ADDIS ABABA UNIVERSITY
COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES
SCHOOL OF INFORMATION SCIENCE

ASSESSING THE EFFECT OF HUMAN ERROR FACTORS TO CBE INFORMATION SECURITY

MIHRET SETU

JANUARY, 2020

ADDIS ABABA, ETHIOPIA

ADDIS ABABA UNIVERSITY
COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES
SCHOOL OF INFORMATION SCIENCE

ASSESSING THE EFFECT OF HUMAN ERROR FACTORS TO CBE INFORMATION SECURITY

By: Mihret Setu
Advisor: Dereje Teferi (PhD)

A Thesis Submitted to the College of Natural and Computational Sciences of Addis Ababa University as a Partial Fulfilment of the Requirements for the Degree of Master of Science in Information Science

January, 2020
Addis Ababa,
Ethiopia

Name and signature of Members of the Examining Board

Name	Title	Signature	Date
Dereje Teferi (PhD)	Advisor	_____	_____
_____	Examiner	_____	_____
_____	Examiner	_____	_____

DECLARATION

I Mihret Setu, declare that the work presented in this thesis entitled “Assessing the effect of human error factors to CBE information security” is my original work. It is done and presented under the guidance of my advisor Dr Dereje Teferi. This thesis has not been presented for any scholastic achievement in any University and all materials used in this study are fully acknowledged.

Signature _____

Date _____

Mihret Setu

This thesis has been submitted for examination with my approval as university advisor.

Dr Dereje Teferi

Signature _____

Date _____

ACKNOWLEDGEMENTS

I am very grateful to *CBE* for giving me an opportunity to conduct my study. I would like to thank Dr. Dereje, and Ato Yibarek Tesfaye for assisting me during my studies in all aspects during the course of the research. During my research work, I collaborated with my colleagues and friends in various Banks and Organizations to whom I wish to express my sincere gratitude. Above all, I want to thank God Almighty and my family for supporting me in my research and for giving me the greatest joy of my life. Finally, I would also like to thank all the staff at the CBE, especially Information Security Manager, Ato Yitbarek Tesfaye.

Mihret Setu

Table of Contents Page

LIST OF TABLES

LIST OF FIGURES AND GRAPHS

LIST OF ACRONYMS

ANLU: Assessed Nominal Likelihood of Unreliability

APC: Alternative Payment Channel

APOA: Assessed Proportion of Affect

CBE: Commercial Bank of Ethiopia

CU: Relative Percentage Contribution to Unreliability

EPC: Error producing conditions

GISAT: General information security affecting tasks

GTT: Generic Tasks Types

HEART: Human Error Assessment and Reduction Technique

HR: Human Resources

HRA: Human Reliability Analysis

HTA: Hierarchical Task Analysis

IS: Information System

IS-CHEC: Information security core human error causes

SOC: Security Operation Center

TS: Trade Services

ABSTRACT

Humans have been known as the weakest link within information security chain. Organizations often face information security incidents as a result of human error mostly because they tend to emphasise and invest on technical security controls rather than the human factor. However, organizations have begun to show interest towards improving their security regarding the human element or their employees. In recognizing this fact, a lot of attempts have been done. This includes incident responses and training of employees. There are at least two categories of practices for securing the human factor. The first category is a retrospective approach which involves review of previous incidents and determining the root cause of the incident in terms of human error. And the second category is a prospective approach which assigns quantitative probabilities to identify high risk sections. The latter is used to implement solutions to mitigate the high risk tasks and few researchers studied on this area. Evaluation of the current state is the first step towards improving the approach.

The purpose of this research is to identify the factors causing human errors within CBE regarding information security. This is followed by a literature review of human errors in information security. The paper also discusses the role of human factors and how the information security research community has recognised the increasingly crucial role of human behaviour in many security failures.

The research was conducted as a case study within a public financial sector organization, CBE. In the case study, HEART, one of Human Reliability Analysis (HRA) method is applied to selected divisions of the bank.

In order to keep validity, pilot test on the checklist questions for the semi-structured interview is done by selected respondents before data collection began. The feedback was used to update the contents. The study involved 45 interviewees out of 63 potential interviewees from different roles including branch operations officers, system administrators, IT officers, finance officers and managers, and quality and process officers. After assessing the current state of the bank concerning human factor information security, the most unreliable tasks in the bank were human resources, finances and branch offices. Divisions with relatively high human involvement have shown significant error probability. Accordingly, human resource is predicted to be the most probable office for human error with the probability of failure being 0.058. System information confirmation /feedback inadequacy contributes the highest among the factors for error which is 40.91% within human resource division. In general operator inexperience, highly repetitive tasks and delayed or unclear system confirmation are projected to be the top causes or factors for human error in the bank. This is mainly attributable to the lack of attention given to the soft factors that impact any employee activity by higher managers. In order to minimize the effects that take advantage of those

factors the researcher give improvement area recommendation based on exhaustive literature review and practiced HEART remedial/preventive measures. The research targets are stakeholders, individuals who are in charge of securing the assets of their organizations and institutions. Among the top error producing factors prolonged & repetitive activities, inexperienced person performing at the bank and inadequacy system feedback showed high probability to errors.

Key words: *Human error, Human Error Assessment and Reduction Technique, Human Reliability Analysis (HRA), Human Based Information Security*

CHAPTER ONE

INTRODUCTION

1.1 Overview

The Digital Age is transforming organizations to innovate and apply new technology and infrastructure. This causes the connectivity and dependency on digital systems. Organizations, authorities, individuals, and operations are still at risk.

The human element is playing an ever-increasing role in information security and certainly the current set of international standards and best practices is not comprehensive enough to make it secure (von Solms & van Niekerk, 2013). Within the Global Finance sector there is increasing recognition of the role that human error plays in compounding incidents in terms of financial risk, process delays, organizational security and reputation and in terms of employee motivation and retention. In particular, human error that results in an information security incident can lead to consequences far wider than a single organization.

Organizations have implemented suitable information security solutions; components of such an information security solution and its management involve processes, technology and people. Unfortunately, many of these information security solutions are innately flawed (Alnatheer & Nelson, 2009). Although processes and technologies can be created to be theoretically secure, how truly secure they are depends on the people involved in their use and implementation (Furnell & Thomson, 2009). The efficiency of different technical security controls is based on people who interact with the information daily. An understanding of human behavioural aspects is required in order to improve the security of information assets.

It was indicated that technology was less likely to cause problems than a human error, which is a cause of the majority of breaches in security, 75% of organizations were revealed to suffer security breaches by insiders (Information Security Breaches Survey, 2015). It has also been captured in research that organizations routinely overlook human error as a major cause of security breaches and prioritise their attention on their technical controls (Liginlal et al, 2009). The IBM X-Force Threat Intelligence Index 2017 (Alvarez et al, 2017) found that the financial services and healthcare industries suffered 53% and 46% respectively of incidents that related to inadvertent insiders. Kelly (2017) stated that almost 90% of cyber-attacks are caused by human error. Several researches have shown that most of information security cases relate to human fault (The Inquirer, 2017, Evans et al, 2016, Kelly, 2017, Insurance Times, 2014).

Current information security research into human error utilising established mechanisms such as Human Reliability Analysis (HRA) is limited with little empirical validation of proposed techniques and frameworks (Gertman, 2013; Goodliff & Widdowson, 2015). Researchers have identified the needs of causal socio-organizational analysis approaches, such as the utilisation of HRA, to determine human errors in the workplace (Maddah & Ghasemi, 2015). However, these approaches are not being utilised by organizations to feed into preventative risk management practices and therefore reduce or prevent the occurrence of human error related information security incidents. HRA is a technique typically used in high reliability sectors such as rail, aviation and energy areas to identify and solve the human contribution to risk (Bell & Holroyd, 2009) and prevent human error events which affect the successful completion of tasks as intended. HRA can therefore enable an organization to implement specific remedial and preventative measures to mitigate performance shaping factors or error producing conditions that could lead to information security incidents and breaches. Although researchers have identified the need to apply HRA in the information security area, there is little empirical research found on using HRA approaches to analyse the information security incidents (Gertman, 2013). Hence, there is a need for a systematic approach, such as HRA, to analyse human error related incidents within information security. The depth of published data with regard to human error related information security incidents is limited in that human error is treated as a binary yes or no rather than delving in to the causal factors of the incident. There is a need of a systematic approach to capture human errors in organizational risk and incident registers. The approach should be able to both reactively, through incident management, and proactively, through risk management, identify causal factors that have, or could lead to, information security incidents as part of the undertaking of associated tasks. An organization could therefore apply the relevant remedial preventative measures to resolve incidents or prevent incidents occurring to both reactively, through incident management, and proactively, through risk management, identify causal factors that have, or could lead to, information security incidents as part of the undertaking of associated tasks. An organization could therefore apply the relevant remedial preventative measures to resolve incidents or prevent incidents occurring.

The primary motivation for this paper is to address the above-mentioned challenges by applying a HRA approach called Human Error Assessment and Reduction Technique (HEART) to analyse human error issues proactively through task classification and expert evaluation of factors. Numerous HRA approaches have been proposed in the literature. For the purpose of this work, HEART has been adapted based on existing documentation for HEART (Williams, 1992). HEART has been selected as the preferred base for the proposed approach because it enables to assess the human error roots in a comprehensive manner which has been empirically validated in other

industry areas. In addition, HEART can also be used for the retrospective review of incidents as well as part of probabilistic risk assessment due to the fact that it can be used to establish the predicted likelihood of human error in completing a task as intended. This likelihood calculation is termed the human error probability (HEP). It is also a generic technique that is applicable to information security as well as other areas which requires only limited experience and resources to apply.

This research also discusses what constitutes a human error related information security incidents, and presents HEART as a HRA technique that can be utilised effectively within the information security area including undertaking an assessment of information security incorporated into preventative risk management practices.

Published research has also asserted that current incident learning activities are focused on technical aspects and that in order to increase the learning outcome from incidents organizations should invest greater resource to reveal underlying causes (Tøndel et al, 2014).

A financial institution is responsible for the supply of money to the market through the transfer of funds from investors to the companies in the form of loans, deposits, and investments. Therefore, in order for the bank to identify, recognize and address the human error factors behind information security incidents we need a systematic method to analyse human errors which could be integrated into Information security culture.

This research used HEART to proactively identify error causal factors that could lead to information security incidents as part of the undertaking of associated tasks/roles. Recent work by different authors suggested that HEART could potentially be applied in the information security area (Evans et al, 2016). In light of the foregoing discussion, the authors determined that HEART could be easily applied in any environment and especially could provide benefits in determining the factors influencing the successful completion of tasks more vulnerable to human error.

Safety science research aid in understanding why information system operators do not act in accordance with with information security controls (Young & Leveson, 2013). Lawton (1998) gave emphasis to rule abuses and the stimuluses given by violators. He determined that mostly violations happened involuntarily as staffs were devoted to finishing the assignment (Lawton, 1998). Time burden, load of work, and consuming a “faster way of operating” were some of the human factor matters that effect the engagement in unsafe actions by staffs (Lawton 1998, Young & Leveson, 2013). Human participation in securing information is too important for organizational leaders to continue to overlook the impact of psychology-based experts to examine the human activities in

information security (National Security Agency, 2015). In particular, there is a lack of empirical research in the field of information security and human errors.

Researchers have identified the needs of causal socio-organizational analysis approaches, such as the utilization of Human Reliability Analysis (HRA), to determine human errors in the workplace (Maddah & Ghasemi, 2015). A research by (Evans et al, 2015) identified that it is essential that HRA be applied within the information security area and that an appropriate HRA technique (specifically HEART) be selected using an approach that will be fit to an information security situation. Besides it is a generic technique that is applicable to information security as well as other areas which requires only limited experience and resources to apply.

1.2 Statement of the problem

The security research community has recognised that human behaviour has a crucial role in many security failures. In information security literature, humans are often referred to as the weakest link in the security chain. Although human behaviour and resulting errors often facilitate security breaches; the issue is not adequately addressed by many current security models.

Most report indicate that half of substantial security events happening are caused by a certain element, individuals. (Ahmad et al, 2012) concluded that trends in information security incident response placed an imbalanced focus on technical aspects and did not incorporate holistic socio-organizational perspectives. Most common information security incidents connect to human error (Evans et al., 2017; Kelly R., 2017; The Inquirer, 2017). Many security experts are unaware of science of human factors besides they associate human fault to a training and awareness topic which is a misconception (National Security Agency, 2015).

People and computer users are the center of the security concept and that the significance of human aspects in the field of information security should not be simple (Safa et al., 2016). Current human factors information security research places an imbalanced focus on intentional actions rather than unintentional human error (Rajamaki et al., 2018). Information systems and human behaviour related researches predominantly address the problem of intentional violations and non-compliances (Boss et al., 2009; Bulgurcu et al., 2010; Ifinedo, 2014; Puhakainen & Siponen, 2010; Hovav et al., 2012) resulting in proportionally limited work relating to unintentional human error (Djajadikerta et al., 2015; Kankanhalli et al., 2008). Therefore, there are limited published works researching human error and how it affects information security. Published researches appears to be theoretical using techniques such as surveys (Furnell et al., 2018) rather than empirical validation based on techniques including interviews or action research and case studies.

Johannesen et al. (2010) stated that nearly 90% of cyber-attacks are triggered by human fault. He also presented that human error is the consequence rather than the cause of information security incidents. He (2014) identified that incident response often focuses on solving the direct cause of the incident rather than investigating the in-depth cause which is often not a technical problem. Human factors present a threat to availability of information through the unauthorised alteration of sensitive information as a result of error, oversight, tiredness, incompetency, stress and so on. Information system incidents often happen when a security measure has been used that is technically adequate but blind to human behaviour. For example, password validation policies commission people to choose a complex password. Such a password would likely be a combination of letters with at least one letter capitalised and digits that some users may find difficult to remember. As a result, people write down their passwords in unsecure places.

Current measures fail detecting the factors of human error associated to information security incidents. Trends in information security incident response placed an imbalanced focus on technical aspects and did not incorporate holistic socio-organizational perspectives (Ahmad, 2012). Similarly researches show that current incident learning activities are absorbed on technical pieces and that in order to increase the learning result from incidents organizations should devote greater resource to reveal underlying causes (Tøndel et al., 2014). This was due to the lack of a comprehensive and structured framework to establish the fundamental causal factors of human error related information security incidents and their associated probability of occurrence through validated methods. (Schultz et al., 2005) indicated the shortage of professionals and researches of information security within human factors. They highlighted the significance of considering the influence of the work surroundings and culture on staffs engaged in both productive and appropriate security-oriented conducts. Accordingly, human activity has often been disregarded within information security study and organizational business approach.

A review concluded that there is little work that moulds technical security issues with a wider Human computer interaction (HCI) perspective, particularly in the areas of theories, models and frameworks (Dhillon and Backhouse, 2001). In particular, there is a lack of empirical research in the field of information security and human errors. One possible reason for this could be due to organizational unwillingness to share information and statistics on security. However, research in this area is important because user concern for information privacy has the potential to affect the future of e-commerce.

Cybercriminals attentively take advantage of connected systems, technological vulnerabilities, human errors, and unprepared organizations. According to (Keely, 2017), most common cyber threats are phishing, spyware, ransom ware and Trojans. Threats are rising as malicious cyber

actors are seeking to compromise credentials. The top three threat vectors are email links and attachments, web-based download, and application vulnerability (Keely, 2017).

Woretaw and Lessa (2012) explained information security awareness in the Ethiopian banking as unsatisfactory. Consequently, the level of proper information security governance in the banking sector in Ethiopia is a critical area of improvement. Negussie (2015) also stated that information security issue is not only a problem that technology can address alone but also a problem of a management to solve. The study revealed that there is no as such common Information security governance standard within the banking industry of Ethiopia. Therefore, in order for the information security field to identify, understand and address the human error factors behind information security incidents, we need a systematic method to examine human errors. Therefore, this approach can enable an organization to implement specific counteractive and preventative measures to mitigate routine shaping factors or error producing conditions that could lead to information security incidents and breaches. Even though researchers have recognized the need to apply this approach, it is not being used to address cyber security which could reduce risk within a risk-based approach (Gertman, 2013).

Hence, the primary focus of this research is to identify causes for human error and contribute to the reduction of human error leading to information security incident at CBE.

1.3 Research questions

The purpose of this study is to identify tasks and factors for human error leading to information security incident in CBE through answering the following research questions: -

1. How does commercial bank of Ethiopia addresses information security towards human error?
2. Which tasks cause humans/employees of CBE make errors leading to information security incident?
3. What are the factors with high risk for tasks in research question 2?

1.4 Objective of the study

1.4.1 General Objective

The general objective of the study is to identify factors of human error for information security incident at CBE using a human reliability analysis method.

1.4.2 Specific Objectives

To achieve the above general objective, the following specific objectives are addressed in the research work.

- Review conceptual and empirical literature to understand different models in information security models and identify the research gap.
- Identify procedures currently designed for information security towards human error at CBE.
- Compare methods used for human error analysis in the literature to select the best approach for the study
- Identify sources for human error at CBE in relation to the selected method
- Provide conclusion and recommendation

1.5 Scope and Limitation

This research focuses on a single case study research, which is bound only in one organization, CBE. The study doesn't include causes for intentional information security incidents caused by insiders or employees of the bank. This research does not cover each division within the bank but the ones which are believed to be susceptible for human error leading to information security incident. As a result of time and budget scarcity, the study will be conducted on sample divisions which are believed to be error-prone and with record of frequent incident report. The rational for the selection of those divisions and individuals is further discussed in chapter 3. As the title implies the scope of this study is limited to assessing the human error aspect which endangers the bank's information security.

1.6 Significance of the study

The study has a significant contribution for both academic researchers and practitioners. Academic researchers would benefit from the theoretical contribution as the research would try to fill the current literature gap mainly on human based information security for banks context and also in general. The Bank information security directory is the primary expert that will use the proposed platform as a guide to make information security risk assessments and strengthen the bank security stance. It also serves as a point of reference for practitioners and researchers who want to conduct more research in information security area in Ethiopian banks.

1.6 Organization of the thesis

Including this introductory chapter, this thesis comprises five chapters. Chapter one gives general introduction for the study and state about research problem, research questions, objective of the research, significance along with scope and limitation of the study. Chapter two is dedicated to present the ideas found on the previous literatures. Basically this chapter present definition of human error, information security incidents of human error, system approach, HEART and related work. Finally gaps on the literature are reported. Chapter three present the methodology used in this research. It describes research approach and methods along with justification. In addition, this chapter states the techniques used to analyse the data and present how study validation and reliability of the study is taken. Chapter four, report the analysis of both qualitative and quantitative study along with findings. After the study findings are triangulated, detail discussions are presented. The last chapter present conclusion and future research recommendation by acknowledging the research limitations.

