as possible, making sure you follow the given instructions in each question.**

SECTION A - Personal details **Please tick in the appropriate box**

1. What is your highest academic qualification?

☐ Ordinary Level ☐ Advanced Level

☐ Certificate ☐ Diploma

☐ Degree ☐ Masters Degree

☐ Other. Specify …….

2. For how long have you been using this particular Information System?

☐ Less than two years ☐ One – two years

☐ More than two years ☐ More than five years

3. Programme under study ……

4. How do you rate your IT skills?

☐ Struggle a lot (Have problems handling files/folders and programs. Have lost data at times)

☐ Below average (Often need help and should learn more)

☐ Average (Can do what is expected but should learn more)

☐ Good (Manage fine and sometimes help other users)

☐ Very good (Have no problems at all. Often help other users)

☐ Others (Specify) …….

Please use the following ratings from 0 to 4 as follows

Rate	Meaning
4	Always
3	Regularly
2	Sometimes
1	Rarely
0	Never

SECTION B - Password behaviour

Score

1. I share my username and/or passwords with colleagues. ……..……
2. I have a tendency to forget my password(s). ……..……..
3. I write difficult password(s) on pieces of paper. ……
4. I choose good passwords. (i.e. not easily guessed ones). ……
5. How often do you change your password(s)? …….....
6. Some of my user accounts share the same password. (e.g. e-learning account, personal email account,) ……..

SECTION C - Impersonification / Social Engineering

1. I either use somebody's student ID or let somebody use my student ID to gain access to the computer lab / library ……..
2. If I receive email with an interesting subject e.g. "new computer games", I open it. ……..

SECTION D - Carelessness

1 I leave my logged on computer un-attended to. …….

2. Ignore warnings from a web browser e.g. warning of a potentially harmful website. ……
3. I let other people use my logged on computer. ……
4. Do you open an attachment from an unfamiliar email address ……

SECTION E - IT security training

1. I receive training on IT security practices ……..
2. I refer to the IT policy / rules for guidance. ……..

SECTION F - Security policy

1. Do you have rights to add your own software on college computers? (i.e. any software other than that technicians install for you) …..…….……

Thank you for your co-operation.

APPENDIX E

QUESTIONNAIRE - HUMAN FACTORS IN INFORMATION SECURITY
Questionnaire database users

Introduction

I am Mary Muhonde and am carrying out a research study entitled "**Towards minimizing Human Factors in Information Systems Security".** Data collected from this research study will be treated with utmost confidentiality and will be used strictly for academic reasons.

Instructions

- **Please do not write any form of your identification details e.g. your name**
- **Fill in the questionnaire as honestly as possible, making sure you follow the given instructions in each question.**

SECTION A - Personal details **Please tick in the appropriate box**

1. What is your highest academic qualification?

☐ Ordinary Level ☐ Advanced Level

☐ Certificate ☐ Diploma

☐ Degree ☐ Masters Degree

☐ Other. Specify ……

2. For how long have you been using this particular Database Management System?

☐ Less than one year ☐ One – two years

☐ More than two years ☐ More than five years

3. How do you rate your IT skills?

☐ Struggle a lot (Have problems handling files/folders and programs. Have lost data at times)

☐ Below average (Often need help and should learn more)

☐ Average (Can do what is expected but should learn more)

☐ Good (Manage fine and sometimes help other users)

☐ Very good (Have no problems at all. Often help other users)

☐ Others (Specify) ……

Please use the following ratings from 0 to 4 as follows

Rate	Meaning
4	Always
3	Regularly
2	Sometimes
1	Rarely
0	Never

SECTION B - Password behaviour

Score

1. I share my passwords with colleagues. ……
2. I have a tendency to forget my password(s). ……..……..
3. I write my password(s) on pieces of paper. ……
4. I choose good passwords. (i.e. not easily guessed ones). ..……
5. How often do you change your password(s)? ……...
6. Some of my user accounts share the same password ...…….

SECTION C - Input / Output Screen Design

1. The screen design of the program I use results in human errors ..……..

SECTIOND - Impersonification / Social Engineering

1. If I receive email with an interesting subject e.g. "critical security updates", I open it. …….
2. I provide my username and password over the telephone to technicians for the purposes of fixing faults. …….

