ADDIS ABABA UNIVERSITY

COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES

SCHOOL OF INFORMATION SCIENCE

TOWARDS IMPROVING INFORMATION SYSTEMS VULNERABILITY ASSESSMENT PRACTICE IN AN ETHIOPIAN BANK

BY

ABEJE ABAY

JUNE 2021

ADDIS ABABA, ETHIOPIA

ADDIS ABABA UNIVERSITY

COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES

SCHOOL OF INFORMATION SCIENCE

TOWARDS IMPROVING INFORMATION SYSTEMS VULNERABILITY ASSESSMENT PRACTICE IN AN ETHIOPIAN BANK

A Thesis Submitted to School of Graduate Studies of Addis Ababa University in Partial Fulfillment of the Requirements for the Degree of Master of Science in Information Science and Systems (*Information Systems Specialization*)

By: ABEJE ABAY

Advisor: LEMMA LESSA (Ph.D.)

June 2021
Addis Ababa, Ethiopia

ADDIS ABABA UNIVERSITY

COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES

SCHOOL OF INFORMATION SCIENCE

TOWARDS IMPROVING INFORMATION SYSTEMS VULNERABILITY ASSESSMENT PRACTICE IN AN ETHIOPIAN BANK

By: Abeje Abay

Name and Signature of Members of the Examining Board

Lemma Lessa (Ph.D.)	_____	_____
Advisor	Signature	Date
Temtim Assefa (Ph.D.)	_____	_____
Examiner	Signature	Date
Getachew Hailemariam (Ph.D.)	_____	_____
Examiner	Signature	Date

Declaration

This thesis has not been accepted for any degree and it is not been being concurrently submitted in candidature for any degree in any university.

I declare that this thesis entitled "*Towards Improving Information Systems Vulnerability Assessment Practice in an Ethiopian Bank*" is a result of my own investigation, except where otherwise stated. I have undertaken the study independently with the guidance and support of my research advisor. Other sources are acknowledged by citations giving explicit references. A list of references is appended.

Signature_____

Abeje Abay

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

Advisor's signature: _____

Lemma Lessa (Ph.D.)

Acknowledgments

Next to God, I owe my foremost gratitude to my advisor Dr. Lemma Lessa. Dr. Lemma, I am highly surprised what you are doing to your students. Your commitment, pleasure, respectful, generosity, support, and understanding to your students is extraordinary. Your remainder emails and SMS texts were my alarms and this makes me to finish this thesis. As a whole, you are like as an advisor, father and mentor. God Bless You Dr. Lemma. Thank you very much.

Finally, I would like to thank all the individuals who have a role for the accomplishment of this research including my Families, friends, co-workers, and Bank ABC staffs for their support and cooperation.

Abeje Abay
June 2021
Addis Ababa, Ethiopia

Abstract

Now a day, information systems security is becoming a day-to-day concern for many organizations. Information security aims to protect the confidentiality, availability and integrity of information. One of the challenges faced by organizations is securing their information systems in light of the rising threats and compliance requirements. Vulnerability assessment is discovering the weaknesses and security holes of the information systems. Conducting vulnerability assessment stood out as one of the strategy to protect information systems from different cyber-attacks. It is one of the prerequisites as to what security control mechanisms to put in place. Extant literature indicated that a full-fledged security vulnerability assessment has not been a regular practice in banks in Ethiopia. This study intends to suggest strategies and recommendations for improving the information systems vulnerability assessment practice in a bank in Ethiopia. A qualitative case study research method is applied. Interview and document analysis were the data collection techniques. The respondents were purposively selected based on their role to vulnerability assessment practice and experience. This study used thematic analysis and the researcher transcribed interview recordings and used coding techniques. Initially the researcher read and re-read the transcripts from the recorded interview in order to filter out or identify the themes. And then review different initial codes to produce sub- themes. Next the sub themes were reviewed to define and name the themes. After the themes finalized the write up of the report has begun. The analysis has provided the following themes namely: - Creating baseline, vulnerability assessment, risk assessment, remediation, verification and Monitoring security and network traffics. The results of the analysis imply that bank does not have a defined vulnerability assessment procedure and policy. This indicates that the bank has many challenges on vulnerability assessment processes like baseline creation, vulnerability assessment, risk assessment, remediation, verification, and monitoring phases. The researcher highlights some recommendations and strategies for effective vulnerability assessment process.