CHAPTER TWO

LITERATURE REVIEW

2.1 Overview

The main goal of this chapter is to review related literature in Information Security regarding human based factors that could cause incidents or breaches as a result of a certain task any employee is performing. This chapter offers background information and reviews related works which are relevant for this research. It involves the concepts of information security, human factors, business and organizational oriented issues. This chapter also discusses the theories and existing state-of-the-art works around HRA.

A literature review is a method of identifying, interpreting and evaluating all available research sources relevant for a specific research question or topic area. The researcher follows a list of keywords, including Information Security, Information Security related human error HRA, Human error are used to search through widely familiar database sources such as ACM, IEEEXplore, and Google Scholar.

2.2 What is Information security?

The Federal information security management act (FISMA) defines the relation between information security and the CIA threesome as follows. The term "information security" means protecting information as well as information systems from unofficial access, usage, discovery, interruption, alteration in order to provide three pillars of information security.

A) Integrity: guarding against improper information modification or destruction, and includes ensuring information non repudiation, accuracy, and authenticity;

B) Confidentiality: preserving authorized restrictions on access and disclosure, including a means for protecting personal privacy and proprietary information; and

C) Availability: ensuring timely and reliable access to, and use of, information.

Integrity: is the protection of information, processes, or systems from intentional or accidental unauthorized modification. In the same way we count on people to behave a certain way, we rely on our information to be a certain way. Data integrity is a requirement that information and programs are changed only in a specified and authorized manner. System integrity is a requirement that a system "performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system. *Errors* and omission are an important threat to data and system integrity. These errors could be caused by data entry clerks processing hundreds

of transactions per day. Even the most sophisticated programs cannot detect all types of input errors or omissions. In some cases, the error is the threat, such as a data entry error or a programming error that crashes a system. In other cases, the errors create vulnerabilities. Integrity and confidentiality are interrelated. If a user password is disclosed to the wrong person, that person could in turn manipulate, delete, or destroy data after gaining access to the system with the password he obtained. Many of the same vulnerabilities that threaten integrity also threaten confidentiality. Most notable, though, is human errors.

Confidentiality: As it pertains to information security, confidentially is the protection of information from unauthorized people and processes. The information security goal of confidentiality is to protect information from unauthorized access and misuse. The best way to do this is to implement safeguards and processes that increase the work factor and the chance of being caught. This calls for a spectrum of access controls and protection as well as ongoing monitoring, testing, and training.

Availability: The final component of the CIA triad is also most often left out of consideration when one thinks about security. Availability is the assurance that systems and data are accessible by authorized users when needed. If we can't access the data need, when needed, it is not secure. Threats to availability include loss of processing ability due to natural disasters; hardware failures; programming errors; human errors; injury, sickness, or death of key personnel; distributed denial of service (DDoS) attacks; and malicious code. Kruger (2006) defines information security as the protection of the confidentiality, integrity, and availability of computerized data and of the systems that process, maintain and report these data; during processing, storage and dissemination of output. As with other business assets, information requires protection to ensure that it is available and confidential and that its integrity is preserved where necessary (Pfleeger,1997). Information security is about implementing adequate controls to protect information assets. Controls cover a wide spectrum of technology such as firewalls, processes such as change management, and human elements such as information security induction training.

2.2.1 Information Security Incident Definition

There are numerous examples of standards and published materials that define what constitutes an information security incident. These definitions all vary depending on their particular focus. ISO/IEC 27,000 (The British Standards Institution, 2017) defines an information security incident as a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security through the preservation of confidentiality, integrity and availability. The Information Commissioner's Office

(ICO) (Information Commissioner's Office, 2012) does not explicitly define an information security incident but outlines that organizations must protect themselves through appropriate technical and organizational measures against unauthorised or unlawful processing, accidental loss, destruction of or damage to personal data in accordance with the seventh data protection principle. The Government National Cyber Security Strategy (HMG, 2016) defines an incident as actual or potential occurrences of an adverse cyber event that may compromise or cause harm to a system or network. The UK National Cyber Security Center (National Cyber Security Center, 2017) further expands upon this definition as a rupture of a system's security policy to alter its reliability or accessibility or any unauthorised access or attempted of access to a system.

In Healthcare, the NHS Information Governance Toolkit (NHS Digital, 2017) makes some minor amendments to the ISO27000 definition where the term 'failure of controls' is replaced with 'failure of safeguards'. Supporting NHS guidance on reporting, managing and investigating information governance and cyber security incidents (HSCIC, 2015) defines an information governance serious incident requiring investigation (SIRI) to be a breach of the Data Protection Act, or the Common Law Duty of Confidentiality including the unlawful disclosure or misuse of confidential data, recording or sharing of inaccurate data, information security breaches and invasion of people's privacy. The Payment Card Industry Data Security Standard (PCI Security Standards Council, 2016) takes a different approach for the finance area and adopts the terms compromise, data compromise or data breach in relation to an information security incident and defines this as an intrusion into a computer system where unauthorized disclosure/theft, modification, or destruction of cardholder data is suspected.

2.3 Human role in Information Security

Within the computer information security industry, much attention is often focused on technical aspects with some organizations viewing technical solutions as a direct answer to their information security problems. Human error-related information security incident is defined as 'an 'active failure' by a person (the threat) performing an 'intentional action' resulting in the failure to complete a task as intended or achieve the desired outcome due to the exploitation of a 'latent condition' (the vulnerability) leading to a compromise or breach of information confidentiality, integrity or availability or associated law through the failure of technical or organizational safeguards causing disruption to business operations or causing harm or distress to individuals including breaches of privacy (Evans et al., 2019). Although security technologies such as firewalls, antivirus software, and VPNs are valuable weapons in an organization's information security weapon mass, pursuing a purely technological approach presents severe disadvantage.

Resolving information security difficulties without constant human collaboration even with the best technology cannot succeed.

Common cases of incorrect uses of technology are making unofficial reconfiguration of systems, sharing of passwords, discovering inappropriate information. Additionally, using the incorrect email address, attaching the wrong file, or transmission over insecure channels, allowing access to data by losing hard copies of sensitive reports, failing to password-protect or log off a computer, and circumventing or failing to use firewalls. Criminals look for and are prepared to exploit weaknesses in network designs, software, communication channels, and people. The opportunities are plentiful. Criminals are not always outsiders. Insiders can be tempted to "make copies" of information they have access to for financial gain. The ability to obtain unauthorized access is often opportunist. In this context, opportunistic means taking advantage of identified weaknesses.

As far as the risk that malicious insiders cause for their organizations, much of the damage instead relates to simple human fault, unreliable obedience to security policy mostly without knowing it and errors related to behaviours, such as sharing and reusing of password. Ineffective patch management is also among the widely reported accidental/passive risks by employees. Recent survey from Sungard Availability Services indicated that most IT professionals recognize out-of-date security patches as a problematic.

Report from Trend Micro Labs 2014 regarding Web apps emphasised human error and patch management as unreliable layers to security. This study also indicated how Web apps are usually very tailored complicating their standardization across the business and causing vulnerabilities for human error. Human error covers many of the prospects employees could accidentally put their firms at risk of a breach. IBM Security Services 2014 Cyber Security Intelligence Index report gathered data from 1000 of the company's customers and revealed that human error was the reason for 95% of reported cyber security incidents. Most common errors were clicking on a malicious link in an email plus keeping default usernames and passwords, system misconfiguration and poor patch management as well.

Many different terms are used to describe human-centered security, including human-centric security, people-centric security or people-focused security. They all relate to the aim of mitigating or reducing the risk of human error. The Information Security Forum **(**2019) research identified that organizations are struggling to manage the risk of what is called "the accidental insider" the authorized member of staff making accidental errors. Equally, traditional security controls are proving to be less effective at preventing external malicious attacks. Attackers are transitioning away from malware-based attacks to more targeted, social engineering-based attacks designed to coerce or in-

fluence the accidental insider into making exploitable errors. Organizations that are already taking a human-centered approach to information security typically spend extended periods of time observing human interaction with technology, controls and data, to identify which specific cognitive biases are triggered, and understanding why this is the case. This has enabled effective and targeted investment in human-centered security improvement programs which prioritize the highest risk areas. There is, however, insufficient good practice in order to identify which solutions merit more investment than others, so it will depend on the organization, the specific human vulnerabilities that lead to errors in decision making, and the most common types of attacks experienced.

A human-centered approach to security can help organizations to significantly reduce the influence of cognitive biases that cause errors. By discovering the cognitive biases, behavioral triggers and attack techniques that are most common, tailored psychological training can be introduced into an organization's awareness campaigns. Once information security is understood through the lens of psychology, organizations will be better prepared to manage and mitigate the risks posed by human vulnerabilities.

2.4 Human Error

Human error has a history of causing several information security incidents. Between 2017 and 2018 human error was the cause of nearly 90% of data breaches reported according to Kroll (the Information Commissioner's Office (ICO)).Verizon's 2019 Data Breach Investigations Report (DBIR) found human error to be the underlying event in 21% of breaches. Top actions regarded as a human related by Verizon include loss, miss delivery and other types. Schultz, (2005) stated that solutions for securing information should include human error and weak decision making as one of the most important pieces of information security. Human errors can be deliberate or careless. However, some authors such as Kraemer and Carayon (2007) believe that human errors are careless accidental incidents exacerbated by poor ISSs. Their investigation concludes that indirect forces, such as communication and security culture, are the sources of human error. Consequently, ISSs with an extremely high technical backbone can be stumped by human error. In other words, many technical measures can be defeated by errors made by people. Security policies are designed to restrain behaviour in order to eliminate errors.

Human involvement in information security should not be overlooked (National Security Agency, 2015). The lack of researches focused on human behaviour for information security greatly affects the misinterpretation of human decision-making during operation of information system.

According to Kraemer and Carayon (2007) human error factor is labelled as any act causing an uninvited outcome. Dhillon (2003) defines the term human error to be a failure to carry out a

specified job or task which could result in the disruption of scheduled operations. The definition also incorporates the undertaking of a prohibited action which could also lead to the same negative outcome. Johannesen et al. (2010) expand upon this view and argue that human error is a judgement made in understanding and that it represents a symptom rather than a cause. They also suggest that organizations that believe they have a human error problem actually have an organizational or technical problem which presents itself in the form of human error.

In order to prevent human errors from occurring in information security contexts, it is important to identify the different types of human errors and inform users of the possible risks and put in place strategies to avoid them. Within the field of human factors, various models and concepts have been developed for understanding and characterizing various types and levels of human error. These models and concepts have been successfully applied in various industries to analyse the causes of accidents (Reason, 1997). Generic Error Modelling System (GEMS) explores the cognitive mechanisms involved in human error as well as the role of organizational and management factors in the creation of error-prone conditions (Reason, 1990, 1981). This model offers a potential framework for explaining human errors in information security. In GEMS model, mental operations can be in either attentional mode or schematic control mode.

2.4.1 Attentional Mode

This mode is concerned with the consciousness and the working human memory of the user. This type of mode is slow, requires effort and is difficult to sustain for a prolonged period of time. This mode is typically used by humans for tasks such as goal setting, monitoring progress, recovering from errors/mistakes, etc. In the context of security, a user may use this mode for recalling their system logon details such as username / password.

2.4.2 Schematic Control Mode

This mode helps to processes familiar information very quickly. It does not require any conscious effort or great mental exertion. This mode is not limited in terms of the amount or duration of the stored information. Within the various cognitive processing stages, different types and levels of human error may occur.

2.4.3 Categories of Behaviour to Distinguish Types of Error

Researchers argue that human errors may be divided into categories of behaviour based upon an individual's level of performance. The errors could be distinguished by both psychological and situational variables.

- *Skill-based Errors*

These types of errors are made with routine, and are automatic and unconscious. They occur under schematic control mode. Errors of this type are known as slips, unintended actions, or lapses.

- *Rule-based Errors*

This type of behaviour selects and applies formerly stored rules to the information. For most part it is automatic and unconscious. This type of behaviour occurs when a change is needed to modify the automatic behaviour found at the skill-based level. The user may apply a memorised rule with periodic checks to monitor the progress and outcome of the action.

- *Knowledge-based Errors*

This type of behaviour operates under first principles and occurs under attentional control. Knowledge-based behaviour only occurs after repeated failure and without a pre-existing solution.

In general, the majority of errors are likely to be skill-based, not rule- or knowledge-based.

The National Research Council of Computer Science and Telecommunications Board, has distinguished between two main types of human error: *accidental* and *deliberate*. Accidental causes are non-deliberate and unintentional, e.g. a programming error that causes a system to crash. Whilst deliberate causes are referred to as attacks whereby the perpetrator seeks to cause damage deliberately. The model reinforces the fact that humans will always be the weakest link in the overall process. Recently, information security researchers have begun focussing on human errors, producing statistics identifying it as a large component of problems in computer security. The Global Financial Services Industry (GFSI) Security Survey revealed that the majority (86%) of respondents confirm that human error is the leading cause of information systems failure and in the National Institute of Standards and Technology, where 65% of the economic loss attributed to information security breaches was caused by human error, whereas only 3% of the loss was attributed to malicious outsiders. (Deloitte, 2008).

Human errors by computer users cause information security breaches in a variety of ways. These errors could be caused as a result of lack of computer knowledge, technical errors or simply carelessness on the part of the computer users.

In Reason (1990), human error can be put into three classes:

• *Lapses and Slips* are basically the right activities which went wrong. These are the most predictable errors and are usually characterized by inaccurate performances. The characteristic of this error class is that the intention is correct, but the execution is wrong. For example, accessing the firm assets via public Wi-Fi which is usually compromised by intruders.

• *Mistakes* are right actions but under a faulty plan. The characteristic is that the intention is incorrect, which leads to incorrect actions. For example, encrypting a highly sensitive email, but not in the right way, making the message being sent all in the open.

• *Violations*: these errors involve some types of deviation from rules or procedures and consequently, contain a risk-taking element. There are generally three basic types. The first is the routine violation, for example, taking a prohibited shortcut during a procedure or corner-cutting an operation. If there is satisfactory reason for a rule, then it turns publicly intolerable to break the rule. Therefore, a rule rooted in organizational culture is very essential for secure activities. However, following bad rule like rejecting staff's entree to social medias using information security as an excuse violation will prevail as people start to break other rules. First the rule should be fixed before the entire culture is compromised. The second is the situational violation, usually a cause of time or resource limitations which appeals as the only way to carry out a task practically under such situations, for example, staff shortages.

The third is the extreme violation, for example, someone tries to test how far the system can be pushed in a normal operation, or disable security links, etc. Extreme violations may include email received by an employee that looks like as important as the work email. This is a very difficult to foresee since clearly there is no technology that has completely resolved the malicious email trick.

System approach aligns to the case made by Johannesen et al. (2010) in that human errors are the consequence as oppose to the cause. As the human errors are understood to be systemic organizational contextual factors, countermeasures are designed to address the conditions in which humans work and organizational processes. *Latent conditions* can introduce unfortunate effects in the form of error producing conditions such as those captured within the *Human Error Assessment and Reduction Technique (HEART)* (Williams, 1992), or long lasting weaknesses in system defences. When a known activity or customary routine takes over (or captures) an unknown activity, capture errors could happen giving rise to cognitive failures or errors (Norman, 1981) that can result in security breaches. For instance, capture errors can be used to show the truth that people frequently press OK when they know that they should not. In essence, the act of pressing the OK button is so customary and typical that people often abide by this routine without properly bearing in mind the percussions. During times of inattention or tiredness, these errors are typically often. Inattention and tiredness could also cause Post-completion errors in which the individual fails to undertake an important 'clean-up'action that is needed after the chief target has been concluded (Anderson, 2008). For instance, from an information security standpoint, the chief target may consist of sending an email from a secure system. Once that target has been concluded, it is then vital to finish the closing action of logging off the system. A condition where the individual in

question is unable to finish that closing task involves a post-completion error, exposing the system to a probable security infringement.

Five diverse kinds of human factor errors can be used to elaborate on information security breaches as differentiated by Swain and Guttman (1983). First, where people fail to remember to do a required action, there are acts of omission. For example, this could involve the disappointment to often change passwords in an information security domain. Second, errors are normally acts of commission, in which people write down a password which is an incorrect procedure or action. Third, doing something pointless involves a number of faults caused by irrelevant acts. Fourth, performing something in an incorrect order involves errors which can be caused by sequential acts. Finally, Swain and Guttman (1983) refer to time errors as triggered by peoples 'failure to perform a task within the stipulated required time.

In general, the majority of human errors could be seen as unintentional. This includes the way in which the individual communicates with a system is connected to accidental human factor errors, and people may come across issues in identifying, comprehending and utilizing the security features (Furnell and Clarke, 2005).

2.5 Information Security Incidents as a result of Human Errors

According to the IBM Chief Information Security Officer Assessment report (2014) 95% of information security incidents involve human error. Information security risk managers and chief information security officers can benefit from the insights of studies on the human factor to reduce human error related to security. Human errors are usually defined as circumstances in which planned actions, decisions or behaviours reduce or have the potential to reduce quality, safety and security. Examples of human error involved in information security include the following:

- System misconfiguration;
- Poor patch management;
- Use of default usernames and passwords or easy-to-guess passwords;
- Lost devices;
- Disclosure of information via an incorrect email address;
- Double-clicking on an unsafe URL or attachment;
- Sharing passwords with others;
- Leaving computers unattended when outside the workplace;
- Using personally owned mobile devices that connect to the organization's network.

In 2018, *Risk.net* spoke to chief risk officers, heads of operational risk and senior practitioners at financial services firms, including banks, insurers, asset managers and infrastructure providers. Based on the risk concerns most frequently ranked by those practitioners as the industry's top 10 operational risks for 2018 IT disruptions and Talent risks are mostly related with human error discussed below.

Whether from a disabling cyber-attack, or the more routine causes of human error or failure of aging hardware are considered the top threat to financial services firms for 2018 by senior operational risk practitioners.

Guarding against known risks such as DDoS is a given. What worries operations risk managers more and more are the harder-to-measure disruptive threats – cyber and physical – to their firm's networks. Malware, employee error and plain old hardware failure can be just as crippling when it comes to a loss of operational functionality. The disruption to services from successful ransomware attacks is usually far more costly than payment made to cyber thieves, as the 2017 WannaCry attack showed. Still harder to quantify are the thousands of man-hours invested in universal training for staff, or spent trying to trace when and where successful breaches occurred.

Practitioners noted that many of the previous year's worst IT disruptions can be attributed to faulty software. The US Comptroller of the Currency notes weaknesses in controls and governance related to information security within banks. Patch management – the application of fixes or updates when vulnerabilities are identified in software – and access management are of particular concern, because they are the soft spots through which attackers can penetrate a bank's outer perimeters. Talent risk enters the top 10 as the finance industry struggles to attract, train and retain the best and brightest among competition from other sectors such as technology. It's not just front office jobs banks have repeatedly warned that they are struggling to attract and retain sufficiently experienced risk managers. This is having real world consequences for the quality of their operation risk management. More than one bank *Risk.net* spoke to for the top 10 witnessed an increase in reporting failures due to human error, where less experienced staff had been pushed into high-pressure roles; others point to project overruns due to a shortage of staff.