SECTION D - Carelessness

1. I leave my logged on computer unattended to ……
2. I let other people use my logged on computer. ……....
3. Ignore warnings from a web browser e.g. warning of a potentially harmful website. ……
4. I lock my office whenever I leave it, even if it is for a short while like going to the toilet? ……
5. I print sensitive documents like exams or student results or staff personal details on printers other people may access? ……
6. I use my organization's e-mail address on the Internet even for competitions, chain letters, etc ……

SECTION E - IT security training

1. I receive training on IT security practices ……..
2. I refer to the IT policy / rules for guidance. ……..

SECTION F - Impact of human errors in information systems security

Human error problems may result in the following
(**Use the rating on previous page)**

a) a compromise of information integrity …….

b) distribution of confidential information ……..…….

c) availability of incorrect / inaccurate information …..……

d) unfair economic loss / gain …….

e) information system interruption .…….

SECTION G - Data capture errors

What are the common errors that you make during data capture e.g. entering an incorrect mark for a student

i) …….

ii) …….

iii) …….

iv) …….

SECTION H- What are inconveniences do you experience as a result of human errors

i) Error

……..

Inconvenience

……..

ii) Error

……..

Inconvenience

……..

iii) Error

……..

Inconvenience

……..

Thank you for your co-operation.

APPENDIX F

HUMAN FACTORS INFORMATION SECURITY POLICY

VERSION 1.0

CONTENTS

1.0 Purpose

This policy aims at giving guidelines to university students and staff in order to minimize human error in information security.

2.0 Scope

This policy applies to students and staff in local universities.

3.0 Policy

In order to ensure the integrity, confidentiality and availability of sensitive and personal information, appropriate measures must be taken when using computers.

3.1 Code of conduct

Suspected security policy violations such as ignoring warnings from browser", "leaving a logged on computer unattended to" and other forms of compromise, should be immediately reported to the proper IT personnel.

3.2 Appropriate measures include:

3.2.1 Limiting access to computers only to authorized personnel

3.2.2 Adhering to all password policies and procedures"

3.2.3 Passwords will be established and maintained to provide system security.

- **3.2.3.1** Each password must be at least eight characters long, using numbers, capital letters and lower case letters.
- **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 Making sure that computer screens are positioned in such a way that hinders public. 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 systems administrator is to implement a security program that caters for user education, procedure and training policy across the whole university.

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

Disciplinary measures in the form of negative reinforcement will be applied on anyone found violating this policy.

7.0 Definition of terms

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

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.

APPENDIX G

```
CARELESS RELIABILITY
  /VARIABLES=Carelesness1 Carelesness2 Carelesness3
  /SCALE('ALL VARIABLES') ALL
  /MODEL=ALPHA.
```

Reliability

[DataSet1] H:\Data Analysis Muhonde\combined all grps for comon variables.sav

Scale: ALL VARIABLES

Case Processing Summary

		N	%
Cases	Valid	138	100.0
	Excluded[a]	0	.0
	Total	138	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	N of Items
.868	3

APPENDIX H

```
I.T. SECURITY RELIABILITY
/VARIABLES=SecTraining1 SecTraining2
/SCALE('ALL VARIABLES') ALL
/MODEL=ALPHA.
```

Reliability

[DataSet1] H:\Data Analysis Muhonde\combined all grps for comon variables.sav

Scale: ALL VARIABLES

Case Processing Summary

		N	%
Cases	Valid	138	100.0
	Excluded[a]	0	.0
	Total	138	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	N of Items
.727	2

APPENDIX I

```
PASSWORDS GROUP 1 RELIABILITY
  /VARIABLES=PaswrdsA PaswrdsC PaswrdsB PaswrdsF
  /SCALE('ALL VARIABLES') ALL
  /MODEL=ALPHA.
```

Reliability

[DataSet1] H:\Data Analysis Muhonde\combined all grps for comon variables.sav

Scale: ALL VARIABLES

Case Processing Summary

		N	%
Cases	Valid	138	100.0
	Excluded[a]	0	.0
	Total	138	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	N of Items
.816	4