Key words: *vulnerability, vulnerability assessment, Vulnerability assessment lifecycle*

Table of Contents

List of Tables

List of Figures

List of Acronyms

CEH	Certified Ethical Hacking
CNA	CVE Numbering Authority
CSOC	Cyber Security Operation Center
CIS	Center for Internet Security
CVE	Common Vulnerabilities and Exposure
DAST	Dynamic Application Security Testing
ICD	IBM Control Desk
IS	Information Systems
ISACA	Information Systems Audit and Control Association
IT	Information Technology
NBK	National Bank of Kenya
NIST	National Institute of Technology
NVD	National Vulnerability Database
SANS	SysAdmin, Audit, Network and Security
SIEM	System Information and Event Management
SS7	Signaling Systems no 7
TTPS	Tactics Techniques and Procedures
VA	Vulnerability Assessment

CHAPTER ONE

INTRODUCTION

This chapter sets the background for the research, presents the problem statement, research questions and the objectives of the research, the significance of the study and the scope of the research.

1.1 Background of the study

The banking industry has become highly competitive by undergoing a significant change in the way it conducts its businesses. Technology become continuously played an important role in the day-to-day performance of banks and the services provided by them. The application of information and communication technology concepts, techniques, and implementation strategies to banking services has become a subject of fundamental importance and concerns to all banks and indeed a prerequisite for local and global competitiveness (Akinlohu, 2007). Technical advancement in banks led to the introduction of new management methods and financial instruments, which have opened up new markets in the industry (Osiro, 2011). There has been intense competition, growing customer satisfaction and the need to improve profit to cover increasing cost and inflation factors which gradually bring a wide spread appreciation of the need for strategies. With our increasing dependence on information technology, the consequences of computer crime can be extremely series (Mahncke, et al, 2009). Information systems security is also a crucial issue for most organizations. The massive use of internet and its service brings, the number of attacks to information system is increasingly higher and, consequently the need to protect the information systems is becoming Imperious. Banks forced to acquire technologies to safeguard the bank from the increased risk and the technology used as a basis for competition, source of threats and a means for the countermeasure to threats.

The bank sector is a target for criminals and other malicious actors. With its high dependence on e-banking, mobile payments and agent banking, risk of cyber-attacks supported by identity thefts, hacking, social engineering attacks will continue. The attack strategies, sophisticated techniques and the opportunities for intruders have increased as banking sectors rely on the internet. The introduction of the internet believed to have resulted in the sudden vulnerability of banks to attacks not only from people inside the bank, but also from anywhere through the internet. For this vulnerability, banks use strong access controls, firewalls, and other controls as a means of strategy to protect their assets from attacks. Protecting systems requires multiple layers of security from the physical security of equipment, updating of operating systems and application software, to prevent intrusions on their network (Patricia, et al, 2010).

Business and government in any part of the globe have always been concerned with physical and information security. They have been protecting their physical assets with locks, guards, and they have guarded their networks and information assets by means of technology based security measures. The rise of the internet has completely changed the nature of information security because banks face global threats to their networks and sensitive data. To better prepare against attacks organizations should continually assess their overall cyber risk profile, remediate were recommended and proactively managing their defense.