Survey done by Opinion Matters research group indicates that 83% of security professionals believe that staffs have unintentionally exposed sensitive data at their firm (Razvan M. 2019). Similarly, it was found that inadvertent incidents were usually related to company's' failing to encrypt data before use. Most common technologies which caused inadvertent breaches by staffs were outside emails (51%), company email (46%), file sharing (40%), teamwork tools (38%), and message apps (35%).

These incidents related to email attachments are mostly sharing to incorrect email, forwarding of sensitive information, and forwarding data to private email addresses. This research also indicates that 79% of companies use sensitive corporate data inside with no encryption also 64% again send sensitive corporate data outside with no encryption.

Organizations should work to identify and minimize human error leading to major breaches. Similarly, a recent research report on cyber investigations of breaches implicated human error as a factor in 95% of security incidents (IBM Global Technology Services, 2014). This provides a picture that the vast majority of human errors are as a result of a slip or lapse, whereby the person that the human error relates to performed a task but did so incorrectly rather than the incident occurring due to them not performing a task. The most common primary elements of roles associated with human error related information security incidents within the public sector organization were communications and administration. The most common specific activities that led to the incidents within the participating organization were Sending an Email 76 (25.5%), Posting Documents 69 (23.2%), Data Filing 52 (17.4%) and IT System Configuration, Administration, Development or Support 22 (7.4%). A recently developing issue regarding information security is human factors since human error is becoming responsible to large portion of breaches, ransomware occurrences, and cyber-attacks (Kraemer Carayon, 2007). Attackers access systems through manipulation of human error via poor policies, technology-induced vulnerabilities, noncompliance, malware, spear phishing, and social engineering s. Most common specific activities that led to the incidents within the participating organization were Sending an Email 25.5%, Posting Documents 23.2%, Data Filing 17.4% and IT System Configuration, Administration, Development or Support 7.4% (Evans et al., 2019).

The Defense Travel System (DTS) of the United States Department of Defense (DOD) sent an unencrypted email that has an attachment to the incorrect email addresses (David Bisson, 2019). This email has revealed private information of about 21,500 sailors, marines and civilians. These emails contained victims' bank account records, shortened social security numbers and emergency contacts. Information shared by any organizations lacking appropriate encryption will attract and enable cyber criminals in between two email servers to intercept and access those emails. Following the incident, they applied an email recall system to reconsider the number of email addresses to sending the email. In 2017, the United States Department of Homeland Security's Computer Emergency Readiness Team (CERT) sent customer credit reporting agency information about a vulnerability affecting only few versions of Apache Supports. Then the agency sent a mass internal email about the vulnerability. Also there was a misconfiguration on the inspection device because of a digital certificate that expired 10 months ago. Collectively, these errors empowered a malicious ac-

tor to hack into the agency's system. In the meantime, an attacker is believed to have revealed private information of 145 million people in the US and more than 10 million UK citizens.

In 2018 a digital certificate used by Swedish multinational networking and telecommunications firm Ericsson software expired. As a result, users of different UK mobile carriers lost service such as GiffGaff, Lyca and O2 Mobile. When such certifications expire they do not only cause quite long unavailability they also leave critical systems unsecured. In the meantime hackers take advantage of the temporary outage to evade safeguards.

2.6 System Approach

The human error problem can be viewed in two ways: the person approach and the system approach. Each has its model of error causation and each model gives rise to quite different philosophies of error management. The basic premise in the system approach is that humans are fallible and errors are to be expected, even in the best organizations. Errors are seen as consequences rather than causes, having their origins not so much in the perversity of human nature as in "upstream" systemic factors. These include recurrent error traps in the workplace and the organizational processes that give rise to them. (Reason,2000). According to the macro ergonomic work system model developed by Carayon and Smith (2000) a work system may be conceptualized as having five elements: the individual, task, tools and technologies, environment and the organization. The interplay of these elements may create conditions that contribute to human error and violations. These errors may result in security vulnerabilities and sometimes result in security breaches, if the vulnerability is exploited.

The macro ergonomic conceptual framework shown on *figure 1* uses to identify and describe the work system elements contributing to human errors that may cause vulnerabilities. The work system model guides to define specific categories of elements that may contribute to human errors and violations. The middle section of the framework describes the various dimensions of human errors and violations. Within various cognitive processing stages, different types and levels of human error may occur. Perhaps the most widely known and accepted human error taxonomy is the skill-rule-knowledge (SRK) framework of Rasmussen. This framework postulates that errors may be divided into categories based upon an individual's level of performance. The errors are distinguished by both psychological and situational variables that together define an 'activity space' on to which the three performance levels are mapped. The three performance levels are:

1. skill-based level errors, which are made with routine, highly practised tasks in a predominantly automatic capacity with occasional conscious checks on progress. It is thought that in this activity space people perform very well most of the time;

2. rule- based performance level occurs when a change is needed to modify the automatic behaviour found at the skill-based level. At this point the person may apply a memorized or documented rule, with periodic checks to monitor the progress and outcome of the actions; and

3. knowledge- based performance is an activity space met only after repeated failure and without a pre-existing solution. Errors have been categorized as either mistakes or slips and lapses (Reason, 1990; Norman, 1981). Using Rasmussen's SRK model of human performance, mistakes can be further categorized into rule-based mistakes and knowledge-based mistakes. Mistakes occur when the action was intended, but turned out to be inappropriate. In contrast, slips and lapses occur when the action (or lack of action) was unintended. For example, a mistake includes applying a security-related patch to the wrong piece of software. A slip or lapse includes forgetting to apply the security related patch to the appropriate piece of software. The Computer and information vulnerabilities may be thought of as "near misses" or the accidents "waiting to happen".

Figure 1:Macro ergonomic conceptual framework (Carayon and Kraemer, 2007)

2.7 The Swiss cheese model of system accidents

Defences, barriers, and safeguards occupy a key position in the system approach. High technology systems have many defensive layers: some are engineered, others rely on people, and yet others depend on procedures and administrative controls. Their function is to protect potential victims and assets from local hazards. Mostly they do this very effectively, but there are always weaknesses. In an ideal world each defensive layer would be intact. The Defences are similar to slices of Swiss cheese with many holes though, these holes are continually opening, shutting, and shifting their location. The presence of holes in any one "slice" does not normally cause a bad outcome. This happens only when the holes in many layers momentarily line up to permit a trajectory of accident opportunity bringing hazards into damaging contact with victims (figure 2).

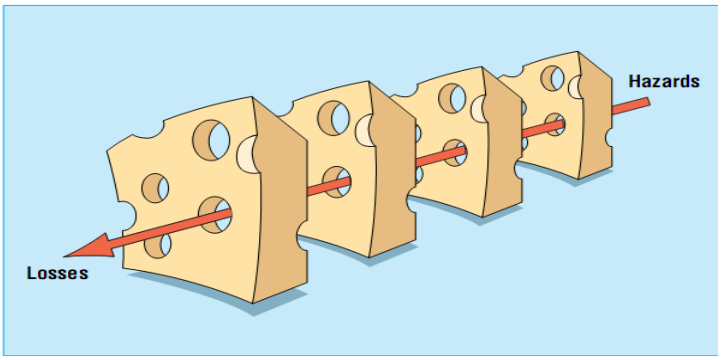


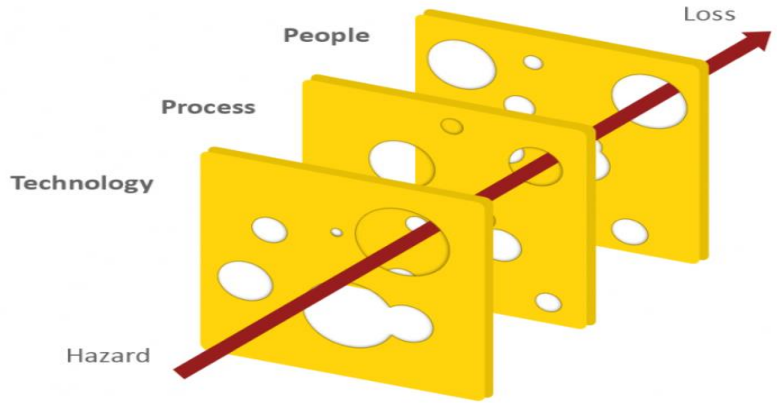
Figure 2: The Swiss cheese model of system accidents (Reason, 2000)

The holes in the defences arise for two reasons: *active failures* and *latent conditions*.

Active failures are the unsafe acts committed by people who are in direct contact with the system. They take a variety of forms: slips, lapses, fumbles, mistakes, and procedural violations.

Latent conditions are the inevitable "residents" within the system. They arise from decisions made by designers, builders, procedure writers, and top level management. Such decisions may be mistaken, but they need not be. Latent conditions have two kinds of adverse effect: they can translate into error provoking conditions within the local workplace (for example, time pressure, understaffing, inadequate equipment, fatigue, and inexperience) and they can create long-lasting holes or weaknesses in the defences (untrustworthy alarms and indicators, unworkable procedures, design and construction deficiencies, etc.). Latent conditions—as the term suggests—may lie dormant within the system for many years before they combine with active failures and local triggers to create an accident opportunity. Unlike active failures, whose specific forms are often hard to foresee, latent conditions can be identified and remedied before an adverse event occurs.

Understanding this leads to proactive rather than reactive risk management (Reasons, 2000).



The Swiss Cheese model, adapted for cyber security. Illustration based on Dante Orlandella and James Reason.

Figure 3: Adapted Swiss cheese model for cyber security (Erlend Andreas Gjære, 2017)

Evidently, researches regarding human error indicate that not single major incident has ever been caused by only a single error. The Swiss cheese figure shown above illustrations this. Some holes of the Swiss cheese are caused by an active fault, whereas the rest are due to hidden/latent circumstances. Security strategies should consider all circumstances or applying a barrier based approach. There are some technological barriers, and then barriers within the procedures. Finally it reaches to people as the last fence. Actually, people are responsible to fix it all after the unexpected issues happen beating all barriers.Often times this happens and sometimes not. This failure can be explained by the alignment of those holes or barriers and definitely not only due to human which stands at the last fence.

2.8 Human reliability analysis (HRA)

Human reliability analysis encompasses the use of both qualitative and quantitative approaches to assess the contribution of humans to risk (Bell and Holroyd, 2009). It can also be described as human performance in terms of completing any activity with no error within a given time and state. (Gu et al., 2014). HRA is a method of both predicting and assessing, as a complement to risk assessment, the failures of human action or inaction, rather than the failure of a physical component (French et al., 2011), that would have a detrimental effect on system reliability or availability (Chandler et al., 2006). There are a number of diverse HRA methods available to address human failure as part of probabilistic risk assessments (Bye et al., 2011). Two HRA methods exist *Retrospective* HRA and *Prospective* HRA. *Retrospective* HRA reviews previous incidents and determine the root cause of the incident in terms of human error. *Prospective* HRA is a method that assigns quantitative probabilities to identify high risk systems. This information is used to

implement solutions to mitigate the high risk situation. This research uses a prospective HRA approach to identify risks proactively from the tasks and factors.

2.8.1 Human reliability analysis (HRA) techniques

This section presents some of the established Human reliability analysis techniques and introduces HEART as a selected HRA method and discusses why it is selected for this research.

Absolute Probability Judgement (APJ): is a generic HRA method which employs expert judgement. It utilises either a group method or single expert method. This technique is straightforward to apply but requires extensive input by experts, who may require specific training, and significant coordination to conclude results (Adhikari et al., 2009).

A Technique for Human Error Analysis (ATHEANA): was created for the nuclear industry and can be used for both retrospective analysis of incidents and as a component of probabilistic risk assessment, however, this technique was found cumbersome and requires a large team to complete the assessment as well as the results not being consistent and repeatable (Adhikari et al., 2009). *Cognitive Reliability and Error Analysis Method (CREAM)*: supports both retrospective analysis and probabilistic risk assessment. It has both basic and extended versions. However, this technique required human factors expertise, requires a high level of resource and takes lengthy time periods to complete (Adhikari et al., 2009).

Success Likelihood Index Methodology (SLIM): was developed for use within the nuclear industry and used expert judgement to derive the human error probability (HEP). It comprises of two modules called Multi-Attribute Utility Decomposition (MAUD) and Systematic Approach to the Reliability Assessment of Humans (SARAH). This technique has a high level of theoretical validity but expert judgement is required and is resource intensive (Adhikari et al., 2009).

T*echnique for human error rate prediction (THERP)*: was developed for the nuclear field and uses an event-tree approach to establish HEP based on a large database containing HEP data relating to nuclear plants. THERP could not only be used for design purposes but also as part of probabilistic risk assessment (Adhikari et al., 2009). However, the technique is very resource intensive and requires a large amount of effort to produce accurate HEPs.

Cyber Human Error Assessment Tool (CHEAT): Within security area, one may consider this presented by Goodliff and Widdowson (2015). They stated that benefit would be gained in the security area from a more rigorous and structured approach. However, the human factor root causes within, CHEAT were derived through analysis of publicly available past security incidents rather

than empirical research. The incident data analysed to develop CHEAT was constrained by a lack of information in the public domain (Thales, 2017).

Human error assessment and reduction technique (HEART): was issued in 1985 and many organizations even sectors used it as an instrument to resolve the concern regarding human reliability (Williams, 1992). This method has been usually used in industries mostly by nuclear industries (Chandler et al., 2006). HEART has well validated likelihood calculations and does not require significant resource to be applied. HEART has been validated empirically (Bell and Holroyd, 2009) and its precision could be judged as 'reasonable' (Chandler et al., 2006). Bye et.al. (2011) also state that analysis the HEART method predictive power is fair.

HEART cover ergonomic, cognitive, and organizational factors (Chandler et al., 2006). HEART would take a low amount of time to perform the procedure (Maddah & Ghasemi, 2015), and is compatible to the security practitioners that have time constraints. HEART can be applied within varied settings where human reliability is important such as industry and healthcare (Adhikari et al., 2009; Bell & Holroyd, 2009; Chadwick & Fallon, 2012). An analyst can learn HEART in a short period of time (Chandler et al., 2006). HEART is known for its fast and quite simple way in quantifying the risk of human error (Bell & Holroyd, 2009). HEART is a well validated tool (Bell and Holroyd, 2009), with both qualitative and quantitative output. This would support practical information security application and provides useful suggestions on how to reduce the occurrence of errors (Adhikari et al., 2009). Mainly, HEART method deals with whole tasks rather than sub-tasks and is more flexible in its application than other HRA techniques, for example THERP and JEDI (Kirwan, 1997). It does not necessarily require the development of a Hierarchical Task Analysis (HTA) which is which involves breaking down the task under analysis in to hierarchy of goals, operations and plans, thus reducing the overall time needed to complete the analysis. HEART is a generic technique and supports the objectives of this research in terms of its empirical results of human error within information security. It has been shown in the literature that HEART could be utilised to potentially address current gaps in human reliability analysis within information security area. In fact, HEART is proposed to be mapped to current cyber-security causing tasks making a Cyber Security HEART method. For instance, the tasks or GTTs known in HEART method could be line up to cyber-security causing tasks starting from routinely operating of information to execution of IT management jobs including applying modifications to the rule base applied within network firewall devices (Evans et al., 2016). Following the identification of GTTs appropriate EPCs can be found. Therefore, HEART is selected to perform the Human Reliability Analysis for this research. In summary, in order for the information security field to effectively deal with the current volumes of incidents it is important that a framework, such as HRA, and associated

applicable technique, such as HEART, be incorporated within current practices. These practices include risk management and incident management to understand both the underlying causes of human error related information security incidents and the risky conditions in order to implement required controls.

2.9 National security strategic management model and CBE services

The banking sector is one of the influential industries in the Ethiopian economy. In the banking business using technology and advancement of services has increased. However, the level of information security risk also increases even with the most advanced automated technologies. Information security standards and best practices are best solution for effective information security management. Each one of them have their own focus areas including advantages and drawbacks. Existing and recommended standards which are mostly used in the banking for information security management and compliance are ISO 27K, COBIT and PCI DSS. Most of these practices lack Human errors assessment in the working places specially task specific using the system approach mentioned earlier. INSA released Critical Mass Cyber Security Requirement Standard Version 1.0 in 2016. CMCSRS version 1.0 stated that governmental and nongovernmental organizations in Ethiopia are highly relying on information and communication technology, and information is becoming invaluable economic, political and social asset of the nation and a resource to transform the economy (p.7). This requirement standard acknowledges the security threats associated with information technology. The standard clearly stated this as, the reliance on information systems in increasing the vulnerability of the organization to cyber-attacks are becoming highly complicated, dynamic and destructive (CMCSRS version 1.0, 2016, p.7). It further stated that it is essential to ensure the security of organizational information systems in order to protect organizations from attacks and minimize the impact of attack on the country. Due to this reason, CMCSRS version 1.0 is issued by INSA pursuant to article 13 of INSA re-establishment proclamation execution council of Ministers Regulation No. 320/2014 (CMCSRS version 1.0,2016, p.7) In addition the standard stated that it should be used as a beginning point. The CMCSRS stated this concept as organization should identify 80-20 in each area and focus on the 20% based on 80 -20 rule (Pareto Principle) (CMCSRS, 2016, p.21-25). This provides an area to scheme cyber security framework based on organization specific events and risk

According to cyber security strategic Management model of Ethiopia (CMCSRS of 2016) the core principles of the security strategic model are:

- Risk based: organization should implement cyber security solutions/controls/ based on risk assessment,

- Embedded security: organization should embed cyber security in their organizational structures and processes,
- Cost effective,
- Focused on human, process and structure, and
- Balanced and aligned with national cyber security and directives (CMCSRS, 2016).

HEART is a human-task based risk assessment approach which is cost effective and validated for both its qualitative and quantitative output.

2.9.1 Functions and Services delivered by Commercial Bank of Ethiopia

2.9.2 Case study organization

The case study organization is CBE, a financial service provider operating nationwide. The history of the commercial bank of Ethiopia dates back to the establishment of the state bank of Ethiopia in 1942. It has more than 1456 branches stretched across the country. It is the leading African bank with assets of 711.96 billion birr as on June 30, 2019.The bank plays a catalytic role in the economic progress and development of the country. Currently, CBE has more than 22 million account holders and the number of mobile and internet banking users also reached more than 2.5 million as of June 30th 2019. It also has strong correspondent relationship with more than 50 renowned foreign banks like Commerz bank A.G., Royal Bank of Canada, City Bank, HSBC bank. It has approximately 37,894 permanent employees and more than 22,000 outsourced jobs as of June 30,2019. The organization was selected through recommendation and agreement (opportunity) with the university. 1 Each unit of the organization including the business are required to develop and pass on a risk assessment based on their respective tasks.