APPENDIX J

```
PASSWORDS GROUP 2 RELIABILITY
  /VARIABLES=PaswrdsD PaswrdsE
  /SCALE('ALL VARIABLES') ALL
  /MODEL=ALPHA.
```

Reliability

[DataSet1] H:\Data Analysis Muhonde\combined all grps for comon variables.sav

Scale: ALL VARIABLES

Case Processing Summary

		N	%
Cases	Valid	138	100.0
	Excluded[a]	0	.0
	Total	138	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	N of Items
.764	2

APPENDIX K

FREQUENCIES OF
VARIABLES=Qualific PeriodIS ITSkills PaswrdsA PaswrdsB PaswrdsC PaswrdsD Paswrds
E PaswrdsF SocailEng1 Carelesness1 Carel
esness2 Carelesness3 SecTraining1 SecTraining2
/ORDER=ANALYSIS.

Frequencies

[DataSet1] H:\Dissertation Mary\Documentation-thesis\Appendices\Appendix K-combined responses.sav

Statistics

		Highest Qualification	Time of using Info Systm	Rate of IT skills	Sharing Password	Forget my Password	Write down password	Use good passwords	Changing password-	Use same password	Opening interesting mail	Leaving logged on computer	Ignore browser warnings	Allow one to use my logged on computer	Receive IT training	Refer to IT policy
N	Valid	137	134	138	138	138	138	138	138	138	138	138	138	138	138	138
	Missing	1	4	0	0	0	0	0	0	0	0	0	0	0	0	0

Frequency Table

Highest Qualification

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Advanced	57	41.3	41.6	41.6
	Certificate	18	13.0	13.1	54.7
	Diploma	31	22.5	22.6	77.4
	Degree	31	22.5	22.6	100.0
	Total	137	99.3	100.0	
Missing	System	1	.7		
Total		138	100.0		

Time of using Info Sys

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0-1 yr	21	15.2	15.7	15.7
	1-2 yrs	66	47.8	49.3	64.9
	more than 2 yrs	30	21.7	22.4	87.3
	more than 5 yrs	17	12.3	12.7	100.0
	Total	134	97.1	100.0	
Missing	System	4	2.9		
Total		138	100.0		

Rate of IT skills

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	struggle a lot	11	8.0	8.0	8.0
	below average	44	31.9	31.9	39.9
	average	61	44.2	44.2	84.1
	good	21	15.2	15.2	99.3
	very good	1	.7	.7	100.0
	Total	138	100.0	100.0	

Sharing Password

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	never	29	21.0	21.0	21.0
	rarely	38	27.5	27.5	48.6
	sometimes	39	28.3	28.3	76.8
	regularly	32	23.2	23.2	100.0
	Total	138	100.0	100.0	

Forget my Password

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	never	45	32.6	32.6	32.6
	rarely	35	25.4	25.4	58.0
	sometimes	50	36.2	36.2	94.2
	regularly	7	5.1	5.1	99.3
	always	1	.7	.7	100.0
	Total	138	100.0	100.0	

Write down password

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	never	51	37.0	37.0	37.0
	rarely	26	18.8	18.8	55.8
	sometimes	50	36.2	36.2	92.0
	regularly	11	8.0	8.0	100.0
	Total	138	100.0	100.0	

Choose good passwords

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	never	18	13.0	13.0	13.0
	rarely	39	28.3	28.3	41.3
	sometimes	42	30.4	30.4	71.7
	regularly	26	18.8	18.8	90.6
	always	13	9.4	9.4	100.0
	Total	138	100.0	100.0	

Changing password-frequency

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	never	27	19.6	19.6	19.6
	rarely	48	34.8	34.8	54.3
	sometimes	43	31.2	31.2	85.5
	regularly	14	10.1	10.1	95.7
	always	6	4.3	4.3	100.0
	Total	138	100.0	100.0	

Using same password

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	never	10	7.2	7.2	7.2
	rarely	23	16.7	16.7	23.9
	sometimes	40	29.0	29.0	52.9
	regularly	45	32.6	32.6	85.5
	always	20	14.5	14.5	100.0
	Total	138	100.0	100.0	