Vulnerabilities will probably exist in large and complex software systems (Stefan, 2000). Vulnerability assessment is in need to determine banks vulnerabilities, what the likely damage would be in terms of confidentiality, integrity and availability of information. To perform vulnerability assessment, organizations need to first identify assets in order of priority, identify possible threats and vulnerabilities and develop security policies and strategies to be protected against threats (Osiro, 2011). Banks invest more for security devices without a strategy to deal with a problem and without continuous vulnerability assessment; it would be costly and ineffective. Banks are now choosing digital solutions to address their customers' needs and this in turn is exposing them to different attacks than ever before. Even if different security devices and preventive mechanisms put in place, the attackers can still break these security systems because every system has a vulnerable hole and attackers first consider discovering vulnerable holes or weaknesses of systems before try to exploit. Even if there is, firewall, IPS, and Antivirus attackers will try to steal a legitimate network access and bypass the firewall by hacking or stealing

credentials. Antivirus also studies incoming traffics and is not primarily focused on the system to see the weakness that a malicious code can exploit. This implies that banks should frequently perform vulnerability assessment to know the weaknesses and patch of their systems before attackers intrude on their system. It should be noted that vulnerability assessments alone don not prevent security incidents and does not necessarily improve security on its own (ISACA, 2017). Hence, a good vulnerability assessment process that provides banks a cost effective and reliable means for assessing vulnerabilities and protection from possible threats needs to be in place. Vulnerability assessment whether credential or non-credential is a key component of security strategy and recognized as a crucial part of information system security.

1.2 Statement of the problem

The researcher tried to review recent literatures to identify the research gap and fill the knowledge gap on improving information systems vulnerability assessment

According to risk based security research newly published in the 2020 midyear quick view data breach report, the first six months of 2020 have been more than 2037 publicly disclosed breaches exposing an incredible 27 billion compromised records, which exceeded the total number of exposed records during 2019 by more than 12 billion records. Perhaps even more remarkable is the fact that 3.2 billion of those records exposed by just eight breaches. “The majority of breaches reported this year has a moderate to low severity score,” this is important because many businesses wrongly assume they are too small to be on the radar of threat actors. The truth is that it is all about the data, and small businesses often have less well-guarded data stores.

Most organizations have realized that security breaches can have a negative influence on the business process continuity, public image, cause financial lose or create problems with legal authorities in case of noncompliance (Osiro, 2011). Effects of cyber security failure leads to the loss of intellectual property, direct financial loss from cybercrime, loss of sensitive business information, sabotage of operations, extra costs for system recovery and stakeholders lack of trust in systems (Tesfaye, 2018).

Banks are among the operators in the financial sector in Ethiopia and bank ABC is the one in financial ecosystem. Due to the nature of its business, bank ABC needs to have strong security systems in order to protect its information asset from highly increasing threats. Along with the continually increasing number of incidences and rapid number of vulnerabilities, the speed at which systems attacked also accelerated (Osiro, 2011). Securing information systems from current and future threats requires abroad and unbiased view of system vulnerabilities, as well as creative consideration of security and stability options in the face of resource constraints. Interoperability, information sharing, collaboration, design imperfections, limitations and the like lead to vulnerabilities that can endanger information systems security and operation (Philip, et al, 2003). These vulnerable holes can provide a backdoor for attackers to attack the victim.

Identifying vulnerabilities and addressing them in a timely manner is crucial in ensuring a secure environment and save money in the end (Osiro, 2011). Even if banks use different protective mechanisms to protect their information assets from attacks a threat may happen to take advantage of security vulnerabilities in a system and bring a negative impact on it.

Many thesis papers addressing vulnerability exist. From these Stefan (2009) has studied observations on operating system security vulnerability and identified that there are many weaknesses in different operating systems. King (2006) proposed a malicious insider composite vulnerability assessment methodology. Osiro (2011) also tried to assess information systems security vulnerability at national bank of Kenya (NBK), the researcher clarified that effective security measures are in place and the bank is using an automated vulnerability assessment tool to identify vulnerable holes and safeguard information systems.