	Divisions (Processes)	Responsibilities	Sub-processes
CORE PROCESSES	Customer accounts and transaction services (CATS)	Managing the accounts of the customers and transaction services	Branches and Head offices
	Trade services	Entrusted with the task of international banking services provided at all branches of the bank with a single contact point of customer service relationship officers assigned for this purpose only.	Services provided are listed below the table*
	Credit services		
	Human	Develop HR strategy, policy and	• HR management

	Divisions (Processes)	Responsibilities	Sub-processes
SUPPORT PROCESSES	resources	procedure; employs and develops existing and future human resource of the bank. It also handles various employee services such as payroll, pension, health care	• HR development • health care • security services.
	Information systems	• data processing and information management • system development and customization • network configuration and setup • software and/or hardware procurement • implementing IS quality and change management	• IT application management (core banking system. • ERP systems • switch system • Alternative payment channels, auxiliary system and electronic data exchange) • infrastructure management (server, network, database, auxiliary infrastructure, data center • Call center and district IT support • management of information system • IT Security (SOC, IT security assessment, BC/DR, threat and system failure and vendor management).
	Facilities management	• Procurement of goods and services • Construction of buildings • Maintenance of buildings, vehicles and office equipment • Providing transportation services for the other bank organs • Disposal of used assets	• Procurement • building and construction, • acquired assets administration • transport management and, • Archives.
	Finance	All accounting and finance related issues listed below. • Maintaining the bank's book accounts • Reconciliation; Consolidation and	• Accounts and reconciliation • Fund management

	Divisions (Processes)	Responsibilities	Sub-processes
		generation financial reports; • Managing the entire local and foreign fund of the bank	
OTHER PROCESSES	Business development	• Product development and management • Conducting researches on various issues • Building the image of the bank via effective communication • Awareness creation on products and services of the bank	• Research and policy analysis • product development and management • communication and • promotion management
	Risk and compliance management	• performs analysing and proposing risk treatment options • Ensures that the bank's policies, procedures and practices are in a state of being in accordance with all of the applicable laws, regulations, code of conduct and standard of good practice.	risk management and compliance.
	Internal audit	• Provides key input for the development of risk based strategic and annual internal audit plan, • Conducts performance, financial, compliance and information system audits. • Consulting the bank's management and staff is also one of its services within the bank.	
	Legal and loan recovery		• Legal services and loan recovery.

Table 1: Processes and services provided by CBE

*The following are major services provided by trade services division:

- ***Documentary credit (L/C)*:** is a written undertaking by a bank given to the seller at a request and/or the instruction of the buyer to make payment or accept and pay bill of exchanging (draft) drawn by the seller up to a stated sum of money within a prescribed time limit and against stipulated documents.
- ***Import*-**available by sight payment/negotiation payment/deferred payment/acceptance payment. If approved by the National Bank of Ethiopia.

- ***Export***-payment available by sight/negotiation/acceptance of bills. If approved by the National Bank of Ethiopia.
- ***Documentary collection***: is a method through which banks handle a seller's commercial documents with or without financial documents in accordance with instructions received from the seller in order to deliver the documents to buyer (importer) against payment and/or acceptance or against other terms and conditions.
- ***Advance payment***: is a method through which a seller receives payment from a buyer prior to shipment or the agreed upon goods or rendering the agreed upon service.
- ***Import***-Payment though bank transfers
- ***Export***-Payment through bank transfers, traveller cheques, cash (as long as it is declared).
- ***Consignment basis payment***: It is a method of payment in which the title to the goods remains with the seller until an agent (distributor) in foreign country sells them. Payment is made to the seller if and when the agent (distributor) sells the goods.
- ***Export***- it is applicable to perishable items: fruits, flowers, meat, molasses, etc. as approved by the National Bank of Ethiopia
- ***Guarantee***: A letter of guarantee issued by an issuing bank/guarantor is a written undertaking by the bank to compensate (pay sum of money) to the beneficiary (local or foreign) in the event that the obligator/principal fails to fulfil his/her /its obligations in accordance with the terms and conditions of the guarantee.
- ***Small export items license (permit):*** is a license issued for small export items to tourists, foreign residents of Ethiopian nationals who wish to take souvenir, samples, gifts, repairs, replacements, exhibitions and personal effects and belongingness, etc.

The main processes or services provided by the bank are shown in table 1. Among the lists, Trade services, Human resources, Information security, Finance, Alternative payment channel, Call center, and Branches are the focus this research. Within the information security unit, the security operation center (SOC) is the main section under this research which is selected for interview. The center provides a holistic view of the bank's information technology (IT) security, with the capacity to register the flow of any logs generated from hardware and software. It further examines correlated and consolidated pattern of possible cyber-attacks. It's responsible for notifying system administrators and security operations center about the nature and source of the cyber-attack. For monitoring this operation, the bank has dedicated team of 15 experts or cyber-attack analysts.

Alternative payment channel is another division within the information system responsible for services related with card management, accounts and reconciliation and technical card support. Under this division the main focus is to the address card management unit. Call Center unit involves both technical and business supports. It is a customer contact center consisting of IT advisors, internal help desk, quality assurance and technical support. CBE has more than 1500 branches nationwide to provide banking services for its customers. But since branches are structured to provide uniform services at different locations only three branches were chosen as a sample to address errors encountered at branch offices.

2.10 Related work

There are limited empirical researches in areas of human error regarding information and cyber security. This section covers recent papers conducted to address human error with information security in mind. The first paper to introduce or recommend HEART in analysing human error within information security area was done by (Evans et, al 2015). This research intended identifying fundamentals of cyber security that would benefit through more research. It also studied literature connected to cyber security reassurance and the influence of human element on it. Finally, it proposed an assurance framework that integrates human reliability assessment, statistical quality control and a vulnerability scoring system. Additionally, the research indicated the use of HEART as a preferred technique among HRA methods.

As Evans et.al (2017) indicated that the real what is currently understood by the information security community. The research utilises HEART to analyse published public sector data breaches and incidents. It also uses a set of GISATs or general information security affecting tasks to map the incidents to HEART GTT. Most common task related to information security incidents are usually routine and highly-practised activities (GTT_ E). Regarding specific activities resulting information security incident posting of information and use of email are most common.

A research done by similar authors (Evans et.al, 2018) developed HEART vs IS method for assessing human error associated information security cases. The study aimed to establish if the HEART technique is applicable to information security also if the in-built likelihood calculations mirror actual incident frequencies experienced within a private sector organization and indeed confirmed that it is indeed very much relevant to information security area only with slight adjustments to the vocabulary of EPCs. The research found out that the most common tasks that led to information security incidents were routine tasks performed rapidly by front-line employees and also the most common EPC is shortage of time available for error detection and correction.

Similar research for the evaluation of information security core human error causes method aimed at public sector vs private sector comparison was done by Evans et.al, 2019. The research performed retrospective analysis of recorded information security incidents using case study in the public sector organizations. This research confirmed that the most common EPC is shortage of time available for error detection and correction.

Metalidoua et, al (2014) reviewed the impact of human factor on information security and argued how awareness of information security could be a key tool in overcoming the weaknesses. The study mainly examined the relationship between human factor and lack of information security awareness. The research recommends that the difficulties related with information security that staffs face daily should to be assumed and resolve. Meaning the security purposes have to be significant and slightly invasive as possible.

Lilia, 2017 conducted a case study and proposed a cyber-security program as a fundamental that would help further improve the development of cyber security strategies based on current literature. The study presented five main popular solutions for cyber security awareness with one of them being awareness phishing simulations which are based on template emails. Thus it describes various scenarios and send them to the employees. The employees' response measures the employees' awareness. This metrics are very similar to a marketing campaign metrics: the number of open emails, the number of clicks, etc.

No.	Author and Date of Publication Title	Objectives	Method	Finding
1	(Evans, He, Yevseyeva and Janicke, 2017) *Analysis of published public sector information security incidents and breaches to establish the proportions of human error*	-is understanding the magnitudes of incidents and breaches related to human error as well as the types of activities that caused these incidents	--utilises HEART to analyse published public sector data breaches --employed GISATs and mapped the breaches to HEART GTT	-- real numbers of private data breaches and information security cases are quite bigger than actually understood by the information security workers --activities resulting information security incident posting of information and use of email are most common. -- Most common task related to information security incidents are usually routine and highly-practised activities (GTT_ E). --The adaptation of the method

No.	Author and Date of Publication Title	Objectives	Method	Finding
				enables the underlying root causes of human error to be understood and acted upon
2	(Evans, He, Maglaras, Janicke, 2018) *HEART-IS: A novel technique for evaluating human error-related information security incidents*	- to describe human error related information security incident and make a new HEART of Information Security method --to establish if the HEART HRA technique is applicable to information security -if the in-built likelihood calculations mirror actual incident frequencies experienced within a private sector organization	-case study method -HRA method (HEART)	- confirmed that HEART is indeed very much relevant to information security area only with slight adjustments to the vocabulary of EPCs. -The most common tasks that led to information security incidents were routine tasks performed rapidly by front-line employees -The most common EPC is shortage of time available for error detection and correction
3	(Evans, He, Maglaras, Yevseyeva & Janicke, 2019) *Evaluating information security core human error causes (IS-CHEC) technique in public sector and comparison with the private sector*	- to perform a retrospective analysis of recorded information security incidents in public sector organizations	-case study - map of incidents to *IS-CHEC* technique	- proportion of human error is far higher than reported - The most common EPC is shortage of time available for error detection and correction
4	(Abraham,2011) *Information Security Behaviour: Factors and Research Directions*	– critically analyses articles in information security behaviour in the context of factors affecting security behaviour of users in organizational environments	-extensive literature review	-brings forward 18 themes for security practitioners and researchers to consider in implementing information security initiatives.
4	(Metalidoua, Marinagi, Trivellas, Eberhagen, Skourlas,	-assessment of human factor in information security; information security awareness in particular	-used a framework to study the relation of Human Factors with the Lack of Information Security	-information security awareness is very crucial to control security incidents as a result of human weaknesses -identified human weaknesses

No.	Author and Date of Publication Title	Objectives	Method	Finding
	Giannakopoulos, 2014) *The Human Factor of Information Security: Unintentional Damage Perspective*		Awareness.	triggering security topics and gave recommendations on ways to overcome them
5	(Evans, Maglaras, *et, al,*2015) *Human Behaviour as an aspect of Cyber Security Assurance*	- to find fundamentals of cyber security that would help from more research based on the literature review findings	-literature review of Cyber security assurance and the influence of human on it	-an assurance framework is proposed that integrates human reliability assessment, statistical quality control and a vulnerability scoring system
6	(Lilia,2017) *Employees' Impact on Cyber Security Human Behaviour Consequences on security measures*	- to identify fundamentals that would help further improve the development of cyber security strategies based on current literature	-case study -reviews existing approaches	-presented consideration of important Human factors including cultural, gender, and attitude differences -presented existing cyber-awareness solutions -human patterns and cybersecurity knowledge have an important impact on the awareness results

Table 2: Related work

A study by Metalidoua et, al, 2014 recommends that the difficulties of information security that employees face on a daily should be assumed and solved. On top of this task centric researches are scarce which could easily explain the tasks each employee is titled to. In summary, in order for the information security field to effectively deal with the current volumes of incidents it is important that a framework, such as HRA, and associated applicable technique, such as HEART, be incorporated within current practices. These practices should include risk management and incident management to understand the underlying causes of human error related information security incidents in order to implement required controls. Successive researches on this issue employed live data pulled out from information security incident registers from both public and private sector organizations as shown on table 2. System approach considers the environmental factors specially

tasks that are prone to human error. Standing from the system approach researches should focus on public incidents which need deep investigations on the activities that were being performed.

2.11 Chapter Summary

The purpose of this chapter is to give insight about human errors leading to information security incident by referring different researches, books and other source relevant sources. This chapter gives a detailed insight about human error, information security related human errors and Human reliability analysis. Exhaustive literatures are reviewed to explain human error incidents along with their best practices. Lastly, gaps on the existing literature are identified. It was revealed that there is a lack of empirical study based on the tasks of employees that enhances information security prospectively in particularly within the financial industries and that HRA methods are underutilized within information security field to address human factors.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Overview

This research used both a qualitative and quantitative method to identify causes for behaviour of employees resulting in information security incident. The research is a case study known as a method for in depth study. "A case study method is a careful and complete observation of an individual or a situation or an institution; efforts are made to study each and every aspect of the concerning unit in minute details and then from case data generalizations and inferences are drawn" (Kothari, 2004). The target population include all employees of the Bank that have access to a computer system from junior levels to executives of both at the core processes and support processes.

3.2 Research Design and approach

This research targets to answer two questions as stated in chapter one. The research used HEART which is both a qualitative and a quantitative research approach mainly to answer research questions two. The Main purpose of research design is "to ensure that the evidence obtained enables us to answer the initial question as unambiguously as possible" ("Research Design", n.d., p. 9). Therefore, it describes potential respondents and how to take sample. Below is the description and justification in the logical structure that the research followed regarding to sample determination, unit of analysis and the data analysis.

3.2.1 Unit of Analysis

The unit of analysis is the major entity that is analysed in a study by (Trochim, 2006). The unit of analysis defines what a "case" is in a case study. A unit of analysis (case) may be an individual, group, department of an organization, organization and process (Yin, 2009). This research analyzed working conditions and task types to reach at the causes resulting in human error. It mainly focuses on tasks that need further study to manage errors caused by humans. This includes divisions with known past incidents or error prone tasks believed to be subject to information security incident. Thus the research used department approach or a division-wise since the objective of this research to identify tasks in general.

3.2.2 Research Population

The study population is "from whom the required information to find answers to a research questions is obtained" and from this the researcher can select appropriate respondents (Kumar R.,

2011). The population addressed consists of workers and their tasks involving computer system interaction used mainly to perform the tasks they are titled to. Experts under each task have a homogeneous nature but their judgement differ by their background which is one of the pillars of HEART.

3.2.3 Sampling Technique

Sampling is a process of choosing a smaller, more manageable number of people to take part in a research. For most researches, unless the researcher has a huge budget, limitless timescale and large team of interviewers, it will be difficult to contact to every person within the research population (Dawson, 2002). For qualitative study purposive sampling techniques is highly recommended in the case study where only a little is known (Kumar, 2011). Employing a purposive sampling techniques allows a researcher to use personal judgement to identify key participants who provide adequate information to answer the research question therefor a purposive sampling is used to answer all research questions. Thus the sample is selected considering divisions having high probability of incident or with known incidents in the past which helps to address human error in the bank. Also the experts included in this research are chosen based on their background or experience to make sure the responses are comprehensible. Regarding sample size determination on qualitative study Kumar (2011) noted that "you are guided by your judgement as to who is likely to provide you with the best information" (P.193). CBE has more than 1500 branches nationwide but since HEART requires Generic task types within the bank this research involved three branches and six divisions from Addis Ababa as a sampling area. This addresses 45 experts from nine divisions within the bank namely Trade services, Information System, Alternative Payment channel, Call Center, Human resources, Finances, and Three branches.

3.3 Methods of Data Collection

Semi-structured interview is "used to collect quantifiable data which is also referred to as 'quantitative research interviews'" (Saunders et.al., 2009, p. 351). There are some reasons for using semi-structured interview. Firstly, from pilot test the experts face difficulties understanding the objective of the interview and they recommend researcher to interpret each terms. Thus this study is based on data collected through semi-structured interview.

3.3.1 Interview Design

All the interview questions are categorized based on all underlying levels of the HEART which are GTTs and EPCs which were rated by experts. This is conducted through Aggregated individual method which entails that the experts do not meet but make estimates individually using GRS.

These estimates are then aggregated statistically by taking the geometric mean of all the individual estimates for each error causes.

The first research question was discussed with the experts to query evidence regarding the practice at the bank. The rest is developed directly from HEART tables or tasks and error causing conditions given as this directly measures the remaining research question. Most researches underline APOA estimation as one of the difficulties of using HEART. Research by (Evans et, al 2018) applied percentage for elicitation of expert judgement but they concluded by recommending usage of decimal approach to collect the APOA which would simplify accurate (pessimistic) scoring and enable the calculation of the nominal likelihood of failure. They also suggested that APOA be obtained using a graphical rating scale (GRS) as proposed by Chadwick and Fallon (2012) as part of the modified HEART tool used to assess human reliability. They discussed that GRS is ideal for HEART because it is easy to use and has been shown to be a fairly reliable data collection method. GRS also enables researchers to easily collect continuous data, making it even more appropriate for evaluating APOAs. The use of a GRS is a common format for user rating as it enables high levels of user acceptability and face validity (Chadwick and Fallon, 2012). Hence the researcher used a written form of the interview for the interviewees to elaborate the process utilizing Graphic Rating Scale (GRS) for estimating each APOA.

Figure 4: APOA question scale

This scale is divided into 5 categories with the linguistic descriptors “Negligible”, “Minor”, “Moderate”, “Major”, and “Extreme”. The use of 5 descriptive anchors is supported by McKelvie (1987) as “subjects using the continuous scale appeared to be operating essentially with five or six categories” (pg.198). As shown above on figure 4, the scale is labelled from 0-10 with 1 decimal place, allowing the assessor to make finer distinctions at their judgment.

3.3.2 Semi-structured Interview

Semi-structured interview is “used to collect quantifiable data it is also referred to as ‘quantitative research interviews’” (Saunders et.al., 2009, p. 351). There are some reasons for using semi-structured interview. Firstly, from pilot test the experts face difficulties to understand practice and

they recommend researcher to elaborate the query. This technique gives a chance for interviewer to explain the question to avoid misinterpretation. Most interviews were made on-site and this approach brought to collect more evidence. The researcher gave further explanations about the terminologies from related researches and HEART manual (Williams, 2015) where necessary only when there is confusion. The Researcher believe that the risk that bias has occurred is low.

3.4 Data Analysis

HEART method mainly analyzes data collected through the variables to produce probabilities for errors. After the semi-structured interviews, both the collected quantitative and qualitative data was analyzed using Microsoft excel. Averaging the APOA given by each expert for each EPC balances their views preventing overly optimistic or pessimistic results which was avoided through using *geometric mean* of the individual APOA results, similar to the approach used for Absolute Probability Judgements (Kirwan, 1997). The following section describes the data analysis procedure used and the mathematical equations fed in to Microsoft excel tool to produce final predictions. HEART is human error analysis tool which follows the mathematical formulas shown below. Each expert within the divisions were presented with the list of GTTs or generic tasks from HEART and information security tasks (Evans et.al,2015) to choose from. Fortunately, there were no differences among the experts within the divisions regarding the task types selection. Following the categorization of tasks, the individual experts' judgement, APOA, gathered using GRS for each EPC were averaged. The average from the experts for each EPC was calculated using Equation (1). This calculated average APOA was used for the subsequent HEART calculations, i.e. Assessed Proportion of Affect, Assessed Nominal Likelihood of Unreliability and Percentage Contribution to Unreliability. The results from this calculation are shown on the fourth column of table 4.