Opening interesting mail

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	never	9	6.5	6.5	6.5
	rarely	19	13.8	13.8	20.3
	sometimes	53	38.4	38.4	58.7
	regularly	51	37.0	37.0	95.7
	always	6	4.3	4.3	100.0
	Total	138	100.0	100.0	

Leaving logged on computer

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	never	8	5.8	5.8	5.8
	rarely	34	24.6	24.6	30.4
	sometimes	54	39.1	39.1	69.6
	regularly	38	27.5	27.5	97.1
	always	4	2.9	2.9	100.0
	Total	138	100.0	100.0	

Ignore warnings from browser

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	never	15	10.9	10.9	10.9
	rarely	21	15.2	15.2	26.1
	sometimes	52	37.7	37.7	63.8
	regularly	44	31.9	31.9	95.7
	always	6	4.3	4.3	100.0
	Total	138	100.0	100.0	

Allow someone to use my logged on computer

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	never	9	6.5	6.5	6.5
	rarely	15	10.9	10.9	17.4
	sometimes	57	41.3	41.3	58.7
	regularly	52	37.7	37.7	96.4
	always	5	3.6	3.6	100.0
	Total	138	100.0	100.0	

Receive IT training

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	never	78	56.5	56.5	56.5
	rarely	26	18.8	18.8	75.4
	sometimes	23	16.7	16.7	92.0
	regularly	6	4.3	4.3	96.4
	always	5	3.6	3.6	100.0
	Total	138	100.0	100.0	

Refer to IT policy

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	never	47	34.1	34.1	34.1
	rarely	47	34.1	34.1	68.1
	sometimes	23	16.7	16.7	84.8
	regularly	9	6.5	6.5	91.3
	always	12	8.7	8.7	100.0
	Total	138	100.0	100.0	

APPENDIX L

```
CROSSTABS
  /TABLES=Qualific PeriodIS ITSkills PaswrdsA PaswrdsB PaswrdsC PaswrdsD PaswrdsE P
aswrdsF SocailEng1 Carelesness1 Carelesness2 Care
   lesness3 SecTraining1 SecTraining2 BY Category
  /FORMAT=AVALUE TABLES
  /CELLS=COUNT
  /COUNT ROUND CELL.
```

Crosstabs

[DataSet1] H:\Final project dataset\combined all grps for comon variables.sav

Case Processing Summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Highest Qualification * Category of respondent	137	99.3%	1	.7%	138	100.0%
Time of using Info Sys * Category of respondent	134	97.1%	4	2.9%	138	100.0%
Rate of IT skills * Category of respondent	138	100.0%	0	.0%	138	100.0%
Sharing Password * Category of respondent	138	100.0%	0	.0%	138	100.0%
Forget my Password * Category of respondent	138	100.0%	0	.0%	138	100.0%
Write down password * Category of respondent	138	100.0%	0	.0%	138	100.0%
Choose good passwords * Category of respondent	138	100.0%	0	.0%	138	100.0%
Changing password-frequency * Category of respondent	138	100.0%	0	.0%	138	100.0%
Using same password * Category of respondent	138	100.0%	0	.0%	138	100.0%
Opening interesting mail * Category of respondent	138	100.0%	0	.0%	138	100.0%
Leaving logged on computer * Category of respondent	138	100.0%	0	.0%	138	100.0%

Ignore warnings from browser * Category of respondent	138	100.0%	0	.0%	138	100.0%
Allow someone to use my logged on computer * Category of respondent	138	100.0%	0	.0%	138	100.0%
Receive IT training * Category of respondent	138	100.0%	0	.0%	138	100.0%
Refer to IT policy * Category of respondent	138	100.0%	0	.0%	138	100.0%

Highest Qualification * Category of respondent Cross tabulation

Count

		Category of respondent					
		cut	uz	library endusers	library staff	database users	Total
Highest Qualification	Advanced	17	19	21	0	0	57
	Certificate	13	1	0	0	4	18
	Diploma	9	1	2	7	12	31
	Degree	0	15	11	1	4	31
Total		39	36	34	8	20	137