For Team members, i /n:

$$\bar{X}_{geom} = \sqrt[n]{\prod_{i=1}^{n} x_i} = \sqrt[n]{x_1 . x_1 \ldots\ldots x_n}$$

Geometric mean of APOAs (1)

For each EPC (i) an Assessed EPC Affect was calculated. This is the total affect that the EPCs has on the task and was calculated using Equation (2).

$$\text{Assessed EPC Affect}_i = [(\text{EPC Multiplier}_i - 1) \times \text{Average PoA}_i] + 1$$

Assessed EPC Affect (2)

This yields the effect of each error causing conditions on the total error probability after rated by the experts. The Assessed Nominal Likelihood of Unreliability (ANLU) provides the assessor with an overall rate of unreliability for the task being analysed. It was calculated using Equation (3)

$$\text{ANLU} = \text{NHU} \times \prod_{i=1}^{n} \left[(\text{EPC Multiplier}_i - 1) \times \text{Average PoA}_i \right] + 1$$

Human error probability (HEP) (3)

This gives the final output from the HEART which is the predicted probability of human error by each task. The relative Percentage Contribution to Unreliability (%CU) made by each of the EPCs was calculated using Equation (4). This allows the researcher to rank the EPCs in terms of their affect on successful task completion and reach final preventive measures.

$$\%\text{CU} = \text{Assessed EPC Affect}_i \div \left(\text{NHU} + \sum_{i=1}^{n} \text{Assessed EPC Affect}_i \right)$$

Relative percentage contribution to unreliability (4)

After the semi-structured interviews, the collected quantitative data was analysed using Microsoft excel to reach the predicted likelihood of Human Error Probability as shown on table 4.

3.4.1 HEART method

An empirical study using the selected HRA technique (HEART) under section 2.8.1 was performed which includes mapping the banks' divisions and selection & rating of error causes to HEART Generic Task Types (GTT) and Error Producing Conditions (EPC) respectively. Calculations evaluated include human error probabilities (HEP) and contribution to unreliability (CU) based on the selection of error producing conditions (EPCs) and the respective tasks. Once the task under assessment was mapped to a GTT the factors (EPCs) that are believed to affect Human Error Probability were identified. After the EPCs have been identified each one was weighted in terms of its impact on the task (division) under assessment. When the EPCs have been identified HEART suggests the application of remedial and preventative measures (RPM) to treat each error causing conditions. The following flowchart is adapted from (Chadwick and Fallon, 2012) to reach HEART final probability predictions.

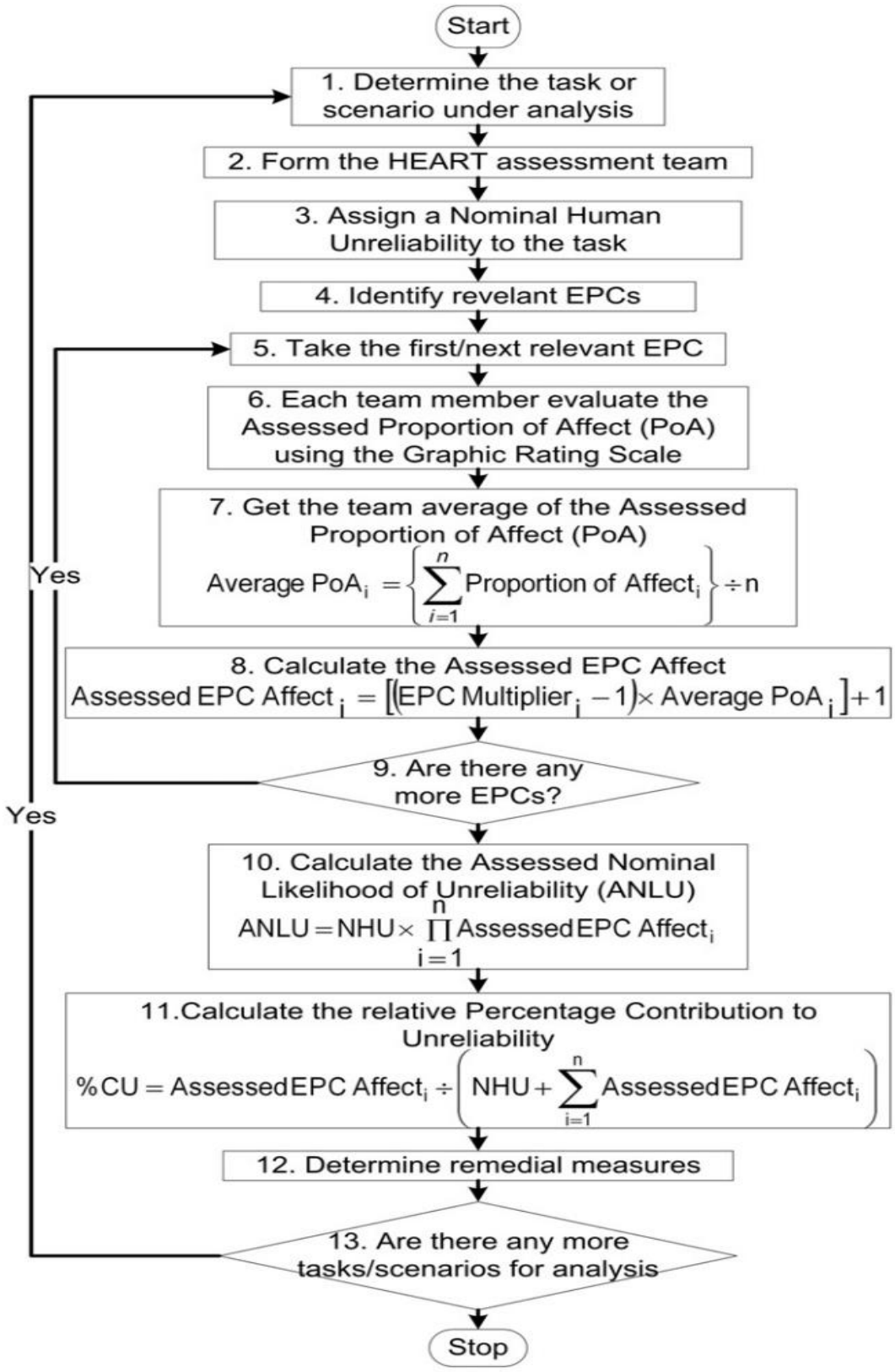


Figure 5: HEART procedure Flowchart (Chadwick and Fallon, 2012)

3.5 Reliability and Validity

The quality on an empirical research including case study, depend on validity, and reliability (Edmonds & Kennedy 2012, cited in Baskarada, 2014). Reliability is concerned with the consistency, stability and repeatability of the informant's accounts as well as the investigators' ability to collect and record information accurately (Selltiz et al., 1976). It refers to the ability of a research method to yield consistently the same results over repeated testing periods. Creswell (2014) suggests that reliability tests should be done to know whether the researcher's approach is consistent across different researchers. The strategy used for this research to achieve reliability is documenting procedures and steps used in the research work (Yin, 2009; Creswell, 2014). In addition, comparison of the findings of this research with the literature is made to refer frequent tasks reported accompanied by information security incidents. The final results including the responses haves been reflected to each unit to use the expert's feedback on the method used during both on the interview and at the final stage of data analysis.

Validity of research is concerned with the accuracy and truthfulness of scientific findings (LeComple & Goetz 1982). A valid study should demonstrate what actually exists and a valid instrument should actually measure what it is supposed to measure. There are many types of validity and many names have been used to define the different types of validity. Campbell and Stanley (1966) have defined two major forms of validity that encompass the many types. They refer to "internal" and "external" validity. Denzin (1970) used the distinction between internal and external validity and applied it to qualitative research. Internal validity is a term used to refer to the extent to which research findings are a true reflection or representation of reality rather than being the effects of minor variables. External validity addresses the degree or extent to which such representations or reflections of reality are legitimately applicable across groups.

Validity issues need to be considered when designing a research project and evaluated when analyzing the credibility of research results. Both interviewees and the researcher may be biased, either consciously or unconsciously (Diefenbach T, 2009). Bias may be overcome by a number of strategies, such as triangulation and member checking. Data triangulation means using several methods for collecting evidence, such as interviews and observations. This allows for studying a phenomenon from different perspectives and increases data quality (R.K. Yin, 2009). Member checking involves returning data material to the respondents for review and shows that their contributions are valued.

Generally, to ensure validity, expert view strategy is used (Creswell, 2014; Simon, 2011). The interview guidelines used for interview was validated through pilot testing and proofreading by

experts on the domain, this help to make sure the lists from HEART address the purpose of the study and eliminate poor wording in the questions. An appropriate sampling techniques, which is purposive sampling is used so that researcher gains deeper understanding about the case from purposively selected experts. To reduce sample bias, sample selection was also based on the ability of the respondents to provide data relevant to the research questions. The researcher made clear the nature of the research for the participant of the interview. There was a discussion over the structured questions written and delivered to each of the interviewee with the researcher. After the discussion interviewees were able to understand why the research is conducted, how the data is collected, and for what purpose it is intended. Hence, it was possible to build a trust-relationship among the interviewees and the researcher. The researcher took their review into consideration to validate the findings. Moreover, to ensure internal validity attempt has been made to base all conclusions on the empirical data.

3.5.1 Pilot Test

The lists of questions used for the semi-structured interview is validated by pilot test. There are six experts purposively selected for the pilot test. Pilot test is used to correct poor wording in checklist questions, correct ambiguity and irrelevant items. Thus researcher read each question and explained the guideline and when the experts require further explanation the researcher explained it more orally even showed further guidelines from the description note or HEART manual including recent modifications made by (Evans et al, 2017) regarding HEART for information security. While the feedback is collected, experts gave score on required questions. According to the feedback, the interview checklist presented was updated to clarify and minimize data interpretation bias. Finally, the researcher used improvement recommendation to both expert judgment and HEART human error reduction directions.

CHAPTER FOUR

DATA PRESENTATION, FINDINGS AND DISCUSSION

4.1 Overview

Semi-Structured interview was conducted with experienced individuals to understand the state of CBEs' human error approach. Accordingly, the interview was conducted with 45 individuals with different duties and positions. Data from interview was used to assess the state of human error probability with respect to each task. The case study analysis is organized using the research questions of this study. As indicated in chapter three, quantitative analysis result is the primary finding from this research. These are answered by quantitative analysis result through mathematical calculation to compare the probabilities. The first question of the research was answered by discussing with the expertise of each divisions and the security division as it requires evidences. HEART technique provides generic recommendations to guide the assessors prioritize the causes for further measures to be taken by the organization. Implementation of appropriate remedial measures reduces the assessed EPC affect and, subsequently, the assessed nominal likelihood of unreliability to an acceptable level (Williams, 2015). The following sections present the findings of the prospective analysis.

4.2 Characteristics of experts

Among the branches, support processes and core processes a purposive sampling was used to select more appropriate groups and individuals. This then addresses 45 experts from all the nine divisions selected from CBE. The following table (table 3) shows the experts' divisions, roles and their experience within this bank.

Department	Number of experts	Position titles
Trade services	5	Trade finance CPC officers
Information System	5	cyber-attack analysts, Information security manager
Human resources	5	Senior HR officers
Finance	5	Senior financial reporting officers
Alternative payment channel	5	Manager Card Management, Accounts and Reconciliation Manager, Director of Alternative Payment Channels, Senior Banking Operation Officers
Call Center	5	System administrators, technical IT officers, senior IT officers
Branch 1	5	Branch managers, branch operation officers
Branch 2	5	
Branch 3	5	

Total	45

Table 3: Summary of expert characteristics

4.3 General results

This section illustrates the overall HEART results after following the flow chart (figure 5) mentioned earlier. The following table summarizes the results driven from the HEART method. This includes mapping of general task types of the divisions, selection and rating of error producing conditions and human error probability of each task shown on table 4. The first column represents the name of divisions of this bank. The second and the third column show the error producing conditions or causes of human error and their nominal multipliers respectively as given by HEART shown on *appendix 1*. Following the interview of each expert which resulted with the rated value of each EPC a geometric mean of this value is taken as an assessed proportion of affect (APOA) which is shown on the fourth column of the table. The fifth column depicts the nominal unreliability probability of each task given by HEART shown on *appendix 2*. Values from the third, fourth and fifth column are taken to reach at the human error probability for each task depicted on the sixth column using equation 3. The last column represents the contribution of each EPCs listed down the second column to the overall human error probability shown on the sixth column calculated using equation 4.

Divisions	EPC	Multiplier	APOA	GTT	HEP	Contribution
Trade S.	14	4	0.79	0.0004	0.0130	25.23%
	2	11	0.79			66.64%
	34	1.1	0.86			8.13%
IS	34	1.1	0.79	2E-05	0.00008033	29.43%
	35	1.1	0.79			29.43%
	9	6	0.49			41.13%
HR	15	3	0.69	0.09	0.58	39.42%
	32	1.2	0.49			18.19%
	14	4	0.49			40.91%
Finance	14	4	0.69	0.02	0.125	49.71%
	36	1.06	0.59			16.77%
	15	3	0.49			32.06%
APC	34	1.1	0.79	0.09	0.0055	12.73%
	11	5	0.9			54.25%
	15	3	0.9			33.02%

Divisions	EPC	Multiplier	APOA	GTT	HEP	Contribution
Call C.	11	5	0.49	0.0004	0.0050	41.63%
	15	3	0.49			27.85%
	25	4	0.39			30.52%
Branch 1	31	1.2	0.49	0.02	0.0360	29.45%
	34	1.1	0.59			28.40%
	22	1.8	0.69			41.62%
Branch 2	31	1.2	0.69	0.02	0.0637	24.14%
	29	1.3	0.59			24.96%
	15	3	0.69			50.48%
Branch 3	36	1.06	0.69	0.02	0.0524	23.14%
	34	1.1	0.59			23.53%
	15	3	0.69			52.88%

Table 4: General Results

4.3.1 Error producing condition results

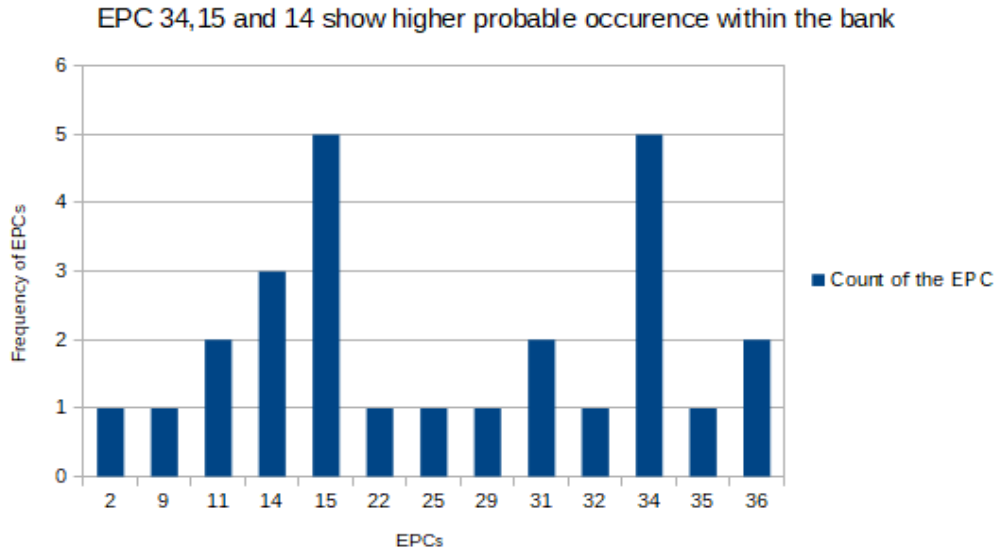
The following table depicts divisions of the bank and the top three causes for human error which is selected among the 38 error causes listed on *appendix 1*. The interview aimed at presenting the error producing conditions to the experts to make them choose only three top conditions which have more likelihood to cause incidents or human errors than the rest. As mentioned in the data collection section for validation purpose no more than three EPCs where selected for each unit.

Divisions	Primary EPC	Secondary EPC	Tertiary EPC
Trade S.	34	2	14
IS	9	34	35
HR	15	32	14
Finance	14	36	15
APC	11	34	15
Call Center	11	15	25
Branch 1	22	34	31
Branch 2	31	15	29
Branch 3	36	15	34

Table 5: EPC Results

The graph below (graph 1) shows the frequency of the EPCs selected by experts from all of the divisions which shows that operator inexperience, highly repetitious tasks and delayed or unclear

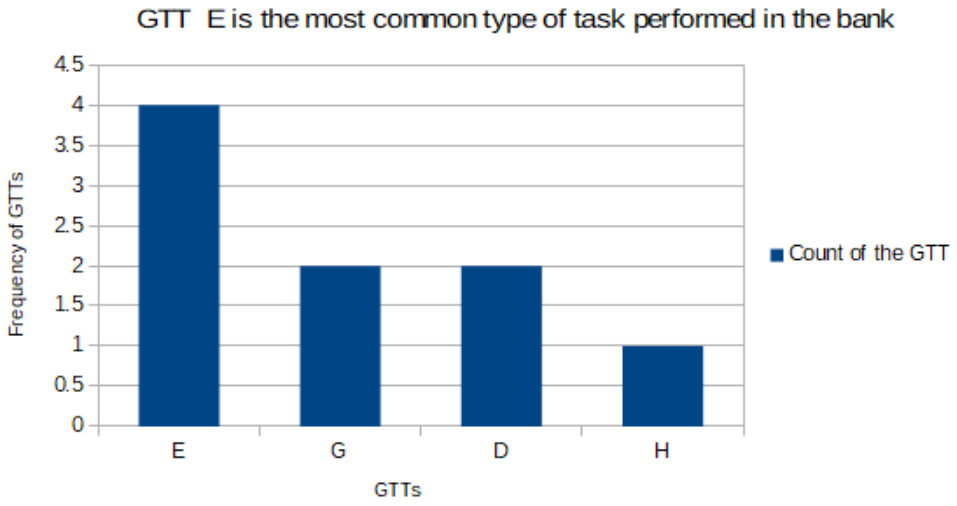
system confirmation are top causes for human error in the bank. Although three of these EPCs show greater frequency of being selected as causes, EPC 14 and 15 have greater effect (multiplier) than EPC 34 shown by table 4.



Graph 1: Error producing or causing conditions Results

4.3.2 Generic task type results

The following graph shown (graph 2) below depicts the distribution of the generic tasks with respect to their frequency under the bank. Four out of the nine GTTs are mapped to the divisions of the bank under this study. As per the graph shown below (graph 2) most of the tasks performed within the bank divisions is a routine work which is highly practised with speedy execution (GTT E). This is then followed by GTT G and D then GTT H follows being the only task mapped only to one division namely information system.



Graph 2: Distribution of Generic Task Types classification within the bank results

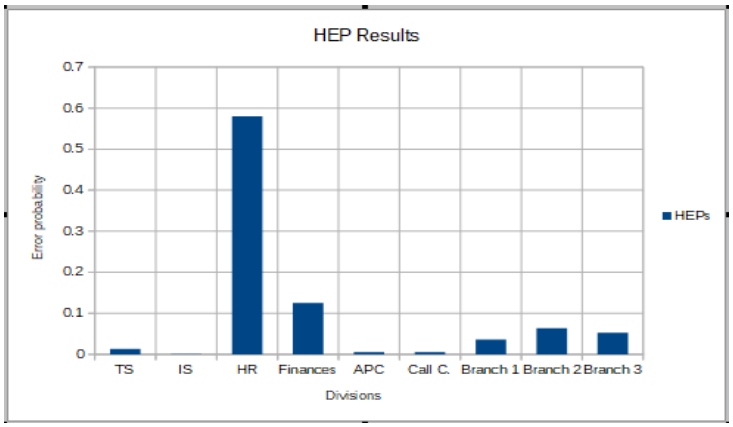
According to HEART each task has a nominal multiplier which was built upon previous incidents occurrence. Following the interview each division of the bank studied were classified under HEART generic tasks which have a multiplier shown below on table 6 that goes in to probability calculation of equation 3.

Departments	Generic Task Types	GTT Multipliers (Nominal probability)
Trade Services	G	0.0004
Information System	H	0.00002
Human Resources	D	0.09
Finances	E	0.02
Alternative Payment Channel	D	0.09
Call Center	G	0.0004
Branch 1	E	0.02
Branch 2	E	0.02
Branch 3	E	0.02

Table 6: Generic Task Types Classification of divisions Results

4.3.3 Human Error Probability (HEP) results

Each generic task type of HEART has an assigned proposed nominal human reliability ranging from 0.00002 to 0.55 which might be confused with the human error probability discussed under this section. The former is a nominal number assigned by the method, while the latter is the calculated probability using the equation given on chapter three. Thus, the probability of human unreliability or error for each division predicted by HEART is depicted on the graph below (graph 3). The probability of human error within Human resources, finances and branches office are predicted with higher probability of failure as compared to the rest of the divisions indicating for a significant human error leading up to information security incident.



Graph 3: Human Error Probabilities of each division Results

4.4 Results per Division

This section presents the result obtained from analysis of the data from interview regarding the research objective. This study resulted in quantitative data. This section has nine parts each with division result of tasks and factors.

4.4.1 Trade Service

This division has more experienced experts among other divisions next to call center division. All experts agree that they experience error frequently. The Generic Category selected by the experts was Category Task G (Completely familiar task). However, the team felt that the task did not allow sufficient time to correct potential error (the one element of the generic task description that did not appropriately match the task being analysed). This Category has a Human *Error Probability* of 0.0130 indicating most probable task subjected for human error but which is found to be one of the least human unreliable tasks as compared to other divisions of the bank as shown on graph 3.

The Error producing conditions (EPCs) that were selected by the team as having the greatest influence on human error are provided below in Table 7. Due to the workload on the staff and the number of data to be entered there is little time to check the entries for error. As a result, *Shortage of time available for error detection and correction* is the primary contributor to the overall Human Error Probability under trade services unit. The secondary and tertiary contributors to Human Error Probability are both *None clear and timely confirmation from the system, and Prolonged activity/ highly repetitive low mental work load tasks* respectively as shown on Table 6.

EPC	% Contribution to unreliability
14: No clear and timely confirmation from the portion of the system over which control is to be applied.	25.23%
2: A lack of time accessible for error discovery and adjustment	67.64%
34: Prolonged activity/ highly repetitious low mental workload tasks	8.13%

Table 7: Contribution of top Human error causes or EPCs to Trade S. HEP

4.4.2 Human Resources

Human resources division has a highest probability of human error and is categorized as GTT D which relate to routine and simple tasks. This Category has a *Human Error Probability* of 0.580 indicating the most probable task subject to human error as compared to other units of the bank as shown on graph 3. Table 8 summarizes the factors for human error within this division as shown below. Lack of timely system information on confirmation has been mentioned as a main cause for human error by the experts. Hence, *no clear and timely response from the system* is the *primary*

contributor to the overall Human Error Probability under this division. The *secondary* and *tertiary* contributors to Human Error Probability are *Inexperienced person performing the task* and *the Information displayed and how it is applied not fully being understood by the person* respectively as shown on Table 8.

EPC	% Contribution to unreliability
15: Inexperience of the person performing the task	39.42%
32: Information displayed and how this is applied not fully understood	18.19%
14:The system information confirmation	40.91%

Table 8: Contribution of top Human error causes or EPCs to HR HEP

4.4.3 Finances

Finances has the second most probable probability following human resources its selected as category of Task E which is routine and highly practised task. This division has a *Human Error Probability* of 0.125 as shown on graph 3. The EPCs that were selected by the team as having the greatest influence on human error is provided below on Table 9. Within finances division similar feedback has been observed as human resources. Accordingly, *Lack* of timely system information on confirmation has been has also been mentioned as the main cause by the experts. Hence, both *none clear and timely validation from the system* is the primary contributor to the overall Human Error Probability under this division. The *secondary* and *tertiary* contributors to Human Error Probability are *Inexperienced person performing the task* and *Task pacing caused by the intervention of others* respectively as shown in Table 9.

EPC	% Contribution to unreliability
14: The system information confirmation	49.71%
36: Pressure from someone else to increase the speed or pace	16.77%
15: Inexperience of the person performing the task	32.06%

Table 9: Contribution of top Human error causes or EPCs to Finances HEP

4.4.4 Information System

The Information system division mainly the SOC of information security unit within CBE is classified as a different task among other divisions within this study. Until recently the security of the bank operation was supported by the national CERT inside INSA. Now the SOC has a similar monitory system for banking operations run by information system division. This division addressed the security operation center of CBE employing qualified operational cybersecurity

professionals who are responsible for response of network intrusion or any incident against CBE network. The Generic category task H (responding to system command even with the supervisory system providing accurate interpretation of system state) is selected by the experts working inside this division. This category has a Human *Error Probability* of 0.00008033 which is a probable task subject for human error but it was identified as the least human unreliable task as compared to the rest of the divisions as shown on graph 3. The causes for possible human error selected by the team as having the greatest influence are provided below in Table 10. Hence, *person performing the task being required to learn a new technique, process* is the primary contributor to the total Human Error Probability for this division. *Prolonged activity/ highly repetitious low mental work loaded tasks* and *disruption of normal work-sleep cycles* have shown the same contribution to the overall Human Error Probability which is 29.43% as shown on table 10.

EPC	% Contribution to unreliability
34: Long activity and highly repetitious	29.43%
35: Interruption of usual work and sleep scedule	29.43%
9: Person performing the task required to learn a new technique, process, etc.	41.13%

Table 10: Contribution of top Human error causes or EPCs to IS HEP

4.4.5 Branch 2

All the branches within this study are categorized as Task E (routine and highly practised) which include branch 2 as referred within this study and they have similar probabilities for error. This category has a *Human Error Probability* of 0.0637 which is one of the most probable task for human error as compared to the rest of the divisions of the bank as shown on graph 3. The EPCs that were selected by the team as having the greatest influence for error on the task performance is provided below on Table 11. Tasks at branches of the bank are mainly routine activities which are highly practised as a result experience of branch operation officers is very crucial. Thus, *"Inexperienced person performing the task"* is the primary contributor to the overall Human Error Probability for this division. The *secondary* and *tertiary* contributors to Human Error Probability are *High-level emotional stress and Low workforce morale* respectively as shown on Table 11.

EPC	% Contribution to unreliability
31: Low workforce morale	24.14%
29: High-level emotional stress	24.96%

15: Inexperience of the person performing the task	50.48%

Table 11: Contribution of top Human error causes or EPCs to Branch 2 HEP

4.4.6 Branch 3

This branch is also categorized as Task E. Thus has a *Human Error Probability* of 0.0524 which is one of the most probable tasks subjected for human error as shown on graph 3. Table 12 sums up the EPCs that were selected by the team as having the greatest influence on human error. This branch has also the same results as branch 3 showing similarity on the basic tasks and procedures followed by branches. Thus, *inexperienced person performing the task* is the primary contributor to the overall Human Error Probability under this division. The *secondary* and *tertiary* contributors to Human Error Probability are *Prolonged activity/ highly repetitious low mental work loaded tasks and Pressure from someone else to increase the speed or pace respectively* as shown on Table 12.

EPC	% Contribution to unreliability
36: Pressure from someone else to increase the speed or pace	23.14%
34: Prolonged activity/ highly repetitious low mental workload tasks	23.25%
15: Inexperience of the person performing the task	52.88%

Table 12: Contribution of top Human error causes or EPCs to Branch 3 HEP

4.4.7 Branch 1

As mentioned above branch 1 also falls under task E implying a routine and highly practised. It has a Human *Error Probability* of 0.02 which is one of the most possible tasks for human fault as compared to other divisions of the bank as shown on graph 3.

The EPCs that were nominated by the experts to have the greatest influence on human error are provided below on Table 13. This branch has also the same results as branch 3 showing similarity on the basic tasks and procedures followed by branches. Thus, *Inexperienced person performing the task* is the primary contributor to the overall Human Error Probability under this unit. The *secondary* and *tertiary* contributors to Human Error Probability are *Prolonged activity/ highly repetitious low mental work loaded tasks and Pressure from someone else to increase the speed or pace* respectively as shown on Table 13.

EPC	% Contribution to unreliability
31: Low workforce morale	29.45%

34: Prolonged activity/ highly repetitious low mental workload tasks	28.40%
22: Little opportunity, such as rest breaks, to exercise etc.	41.62%

Table 13: Contribution of top Human error causes or EPCs to Branch 1 HEP

4.4.8 Alternative Payment Channel

Alternative payment channel is mapped to GTT D which is fairly a simple task performed rapidly or given scant attention. Human error probability predicted by HEART is 0.09 which is again one of the probable tasks subjected to human error as compared to the rest of the divisions of the bank as shown on graph 3. The causes having the greater influence on human error are provided below in Table *14*. Thus, t*he person performing the task lacking an understanding of the policy, standards, process or procedures they are required to adhere to* is the primary contributor to the overall Human Error Probability under this division. Next, the *secondary* and *tertiary* contributors to Human Error Probability are *inexperienced person performing the task and low workforce morale* respectively as shown on Table 14.

EPC	% Contribution to unreliability
31:Low workforce morale	12.73%
11: The person performing the task does not fully understand the policy, etc.	54.25%
15: Inexperience of the person performing the task	33.02%

Table 14: Contribution of top Human error causes or EPCs to APC HEP

4.4.9 Call Center

Employees within this division are relatively more experienced than the rest of the divisions of CBE. They give support both from the business and IT perspective. Employees within this division mention the unclear duties and responsibilities of the task they are required to achieve. This division is mapped to task G (Fairly simple task performed rapidly or given scant attention with the human error probability of 0.005 making it one of the least probable tasks subjected to human error as compared to other units of the bank shown on graph 3. This result considers *he person performing the task lacking an understanding of the policy, standards, process or procedures they are required to adhere to* as the primary contributor to the overall Human Error Probability under this division. The *secondary* and *tertiary* contributors to human error probability are *unclear allocation of role and responsibility and inexperienced person performing the task* respectively as shown on Table 15.

EPC	% Contribution to unreliability

11:The person performing the task does not fully understand the policy, etc.	41.63%
15: Inexperience of the person performing the task	27.85%
25: Unclear allocation of role and responsibility	30.52%

Table 15: Contribution of top Human error causes or EPCs to Call Center HEP

4.5 Discussion

In general, almost all of the divisions under the study make their own risk assessments and forward it to the risk assessment unit; mostly risks related with the tasks they are performing. The bank has a software which monitors human activity online and basically takes care of inappropriate activities on the system. This software is a machine learning technology that keeps millions of logging files and activities used by many banking organizations. But the researcher learned that most of the units don't utilize the software since it detects for the most part inappropriate activities. Hence, most errors made by privileged employees could bypass this system unless they are checked by the experts. This adds more audit work load on the experts besides the normal activity they perform on a daily basis.

Among the nine types of tasks from HEART only four of them were mapped to the tasks within the divisions of the bank. These are GTT E, D, G and H and more than three divisions are categorized under the same task or GTT. The most unreliable tasks in the bank fall under GTT D followed by GTT E; these divisions are Human resources, Finances and branch offices as shown on graph 3. Accordingly, Human resource is predicted to be the most probable task for human error with the HEP of 0.058 followed by Finances division and branch offices. System information confirmation/feedback inadequacy contributes the highest which is 40.91% to the human error probability for human resources division.

It was evident during the analysis that there was some misunderstanding of the background and intended use of the generic error categories and the meaning of the EPCs in their current format by the analysts, e.g. it is apparent from Williams (1986) that Task E is underpinned by error data relating to manual data entry.

This result is similar to the finding of the research (Evans, et al., 2019) where they confirmed this by analyzing a database of human error incidents. The most common tasks were GTTs E and D, they accounted for 89.9% of the reported and validated human error related incidents showing that reported incidents tended to relate to routine and simple tasks. From the database of reported incidents, tasks in GTT D were mainly from entering, updating or deleting data within a system, file or document. In addition, information or equipment safeguard, destruction, deliverance and administration of a system have also been reported as information security affecting tasks. The

human resources division task vulnerability could be aggravated by factors related with system response difficulties, inexperienced worker and inconsistency of meaning of displays from the system and procedures as shown in table 8. Although the human error probability predicted is less than the others, alternative payment channel division also falls under task D which makes the task as vulnerable as the human resources division. But due to differently rated error factors this division is predicted with the less probability to human error as compared to the human resources.

Finances and branches office account for the second highest error prone task showing they also tend to relate to routine and simple tasks. These type of tasks have a history of human error through activities such as filling or sorting of information, scanning, printing and verbal communication of confidential data. Even though, divisions under this task have closely related likelihood of human error, finances have a larger predictability than the others which makes it more close to the human resources. This is explained by the error factors shown on table 9. The results show that significant proportion of human error relate to prolonged activity/highly repetitious workloads, Inexperience of the personal performing the task and inadequate system information confirmation/feedback. The system information confirmation or response difficulty is the primary error factor which is shared with the human resources.

Tasks classified under GTT G are subject to information security incidents known generally through providing information verbally, reading and sending an email, file, document or item, accessing location and sharing of information or equipment in person (Evans et, al, 2019). Trade services has higher probability number than the call center which is again explained by its multiplier of the factor given by HEART. In fact, this factor has the greatest multiplier among the EPCs within this study.

It's a lack of time accessible for error discovery and adjustment. From observation trade services is the busiest division within the bank. They communicate more verbally than the others they also engage with customers in person around their desk.

Information security unit particularly SOC of CBE in this study is the least human unreliable task as compared to the rest of the divisions; it is also a task with the least reported incidents in the literature (Evans et al, 2019). Although there are reports of human error coming from activities such as entry and update of information, requirement of learning a new technique, process or procedure during a task is the second most higher factor among the EPCs listed for this bank by its multiplier. Within this unit most of the employees are cyber security analysts working with shift to monitor the bank's activity. They are required to give immediate responses when a certain case is considered a security incident. So this might involve coming up with the best security solution that

will resolve the situation. On the other hand, the task is enriched with one of the best supervisory systems providing precise interpretation of the system state. Overall, the tasks' instrument compensates for the possible fault employees might make.

Tasks under GTT G (Trade S., and Call C.) are highly practised which are subject to information security incident related with communication via email, accessing of location and verbal communication of vital information. In addition, most common activities leading to incident within these tasks include sending of email to a wrong recipient or attaching unintended file and leaking of vital information to unauthorised person including misinforming as a result of verbal communication which is aggravated by the speedy working environment accompanying the division. As a result, confidentiality of information within this division could be compromised. Management has to be aware that shortage of time is likely to impair the reliability of decisions and should ensure that sensitive decisions are not being taken against the clock. In addition, the required performance standards must be tested for comprehensibility on the user population to ensure that there is no ambiguity. Organizational development specialists and/or behavioural scientists should be involved in facilitating the preparation of satisfactory working protocol. Further improvements could be achieved by means of training to appreciate the cost of failure, and also introduction of supportive systems or increasing the amounts of supervision. Human resources and Alternative Payment Channel are mainly susceptible to incidents accompanying data entry, deletion and update within a system, file or document. Tasks under this category are accompanied by manual access to data such as data entry, deletion or modification which could again expose the integrity and availability of information.

Finances and branch offices are mainly subject to incidents related with posting an item or information and filling in or sorting of information which include wrong data passing through the system which costs the organization and making changes to user accounts unintentionally. In addition, password handling is also a concern that obstructs the user from the normal task procedures which needs systems like secure password management system and authentication tokens which minimizes the risk of humans mishandling confidential information either verbally or written and remembering to remove ex-employees' password from the system as well.

CHAPTER FIVE

CONCLUSION AND RECOMMENDATIONS

This chapter presents conclusion by summarizing the research outcomes and recommendations the bank based on the analysis and findings of the research drawn from this study. This portion also lists recommendations for future research.

5.1 Conclusion

The purpose of this study is to identify causes of information security incident through identifying the tasks and factors to reduce the consequences for future improvements.

Researches are reported that majority of incidents are caused by human error compared to technological vulnerabilities. Thus it is important to study the factors behind each human error. Based on the look at the current literature it is apparent that high reliability sectors underline the importance of socio-organizational analysis approaches to determine human errors in the workplace. This research is conducted using Human reliability analysis method to perform a prospective analysis of tasks in order to enhance information security within the bank. It is a study of causes of human error on the subject of information security at a public financial organization, CBE.

The primary objective of this research is to identify the human error factors to ensure information security. This research is a case study by using HEART method which is both a quantitative and qualitative method on purposefully selected divisions of the bank to collect data.

Human resources, finances and branch offices are predicted with a higher probability for human error respectively. This shows that divisions with relatively high human involvement have shown significant error probability. Accordingly, human resource is predicted to be the most probable task for human error with the probability of failure 0.58. System information confirmation /feedback inadequacy contributes the highest among the factors for the probability of error which is 40.91% within human resource division.

Finance office has a Human Error Probability of 0.125 indicating the second most probable task for human error. This division shares the primary factor with the human resources division which is the system response difficulty as mentioned above with 49.71% contribution to the over all probability. Branches of the bank show similar prediction with each other following finances. This is justified by the similarity in their type of tasks and the factors they consider as an indication for human failure.

In general operator inexperience, highly repetitious tasks and delayed or unclear system confirmation are estimated to be the top causes or factors for human error in the bank.