Time of using Info Sys * Category of respondent Cross tabulation

Count

		Category of respondent					
		cut	uz	library end users	library staff	database users	Total
Time of using Info Sys	0-1 yr	0	7	14	0	0	21
	1-2 yrs	36	11	13	0	6	66
	more than 2 yrs	3	13	3	1	10	30
	more than 5 yrs	0	5	1	7	4	17
Total		39	36	31	8	20	134

Rate of IT skills * Category of respondent Cross tabulation

Count

		Category of respondent					
		cut	uz	library end users	library staff	database users	Total
Rate of IT skills	struggle a lot	9	2	0	0	0	11
	below average	15	16	13	0	0	44
	average	13	15	20	5	8	61
	good	2	3	2	3	11	21
	very good	0	0	0	0	1	1
Total		39	36	35	8	20	138

Sharing Password * Category of respondent Cross tabulation

Count

		Category of respondent					
		cut	uz	library end users	library staff	database users	Total
Sharing Password	never	2	5	5	5	12	29
	rarely	7	12	10	2	7	38
	sometimes	13	10	15	0	1	39
	regularly	17	9	5	1	0	32
Total		39	36	35	8	20	138

Forget my Password * Category of respondent Cross tabulation

Count

		Category of respondent					
		cut	uz	library end users	library staff	database users	Total
Forget my Password	never	6	11	12	6	10	45
	rarely	7	10	9	0	9	35
	sometimes	21	13	13	2	1	50
	regularly	4	2	1	0	0	7
	always	1	0	0	0	0	1
Total		39	36	35	8	20	138

Write down password * Category of respondent Cross tabulation

Count

		Category of respondent					
		cut	uz	library end users	library staff	database users	Total
Write down password	never	9	12	17	8	5	51
	rarely	6	7	5	0	8	26
	sometimes	16	15	13	0	6	50
	regularly	8	2	0	0	1	11
Total		39	36	35	8	20	138

Choose good passwords * Category of respondent Cross tabulation

Count

		Category of respondent					
		cut	uz	library end users	library staff	database users	Total
Choose good passwords	never	8	4	4	2	0	18
	rarely	12	14	9	1	3	39
	sometimes	12	8	15	1	6	42
	regularly	6	5	5	0	10	26
	always	1	5	2	4	1	13
Total		39	36	35	8	20	138

Changing password-frequency * Category of respondent Cross tabulation

Count

		Category of respondent					
		cut	uz	library end users	library staff	database users	Total
Changing password-frequency	never	10	5	5	3	4	27
	rarely	11	14	12	1	10	48
	sometimes	12	10	15	3	3	43
	regularly	4	5	2	1	2	14
	always	2	2	1	0	1	6
Total		39	36	35	8	20	138

Using same password * Category of respondent Cross tabulation

Count

		Category of respondent					
		cut	uz	library end users	library staff	database users	Total
Using same password	never	1	3	2	4	0	10
	rarely	6	7	6	2	2	23
	sometimes	14	9	15	0	2	40
	regularly	15	12	9	1	8	45
	always	3	5	3	1	8	20
Total		39	36	35	8	20	138

Opening interesting mail * Category of respondent Cross tabulation

Count

		Category of respondent					
		cut	uz	library end users	library staff	database users	Total
Opening interesting mail	never	1	0	2	3	3	9
	rarely	1	4	1	2	11	19
	sometimes	10	15	22	2	4	53
	regularly	22	16	10	1	2	51
	always	5	1	0	0	0	6
Total		39	36	35	8	20	138

Leaving logged on computer * Category of respondent Cross tabulation

Count

		Category of respondent					
		cut	uz	library end users	library staff	database users	Total
Leaving logged on computer	never	1	2	1	3	1	8
	rarely	5	6	5	3	15	34
	sometimes	17	13	18	2	4	54
	regularly	14	13	11	0	0	38
	always	2	2	0	0	0	4
Total		39	36	35	8	20	138

Ignore warnings from browser * Category of respondent Cross tabulation

Count

		Category of respondent					
		cut	uz	library end users	library staff	database users	Total
Ignore warnings from browser	never	0	1	3	5	6	15
	rarely	3	1	6	2	9	21
	sometimes	17	17	13	0	5	52
	regularly	14	16	13	1	0	44
	always	5	1	0	0	0	6
Total		39	36	35	8	20	138