The research was applied by a small team of experienced staff to achieve a more insightful, comprehensive and accurate analysis of the task. The interview used 9 generic task types (GTTs) and 38 Error Producing Conditions which are mapped within the selected divisions of CBE. Out of nine task types only four of them were mapped in this study implying that most tasks from the divisions are alike in terms of their daily activity. When using HEART APOA measurement is known to be the most difficult step of the process. Hence, as recommended by a similar research in the literature decimal approach rather than percentages is used to collect the APOA which simplified the accurate (pessimistic) scoring as well as enabled the calculation of the nominal likelihood of failure and also Graphical Rating Score (GRS). Graphical rating score (GRS) is used to take the experts rating of EPCs or core human error causes. During each interview top three EPCs were selected by the interviewees with their rating within a range between 0 and 1. Again as suggested by other researches for validity purpose no more than three EPCs were selected for each division. Following this, the ratings of the interviewees for each division were converted in to a mean value using geometric mean unlike arithmetic mean which considers the pessimistic result required by HEART.

Safeguards that protect against the loss of integrity as a result of human error include access control such as encryption and digital signatures, process controls, monitoring controls such as file integrity monitoring and effective log analysis and behavioural controls such as separation of duties, rotation of duties, and training.

Highly repetitious and work loaded tasks are extremely susceptible to human error which could be minimized with either support system or minimizing a single individual being subjected to prolonged repetitious task. Highly repetitious cycling of low mental workload tasks must be avoided generally when it involves little or no variability. Job enrichment (with the introduction of different, more varied tasks) has been found to minimise tediousness, and better hold attention. Rather than combat these effects, it is better to ensure that such conditions do not arise in the first place i.e. observation tasks demanding high human reliability should never require sessions of longer than one hour's concentration and should not be designed accordingly.

Regarding experiences, personnel criteria should contain specific experience parameters thought relevant to the task and chances must not be taken for the sake of advantage. It's also recommended that system response times in general should never exceed four seconds and there must always be sufficient information to enable operators to step confidently on to the next part of a task and if

doubt exists the feedback is incomplete (Williams, 1986). The findings indicate that there is an obligation for the organizations to ensure effective and flexible system which can assistance the task of the employees. In general, the personnel criteria and system response feedback difficulties mentioned are also the main concerns which could be proactively handled.

Some of the expected limitations of the method throughout the course of the case study include the estimation of APOAs. APOAs driven from most of the EPCs tend to subject to experts but recommended approaches by similar researches have been used which are decimal presentation of the GRS and a geometric average of the experts' judgement instead of arithmetic means. Following the case study, the researcher came to conclude that HEART is indeed applicable to the information security field. Consequently, resources should be allocated in reducing the prioritized tasks discussed on in this research for prospective damage they bring to the bank. Therefore, a reduction in human error generally would be expected to significantly reduce the volumes of information security incidents.

5.2 Recommendation

Based on the findings obtained from the analysis of the study, recommendations for improvement of the future condition are presented as follows.

5.2.1 Future work

This study provides different insights to human errors by adopting HRA methods to information security field particularly to organizational or business setup that will yields better quantitative predictions. HEART is basically a generic task analysis tool future research is to make the scope to address very specific tasks from a retrospective aspect which showed promising results as seen from literature. Using the actual reported human error records to validate and modify HEART approach with respect to the specific organization is also the best way to observe the effect of HEART prediction. Also future studies are recommended to compare the many ways of eliciting expert judgements for team based HEART assessments since APOA assignment is known as the most difficult measurement required from the assessor. Investigation of the relation between different error factors or EPCs is also recommended for future work.

5.2.2 Recommendation for CBE

The Established information security team has to conduct regular rehearsal on human factor risk to gain understanding on the layers of information security leading to information security incident. Focus on challenging areas such as human factor vulnerability and quantification of those elements during risk assessment for better decision making. Human resources and finance divisions are more subject to information security incident due to human error which should be considered for better

security. While conducting the interview system information response was complained by most employees which is clearly felt by most customers of CBE. The result after using HEART also pointed out this fact as EPC 32 and 14 being one of the top factors for error within these divisions. Hence, the system which supports day to day activity of these divisions should be considered as vulnerability and prioritized accordingly.

Reference

[1]. Adhikari S, Bayley Tim Bedford C, Busby J, Cliffe A, Eid M, French S, et.al. (2009). Working paper series human reliability analysis: a review and critique.

[2]. Ahmad A, Hadgkiss J, Ruighaver AB. (2012) Incident response team's e challenges in supporting the organizational security function. doi: 10.1016/j.cose.2012.04.001.

[3]. Abraham. A. (2011) Information Security Behaviour: Factors and Research Directions.

[4]. Alvarez M, Bradley N, Cobb P, Craig S, Iffert R, & Kessem, L. et.al. (2017). IBM X-Force Threat Intelligence Index 2017 The Year of the Mega Breach:1–30.

[5]. Anderson, R. J. (2008). Security Engineering: A Guide to Building Dependable Distributed Systems.2nd ed.

[6]. Hovav, J. D'arcy. (2012). Applying an extended model of deterrence across cultures: an investigation of information systems misuse in the U.S. and South Korea. https://doi.org/10.1016/j.im.2011.12.005.

[7]. Baskarada, S. (2014). Qualitative case study guidelines.

[8]. Bell J, Holroyd J. (2009). Review of human reliability assessment methods. Heal Saf Lab.

[9]. Bye, A., Lois, E., Dang, V.N., Parry, G., Forester, J., Massaiu, S., Boring, R., 59 Braarud, P.0., Broberg, H., Julius, J., Mannisti), I. & Nelson, P. (2011). International HRA Empirical Study- Phase 2 Report: Results from Comparing HRA Method Predictions to Simulator Data from SGTR Scenarios.

[10]. B. Bulgurcu, H. Cavusoglu, I. Benbasat. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness, MIS Q. 34 (3) 523–548.

[11]. B.-Y. Ng, A. Kankanhalli, Y. Xu. (2008). Studying users' computer security behaviour: a health belief perspective, Decis. Support Syst. 46 815–825, https://doi.org/10.1016/j.dss.2008.11.010.

[12]. Creswell, J. W. (2014). Research design: qualitative, quantitative, and mixed methods approaches (4th ed.). USA: Sage Publications.

[13]. Chadwick, L., & Fallon, E. (2012). Human reliability assessment of a critical nursing task in a radiotherapy treatment process. Applied Ergonomics, 43(1), 89-97.

[14]. Chandler T, Chang J, Mosleb A, J. M, Boring R, Gertman D. (2006). Human Reliability Analysis Methods Selection Guidance for NASA. Natl Aeronaut Sp Adm 2006:175. Department of Health. IG Publications.

[15]. Carayon, P. and Smith, M.J. (2000), Work organization and ergonomics, Appl. Ergonomics, 31, 649–662.

[16]. David Bisson. (2019). 7 Data Breaches Caused by Human Error: Did Encryption Play a Role? https://www.venafi.com/blog/7-data-breaches-caused-human-error-did-encryption-play-role

[17]. Deloitte (2008). Global Financial Services Industry (GFSI) Security Survey. http://www.deloitte.com/assets/Dcom-Global /Local%20Assets/Documents/Financial%20Service

[18]. Dhillon BS. (2003). Human reliability and error in medical system. doi:10.1142/5264.

[19]. Diefenbach, T. (2009). Are case studies more than sophisticated story telling? Methodological problems of case studies mainly based on semi-structured interviews. Quality and Quantity, 43(6), 875-894. https://doi.org/10.1007/s11135-008-9164-0/.

[20]. Dawson, C. (2002). Practical Research Methods. Oxford, United Kingdom: How to Books engineering case study? Empirical Software Engineering, 7(1), 9-26.

[21]. Denzin,N.K.(1970).The research act: A theoretical introduction to sociological methods. Chicago: Aldine publishing co.

[22]. Dhillon, G., and Backhouse, J. (2001). Current directions in IS security research: towards socio organizational perspectives, Information Systems Journal, 11, pp.127-153, 2001.

[23]. Erlend Andreas Gjære. (2017) Human Errors in Cyber Security A Swiss Cheese of Failures. https://securityandpeople.com/2017/07/human-errors-in-cyber-security-a-swiss-cheese-of-failures/.

[24]. Evans, Mark & He, Ying & Maglaras, Leandros & Yevseyeva, I. & Janicke, Helge. (2019). Evaluating Information Security Core Human Error Causes (IS- CHEC) Technique in Public Sector and Comparison with the Private Sector. International Journal of Medical Informatics. 127. 10.1016/j.ijmedinf.2019.04.019.

[25]. French S, Bedford T, Pollard SJT, Soane E. (2011). Human reliability analysis: a critique and review for managers. Saf Sci2011; 49:753–63. doi: 10.1016/j.ssci.2011.02.008.

[26]. Furnell, S., & Clarke, N. (2005). Organisational Security Culture: Embedding Security Awareness, Education and Training.

[27]. Furnell, S., & Thomson, K. (2009). 'From culture to disobedience: Recognising the varying user acceptance of IT security', Computer Fraud Security, Vol. No 2, 1999, pp. 5–10.

[28]. Goodliff PB, Widdowson AJ. (2015). CHEAT, an approach to incorporating human factors in cyber security assessments.

[29]. Grispos, G. (2016). On the enhancement of data quality in security incident response investigations:284

[30]. Gertman DI. (2013). Automation, cyber security and risk assessment: HRA where art thou? Trans Am Nucl Sc 2013; 109:2030–3.

[31]. Gu T, Li L, Lu M, Li J. (2014). Research on the calculation method of information security risk assessment considering human reliability. In: Proceedings of the 2014 10th international conference reliability maintainability safety, IEEE.p. 457–62. doi:10.1109/ICRMS.2014.7107238.

[32]. Harwell, M. R. (n.d). Research design in qualitative/quantitative/mixed methods.

[33]. He, Y. (2014). Generic Security Templates for information system security arguments Mapping security arguments within healthcare systems.

[34]. H.G. Djajadikerta, S. Mat, R.T. Trireksani. (2015). Dysfunctional information system behaviours are not all created the same: challenges to the generalizability of security-based research, Inf. Manag. 52 (2015) 1012–1024, https://doi.org/10.1016/j.im.2015.07.008.

[35]. HMG. (2016). National cyber security strategy.

[36]. Holroyd, J. (2009). Review of human reliability assessment methods. Health & Safety Laboratory.

[37]. HSCIC. (2015). Checklist guidance for reporting, managing and investigating information governance and cyber checklist guidance for reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation:1–48.

[38]. IBM Chief Information Security Officer Assessment. (2014). https://www.ibm.com/common/ssi/cgi/bin/ssialias?subtype=ST&infotype=SA&appname=SWGE_WG_WG_USEN&htmlfid=WGJ03008USEN&attachment=WGJ03008USEN.PDF&ce=ISM0484&ct=SWG&cmp=IBMSocial&cm=h&cr=Security&ccy=US

[39]. IBM Global Technology Services. (2014). IBM security services 2014 cyber security intelligence index.

[40]. Information Commissioner's Office. (2012). ICO lo Guidance on data security breach management.

[41]. Information security breaches survey report. (2015). https://www.gov.uk/government/organisations/department-for-business-innovation-skills

[42]. Information Security Forum. (2019). Information Security Forum Tackles Human-Centered Security in Latest Paper

[43]. Insurance Times. (2014). Human error: the biggest cyber security threat? https://www.insurancetimes.co.uk/human-error-the-biggest-cyber-security-threat-/1410557

[44]. Johannesen L, Sarter N, & Cook R. (2010). Behind human error. Pro Quest E-book Central.

[45]. Kelly R. (2017). Almost 90% of cyber-attacks are caused by human error or behaviour, https://non-consecutive/almost-90-cyber-attacks-caused-human-error-behaviour

[46]. Kirwan. (1997). Human factors methods a practical guide for engineering.

[47]. Kothari, C. (2004). Research Methodology: Methods and Techniques (2nd Revised ed.). New Delhi: New Age International (P) Ltd.

[48]. Kruger. (2006). Forming the awareness of employees in the fields of information security.

[49]. Kumar, R. (2011). Research methodology-a step-by-step guide for beginners. Sage Publication.

[50]. Lawton, R. (1998). Not working to rule: Understanding procedural violations at work. Safety Science, 28(2), 77–95. https://doi.org/10.1016/S0925-7535(97)00073-8

[51]. Le Comple, M.D &Goetz,J.p.(1982).problems of reliability and validity in ethnographic research. Review of educational Research 52(no1) 31-60

[52]. Liginlal D, Sim I, Khansa L. (2009). How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management. Computer Secur2009; 28:215–28. doi: 10.1016/j.cose.2008.11.003.

[53]. Lilia. (2017). Employees' Impact on Cyber Security Human Behaviour Consequences on security measures.

[54]. Kraemer, S. & Carayon, P. (2007). Human errors and violations in computer and information security: the viewpoint of network administrators and security specialists. Applied Ergonomics, 38(2007), 143-154.

[55]. Maddah S, Ghasemi M. (2015). Provide guidance to choose appropriate method to evaluate human error. New York Sci J 2015; 8:35–41.

[56]. Marine Corp Times. (2018). Major data breach at marine forces reserve impacts thousands.

[57]. Metalidoua, Marinagi, Trivellas, Eberhagen, Skourlas, Giannakopoulos. (2014). The Human Factor of Information Security: Unintentional Damage Perspective.

[58]. McKelvie, S. J. (1987). Graphic rating scales - how many categories? British Journal of Psychology, 69(2), 185-202. doi:10.1111/j.2044-8295. 1978.tb01647. x.

[59]. M. Evans, L.A. Maglaras, Y. He, H. Janicke. (2016). Human behaviour as an aspect of cybersecurity assurance, Secur. Communication. Netw. 9 4667–4679, https://doi.org/10.1002/sec.1657.

[60]. M. Evans, L. Maglaras, Y. He, H. Janicke. (2019). HEART-IS: a novel technique for evaluating human error-related information security incidents, Computer. Secur. 8074–89

[61]. M. Evans, Y. He, I. Yevseyeva, H. Janicke. (2017). Analysis of published public sector information security incidents and breaches to establish the proportions of human error, Proc. 12th Int. Conf. Hum. Asp. Information Secur. Assur. - HAISA pp. 911–921.

[62]. M. Alnatheer and K. Nelson. (2009). "A Proposed Framework for Understanding Information Security Culture and Practices in the Saudi Context," in 7th Australian Information Security Management Conference, no. December, pp. 1–3 6.

[63]. National Security Agency (2015). Science of Security (SoS) Initiative Annual Report 2015.

[64]. http://cps-vo.org/sos/annualreport2015.

[65]. National Cyber Security Centre. (2017). National cyber security centres incident management. https://www.ncsc.gov.uk/incident-management .

[66]. Negussie, A. (2015). Practices, Challenges & Prospects of Information Security Policy in pp.22-33.

[67]. NHS Digital. (2017). NHS information governance toolkit, https://www.igt.hscic.gov.uk/ .

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

[69]. PCI Security Standards Council. (2016). Payment Card Industry Data Security Standard (PCI DSS) and Payment Application Data Security Standard (PA-DSS).

[70]. Pfleeger. (1997). Security in computing.

[71]. P. Ifinedo. (2014). Information systems security policy compliance: an empirical study of the effects of socialisation, influence, and cognition. https://doi.org/10.1016/j.im.2013.10.001.

[72]. P. Puhakainen, M. Siponen. (2010). Improving employees' compliance through information M. Siponen, A. Vance, Neutralization: new insights into the problem of employee information systems security policy violations, MIS Q. 34 487–502, https://doi.org/10.2307/25750688.

[73]. J. Rajamaki, J. Nevmerzhitskaya, and C. Virag, (2018) "Cybersecurity education and training in hospitals: Proactive resilience educational framework (Prosilience EF)," IEEE Global Engineering Education Conference (EDUCON), pp. 2042–2046.

[74]. Razvan Muresan (2019). Addressing the Human Error Causes of Security Breaches. https://businessinsights.bitdefender.com/addressing-human-error-causes-security-breaches

[75]. Reason, J. (1997). Managing the Risks of Organizational Accidents. Ashgate, Brookfield.

[76]. Reason, J. (1990). Human Error, Cambridge, UK: Cambridge University Press.

[77]. Reason, P and Rowan, J (eds). (1981), Human inquiry: a sourcebook of new paradigm research, Chichester: John Wiley.

[78]. Reason J. (2000). Human error: models and management. BMJ; 320:768–70. doi:10.1136/BMJ.320.7237.768.

[79]. Safa NS, von SolmsR, Futcher L. (2016). Human aspects of information security in organizations. Computer Fraud Secur2016:15–18. doi:10.1016/S1361-3723(16)30017-3.

[80]. Selltiz et.al. (1976). Validity and reliability in qualitative research.

[81]. S. Furnell, W. Khern-am-nuai, R. Esmael, W. Yang, N. Li. (2018). Enhancing security behaviour by supporting the user, Computer. Secur. 75 1–9, https://doi.org/10.1016/j.cose.2018.01.016.

[82]. S.R. Boss, L.J. Kirsch, I. Angermeier, R.A. Shingler, R.W. Boss.(2009)..If someone is watching, I'll do what I'm asked: mandatories, control, and information security,Eur. J. Inf. Syst. 18 151–164, https://doi.org/10.1057/ejis.2009.8.

[83]. Saunders, M., Lewis, P., & Thornhill, A. (2009). Research methods for business students. Italy: Rotolito Lombarda.

[84]. Sari Greene. (2017). sage data security. http://www.amazon.com/Security-Program-Policies-Principles-Certification/dp/0789751674

[85]. Safa NS, von Solms R, Futcher L. (2016). Human aspects of information security in organizations. Computer Fraud Secur 2016:15–18. Doi:10.1016/S1361-3723(16)30017-3.

[86]. Saunders, M., Lewis, P., & Thornhill, A. (2009). Research methods for business students. Security Culture and Practices in the Saudi Context. Proceedings of the 7th Australian Symposium on Human Aspects of Information Security & Assurance.

[87]. Schultz, P. W., Gouveia, V. V., Cameron, L. D., Tankha, G., Schmuck, P., & Franek, M. (2005).

[88]. Values and their relationship to environmental concern and conservation behavior. Journal of

[89]. Cross-Cultural Psychology, 36, 457-475.

[90]. Simon, K. M. (2011). Validity and reliability in qualitative research.

[91]. Swain, A. D., & Guttman, H. E. (1983). Handbook of human reliability analysis with emphasis on

[92]. nuclear power plant applications. NUREG/CR-1278, U.S. Nuclear Regulatory Commission.

[93]. (Washington D.C.).

[94]. Thales. (2017). CHEAT an updated approach for incorporating human factors in cybersecurity assessments.

[95]. The British Standards Institution. (2017). BSI Standards Publication Information Technology Security techniques. Information security management systems, Overview and vocabulary

[96]. The Inquirer. Human error is the root cause of most data breaches. (2017). The Inquirer (https://www.theinquirer.net/inquirer/sponsored/2320308/human-error-is-the-root-cause-of-most-data-breaches).

[97]. Tøndel IA, Line MB, Jaatun MG. (2014). Information security incident management: current practice as reported in the literature. Computer Secur.45:42–57. doi: 10.1016/J.COSE.2014.05.003.

[98]. Trochim, W. M. (2006). Unit of Analysis. Retrieved from Social research methods: https://www.socialresearchmethods.net/kb/unitanal.php.

[99]. Trend Micro Trend Labs report. (2014). https://blog.trendmicro.com/how-can-enterprises-reduce-the-risk-of-human-error-in-cyber-security/.

[100]. Verizon's. (2019). Data Breach Investigations Report (DBIR)

[101]. Von Solms, van Niekerk (2013). From information security to Cyber security.

[102]. Williams J. C. (1992). A user manual for the HEART human reliability assessment method.

[103]. Williams, J.C. (1986). HEART – a proposed method for assessing and reducing human error.

[104]. Proceedings from 9th Advances in Reliability Technology Symposium. England, West Yorkshire:

[105]. University of Bradford.

[106]. Williams, J.C. (2015). Heart a Proposed Method for Achieving High Reliability in Process Operation by Means of Human Factors Engineering Technology. Safety and Reliability.

[107]. Woretaw, A., & Lessa, L. (2012). Information Security Culture in The Banking Sector.

[108]. Yin, R. K. (2009). Case Study Research: Design and Methods. In 4th (Ed.). London: Sage Publications.

[109]. Young, William & Leveson, Nancy. (2013). Systems thinking for safety and security. 1-8. 10.1145/2523649.2530277.

Appendix 1: HEART EPCs

EPC ID	Error Producing Conditions
1	Unfamiliarity with a situation which is potentially important but which only occurs infrequently or which is novel
2	A shortage of time available for error detection and correction
3	Too many alerts, notifications, messages, or inputs leading to important information not being seen or heard and acted upon
4	Too easy to switch off, disable or incorrectly modify alerts, notifications, messages, or inputs leading to important information being missed or not acted upon
5	No means of communicating information in a form which can be understood and used
6	A mismatch between an operator's model of the world and that imagined by a designer
7	No obvious means of reversing an unintended action
8	Person performing the task monitoring numerous incoming information channels at the same time, such as numerous computer monitors
9	Person performing the task required to learn a new technique, process, procedure or way of working which differs in attitude or way of thinking to the previous one
10	The need to transfer specific knowledge from task to task without loss
11	The person performing the task does not fully understand the policy, standards, process or procedures they are required to adhere to
12	The person performing the task does not understand the actual risk exposure
13	The system information communicated is inaccurate, unclear or inappropriate
14	The system information which confirms that an action has been successfully completed, is delayed, takes too long or does not happen
15	Inexperience of the person performing the task
16	Inaccurate or incomplete information communicated by procedures, or from a person to a person
17	Little or no independent checking or testing of output
18	A conflict between immediate and long-term objectives
19	Not enough information to allow completeness or accuracy checks to be undertaken
20	A mismatch between the educational achievement level of an individual and the requirements of the task
21	An incentive to use other more dangerous procedures
22	Little opportunity, such as rest breaks, to exercise mind and body outside the immediate confines of a job

EPC ID	Error Producing Conditions
23	Unreliable instrumentation used to communicate information leading to lack of trust and person performing the task ignoring information
24	A need for decision making which is beyond the capabilities or experience of the person performing the task
25	Unclear allocation of role and responsibility
26	No obvious way to keep track of progress during an activity
27	Task requirement exceeds the physical capabilities of the person performing the task
28	Person performing the task is unaware of its significance and their contribution to corporate objectives
29	High-level emotional stress
30	Evidence of ill-health amongst operatives, especially fever
31	Low workforce morale
32	Information displayed and how this is applied within procedures or working practices is not fully understood
33	A poor or hostile environment (below 75% of health or life-threatening severity)
34	Prolonged inactivity or highly repetitious low mental workload tasks
35	Disruption of normal work-sleep cycles
36	Pressure from someone else to increase the speed or pace at which a task is performed, beyond an individual's preferred pace and capability
37	Additional team members over and above those necessary to perform task normally and satisfactorily
38	Age of personnel performing perceptual tasks requiring the ability to interpret or become aware of something through the senses (sight, hearing, taste, smell or touch)

Appendix 2: HEART Generic Task Types

Generic Task Type	Description	Proposed Nominal Human Unreliability	5th-95th Percentile Bounds
(A)	Totally unfamiliar, performed at speed with no real idea of likely consequences	0.55	0.35 - 0.97
(B)	Shift or restore system to a new or original state on a single attempt without supervision or procedures	0.26	0.14 - 0.42
(C)	Complex task requiring high level of comprehension and skill	0.16	0.12 - 0.28
(D)	Fairly simple task performed rapidly or given scant attention	0.09	0.06 - 0.13
(E)	Routine, highly-practised, rapid task involving relatively low level of skill	0.025	0.007 - 0.045
(F)	Restore or shift a system to original or new state following procedures, with some checking	0.003	0.0008 - 0.007
(G)	Completely familiar, well-designed, highly-practised, routine task occurring several times per hour, performed to highest possible standards by highly-motivated, highly-trained and experienced person, totally aware of implications of failure, with time to correct potential error, but without the benefit of significant job aids	0.004	0.00008 - 0.009
(H)	Respond correctly to system command even when there is an augmented or automated supervisory system providing accurate interpretation of system state	0.00002	0.000006 – 0.009
(M)	Miscellaneous task for which no description can be found	0.03	0.008-0.11

Appendix 3: Research Interview

Human error Factors: the case of CBE Information security

Dear Respondent,

My name is Mihret Setu. Currently I am attending Master of Science in Information Science at Addis Ababa University, Ethiopia.

My research lies on human based error analysis in information security for CBE. Therefore, this is to kindly ask you to participate in the survey that needs data from your esteemed bank to assess the issues in relation to Information Security.

This survey is anonymous. No one, including the researcher, will associate your responses with your identity. Your participation is voluntary. Your response is extremely important.

Therefore, I appreciate if you spend few minutes from your valuable time according to the instruction for each part.

If you require any clarification, please don't hesitate to contact me through either of the following ways. Tel: 0920-51-96-49 or Email: mihretsetu19@yahoo.com

Thank you for your kind contributions in advance.

Human error Factors: the case of CBE Information security

Job Title_____

CHAPTER 1 – Demographic characteristic	
Q1. What is your professional qualification?	a. Diploma/Level IV b. BA/BSc c. MBA/MA/MSc d. PhD
Q2. Which of the following job categories? Indicate your current position?	a. Management level b. Senior level c. Officer level
Q3. Your working experience?	a. 3-5 years b. 5-10 years c. Above 10 years

CHAPTER 2 – SECURITY INCIDENT	
Q4. How many times your organization ever experienced human based error of information security that you know of?	a. 1 to 5 times b. more than 10 times c. Never experienced
Q5. Have you ever faced with human error incident of information security while working?	a. yes b. never
Q6. Do you think your task is vulnerable to human based information security error?	a. yes b. no

CHAPTER-3 Type of Task you are performing
Q7. Please categorize (**Circle**) the type of task you are performing under one of the following general tasks (**A-M**)
A - Totally unfamiliar, performed at speed with no real idea of likely consequences
B - Shift or restore system to a new or original state on a single attempt without supervision or procedures
C - Complex task requiring high level of comprehension and skill

D - Fairly simple task performed rapidly or given scant attention
E- Routine, highly-practiced, rapid task involving relatively low level of skill
F - Restore or shift a system to original or new state following procedures, with some checking
G - Completely familiar, well-designed, highly practiced, routine task occurring several times per hour, performed to highest possible standards by highly-motivated, highly trained and experienced person, totally aware of implications of failure, with time to correct potential error
H- Respond correctly to system command even when there is an augmented or automated supervisory system providing accurate interpretation of system state
M - Miscellaneous task for which no description can be found

Q7. Instructions: Below are conditions that contribute for the likelihood of error in performing a given task, using the scale provided please rate on average how significant each condition is on the probability of committing an error while performing the task. The higher the number selected, the greater the significance of the condition to potentially cause an error. (Note: If the conditions has no effect or are irrelevant, please select '0' on the scale.)

CHAPTER5 – Error producing conditions for the task you are performing
1. **Unfamiliarity** with a situation, but which only occurs infrequently.
Negligible Minor Moderate Major Extreme 0 1 2 3 4 5 6 7 8 9 10
2. A **shortage of time** available for error **detection** and **correction**.
Negligible Minor Moderate Major Extreme 0 1 2 3 4 5 6 7 8 9 10
3. Too many **alerts**, notifications, messages, or inputs leading to important information not being seen or heard and acted upon
Negligible Minor Moderate Major Extreme 0 1 2 3 4 5 6 7 8 9 10
4. Too easy to switch off, disable or incorrectly modify alerts, notifications, messages, or emails leading to important information being missed

Negligible		Minor		Moderate		Major		Extreme	
0	1	2	3	4	5	6	7	8	9	10

5. No means of **communicating** information in a form which can be understood and used

Negligible		Minor		Moderate		Major		Extreme	
0	1	2	3	4	5	6	7	8	9	10

6. A **mismatch** between an **operator's** model of the world and that imagined by a **designer**

Negligible		Minor		Moderate		Major		Extreme	
0	1	2	3	4	5	6	7	8	9	10

7. No obvious means of **reversing** an **unintended** action

Negligible		Minor		Moderate		Major		Extreme	
0	1	2	3	4	5	6	7	8	9	10

8. Person performing the task **monitoring** numerous incoming information channels at the same time e.g. numerous computer monitors

Negligible		Minor		Moderate		Major		Extreme	
0	1	2	3	4	5	6	7	8	9	10

9. Person performing the task required to **learn** a **new technique**, process or procedure

Negligible		Minor		Moderate		Major		Extreme	
0	1	2	3	4	5	6	7	8	9	10

10. The need to **transfer** specific **knowledge** from task to task without loss

Negligible		Minor		Moderate		Major		Extreme	
0	1	2	3	4	5	6	7	8	9	10

11. The person performing the task does not fully understand the **policy**, **standards**, **process** or **procedures** they are required to adhere to

Negligible		Minor		Moderate		Major		Extreme	
0	1	2	3	4	5	6	7	8	9	10

12. The person performing the task does not understand the actual **risk exposure**

Negligible		Minor		Moderate		Major		Extreme	
0	1	2	3	4	5	6	7	8	9	10

13. **System** information communicated is inaccurate, **unclear** or inappropriate

Negligible		Minor		Moderate		Major		Extreme	
0	1	2	3	4	5	6	7	8	9	10

14. The **system** information which **confirms** that an action has been successfully completed, is delayed, takes too long or does not happen

Negligible		Minor		Moderate		Major		Extreme	
0	1	2	3	4	5	6	7	8	9	10

15. **Inexperience** of the person performing the task

Negligible		Minor		Moderate		Major		Extreme	
0	1	2	3	4	5	6	7	8	9	10

16. Inaccurate or **incomplete** information **communicated** by procedures, or from a person to a person

Negligible		Minor		Moderate		Major		Extreme	
0	1	2	3	4	5	6	7	8	9	10

17.Little or no independent checking or **testing** of **output**

Negligible		Minor		Moderate		Major		Extreme	
0	1	2	3	4	5	6	7	8	9	10

18. A conflict between **immediate** and **long-term** objectives

Negligible		Minor		Moderate		Major		Extreme	
0	1	2	3	4	5	6	7	8	9	10

19. There is no enough **information** to allow **completeness** / accuracy checks

Negligible		Minor		Moderate		Major		Extreme	
0	1	2	3	4	5	6	7	8	9	10

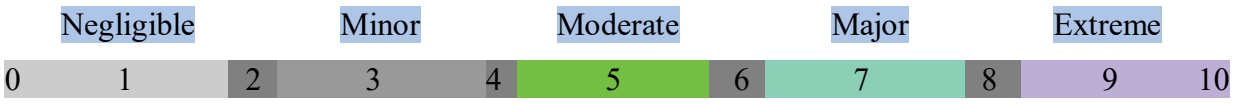
20. A **mismatch** between the **educational** achievement level of an individual and the **requirements**
of the task

Negligible		Minor		Moderate		Major		Extreme	
0	1	2	3	4	5	6	7	8	9	10

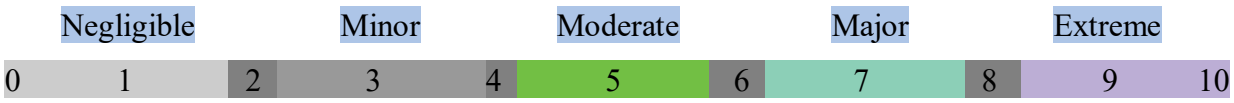
21.An stimulus to use other more **dangerous procedures**

Negligible		Minor		Moderate		Major		Extreme	
0	1	2	3	4	5	6	7	8	9	10

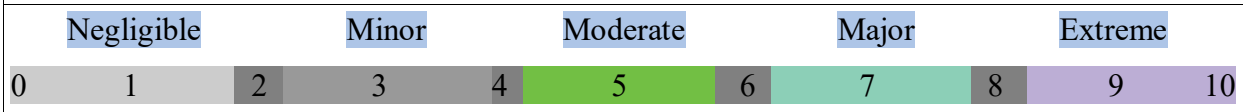
22. Little opportunity, such as rest **breaks**, to exercise mind and body outside the environment of the job



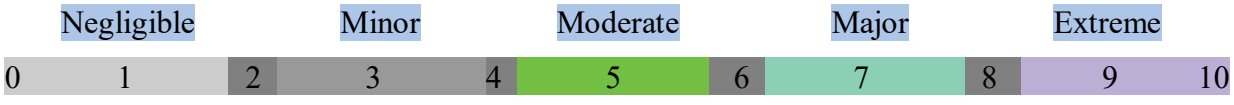
23. Unreliable **instrumentation** used to **communicate** information causing person performing the task ignoring information



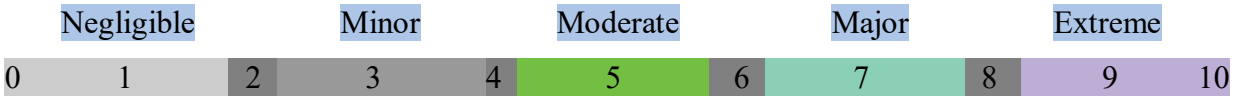
24. A need for **decision** making which is **beyond** the capabilities or experience of the **person** performing the task



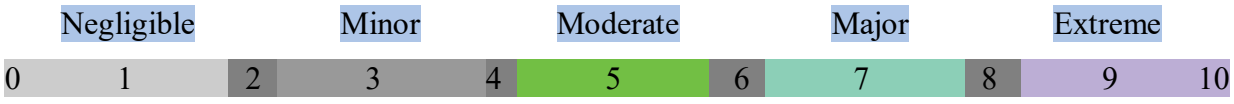
25. Unclear **allocation** of role and **responsibility**



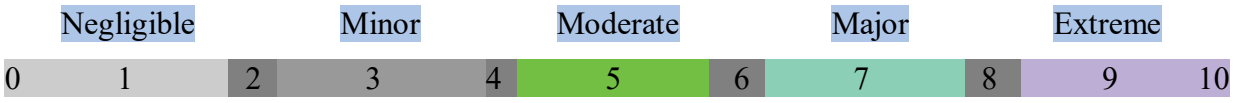
26. No obvious way to keep track of **progress** during an activity



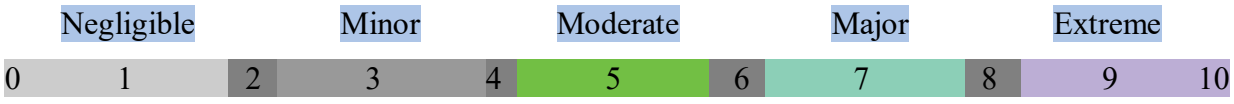
27. Task requirement **exceeds** the **physical capabilities** of the person performing the task



28.Person performing the task is **unaware** of its significance and their **contribution** to **corporate** objectives



29. High level emotional **stress**.



30. Evidence of **ill-health** among operatives especially fever.

Negligible		Minor		Moderate		Major		Extreme	
0	1	2	3	4	5	6	7	8	9	10

31. Low workforce **morale**.

Negligible		Minor		Moderate		Major		Extreme	
0	1	2	3	4	5	6	7	8	9	10

32. The **Information** displayed and how it is applied within procedures is **not** fully **understood**

Negligible		Minor		Moderate		Major		Extreme	
0	1	2	3	4	5	6	7	8	9	10

33. A poor or **hostile** environment (below 75% of health or life-threatening severity)

Negligible		Minor		Moderate		Major		Extreme	
0	1	2	3	4	5	6	7	8	9	10

34. **Prolonged** inactivity or highly **repetitious** low mental workload tasks

Negligible		Minor		Moderate		Major		Extreme	
0	1	2	3	4	5	6	7	8	9	10

35. **Disruption** of normal work-**sleep** cycles

Negligible		Minor		Moderate		Major		Extreme	
0	1	2	3	4	5	6	7	8	9	10

36. **Pressure** from someone else to increase the speed which a task is performed, beyond an individual's preferred **speed** and capability

Negligible		Minor		Moderate		Major		Extreme	
0	1	2	3	4	5	6	7	8	9	10

37. **Additional** team **members over** and above those **necessary** to perform task normally and satisfactorily

Negligible		Minor		Moderate		Major		Extreme	
0	1	2	3	4	5	6	7	8	9	10

38. **Age** of personnel performing perceptual tasks requiring the ability to interpret or become aware of something through the senses (**sight**, **hearing**, taste, smell or touch)

Negligible		Minor		Moderate		Major		Extreme	
0	1	2	3	4	5	6	7	8	9	10

Appendix 4: Letter of Request

የኢትዮጵያ ንግድ ባንክ
COMMERCIAL BANK OF ETHIOPIA
INTER DEPARTMENTAL MEMORANDUM

DATE ቀን	:	April 18, 2019
FROM ከ	:	Manager – Training Operation
SUBJET ጉዳዩ	:	Request for Cooperation to Conduct Research

To whom it may Concern

Addis Ababa University Department of School of Information Science /**BA**/under its letter reference No.SIS/19/2018/2011 dated December/24/2018 has requested our bank to assist **Mihret Seto,** Student to undertake Her Research on **"Human based Error aspect of Information Security "** the case of Commercial bank of Ethiopia.

Therefore, I would like to kindly request you to provide the required assistance and cooperation without compromising confidentiality.

Regards

Sablewengael Tilahun