Allow someone to use my logged on computer * Category of respondent Cross tabulation

Count

		Category of respondent					
		cut	uz	library end users	library staff	database users	Total
Allow someone to use my logged on computer	never	2	3	2	2	0	9
	rarely	5	2	2	5	1	15
	sometimes	12	13	17	1	14	57
	regularly	16	17	14	0	5	52
	always	4	1	0	0	0	5
Total		39	36	35	8	20	138

Receive IT training * Category of respondent Cross tabulation

Count

		Category of respondent					
		cut	uz	library end users	library staff	database users	Total
Receive IT training	never	39	16	13	3	7	78
	rarely	0	6	8	0	12	26
	sometimes	0	10	9	3	1	23
	regularly	0	4	1	1	0	6
	always	0	0	4	1	0	5
Total		39	36	35	8	20	138

Refer to IT policy * Category of respondent Cross tabulation

Count

		Category of respondent					
		cut	uz	library end users	library staff	database users	Total
Refer to IT policy	never	11	7	11	3	15	47
	rarely	28	10	5	0	4	47
	sometimes	0	12	9	1	1	23
	regularly	0	2	6	1	0	9
	always	0	5	4	3	0	12
Total		39	36	35	8	20	138

APPENDIX M

```
ONE-WAY ANOVA
GET
  FILE='H:\Dissertation Mary\Documentation-thesis\Appendices\Appendix K-
combined responses.sav'.
DATASET NAME DataSet0 WINDOW=FRONT.
ONEWAY Qualific PeriodIS ITSkills PaswrdsA PaswrdsB PaswrdsC PaswrdsD PaswrdsE Pa
swrdsF SocailEng1 Carelesness1 Carelesness2 Careles
   ness3 SecTraining1 SecTraining2 BY Category
  /MISSING ANALYSIS.
```

Onaway

[DataSet1] H:\Dissertation Mary\Documentation-thesis\Appendices\Appendix K-combined responses.sav

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
Highest Qualification	Between Groups	26.571	4	6.643	4.983	.001
	Within Groups	175.969	132	1.333		
	Total	202.540	136			
Time of using Info Sys	Between Groups	40.481	4	10.120	20.172	.000
	Within Groups	64.720	129	.502		
	Total	105.201	133			
Rate of IT skills	Between Groups	32.302	4	8.076	15.959	.000
	Within Groups	67.299	133	.506		
	Total	99.601	137			
Sharing Password	Between Groups	45.540	4	11.385	13.669	.000
	Within Groups	110.779	133	.833		
	Total	156.319	137			
Forget my Password	Between Groups	21.133	4	5.283	6.545	.000
	Within Groups	107.360	133	.807		
	Total	128.493	137			

Write down password	Between Groups	20.637	4	5.159	5.663	.000
	Within Groups	121.168	133	.911		
	Total	141.804	137			
Choose good passwords	Between Groups	14.788	4	3.697	2.886	.025
	Within Groups	170.379	133	1.281		
	Total	185.167	137			
Changing password-frequency	Between Groups	1.516	4	.379	.335	.854
	Within Groups	150.629	133	1.133		
	Total	152.145	137			
Using same password	Between Groups	24.840	4	6.210	5.492	.000
	Within Groups	150.377	133	1.131		
	Total	175.217	137			
Opening interesting mail	Between Groups	40.199	4	10.050	15.743	.000
	Within Groups	84.902	133	.638		
	Total	125.101	137			
Leaving logged on computer	Between Groups	29.380	4	7.345	10.794	.000
	Within Groups	90.504	133	.680		
	Total	119.884	137			
Ignore warnings from browser	Between Groups	54.580	4	13.645	19.257	.000
	Within Groups	94.239	133	.709		
	Total	148.819	137			
Allow someone to use my logged on computer	Between Groups	15.790	4	3.947	5.192	.001
	Within Groups	101.116	133	.760		
	Total	116.906	137			
Receive IT training	Between Groups	41.212	4	10.303	11.131	.000
	Within Groups	123.107	133	.926		
	Total	164.319	137			

Refer to IT policy	Between Groups	46.334	4	11.584	9.561	.000
	Within Groups	161.144	133	1.212		
	Total	207.478	137			