Local researchers also tried to study the issue of information system security in bank sectors from different perspectives. Kelmie (2013), in his study proposed an information security management framework for banking industries in Ethiopia. Tesfaye (2018) proposed a cyber-security-auditing framework for banking industries in Ethiopia. Tewodros (2018) in his study identified challenges and practices of cyber security at selected infrastructure in Ethiopia and proposed a cyber-security framework. Mastewal (2020) also proposed information security risk assessment methodology for commercial bank of Ethiopia. Tsedale (2018) assessed information security incident management practice at bank X of Ethiopia, and the researcher proves that there is no separate information security incident management policy in the bank. Even if those researchers focus on information

security areas, no local researcher has addressed vulnerability assessment issues for financial sectors yet. Therefore, this study intends towards improving information systems vulnerability assessment practice at bank ABC and come up with suggestions for improvement.

1.3 Research Questions

- How bank ABC is performing information systems vulnerability assessment?
- What challenges exist in vulnerability assessment practices?

1.4 Objective of the study

The general objective of this study is to identify shortcomings in the vulnerability assessment practice of information systems at bank ABC and suggest strategies for improvement.

Specific objective

- Assess the information systems vulnerability assessment practice at bank ABC.
- Identify challenges and shortcomings of vulnerability assessment practice in the bank
- Recommend strategies of improvement based on best practices.

1.5 Significance of the study

The result of this study will serve as springboard to Ethiopian banks on how to secure their information systems by conducting a regular vulnerability assessment to their information assets and patch those vulnerabilities. Even the study can benefit organizations on how to conduct vulnerability assessment in line with international standard to know their vulnerabilities and recommend the best strategies for improvement based on international standards. Researchers may also benefit as they may study further by considering the gap especially on issues related to vulnerability assessment.

1.6 Scope of the study

The concept of vulnerability assessment can be conducted in financial or other organizations with different perspectives. However, this study focused on improving bank ABC's information systems vulnerability assessment. Physical vulnerability assessment is not taken in to consideration for this study. It also did not include penetration-testing practice though it is one measure of testing a computer system, network or applications to find the security vulnerabilities that an attacker could exploit.

1.7 Organization of the thesis

The research has composed of different chapters and contents.it includes

Chapter 1: this chapter introduces the background of the study, motivation of the researcher and information systems vulnerability assessment practice in financial sectors. Additionally it discusses about how banks are becoming vulnerable to attacks and mechanisms they are using to protect their assets from attacks. It also addresses the research gap on the subject area, which is not addressed by researchers yet with a general and specific objective. The significance and limitation of the study also stated.

Chapter 2: it contains literatures, which helps to explore the research topic about information security, common threats to information systems, banking, and financial services cyber threat landscape, vulnerability assessment, types of vulnerability assessment and related works discussed.

Chapter 3: describes the way enquiries of the study obtained. It consists of the research processes, research design, and source of the relevant data's, participant's selection mechanism, data collection methods and its analysis.

Chapter 4: it is the data presentation and discussion part of the study. It describes the respondent's information, challenges faced during data collection. It also clarifies the analysis of the collected data's presents based on their themes, and answers for the research questions of the study.

Chapter 5: this is the last chapter of the study and consists of summary of the findings, conclusion and recommendations for the improvement of information systems vulnerability assessment and future studies.

CHAPTER TWO

LITERATURE REVIEW

This chapter focuses on the most important concepts that clarify the issue of the research and it discusses about information security, most attack types, vulnerability assessment, vulnerability assessment types and lifecycle, vulnerability assessment tools and related works that has been done by researchers.

2.1 Security

Security is the quality or state of being secure to be free from danger (Michael, et al, 2012). In other words protection against adversaries, from those who would do harm intentionally or unintentionally. A successful organization should have the following multiple layers of security in place to protect its operations (Michael, et al, 2012).

- Physical security: - to protect physical terms, objects or areas to protect from unauthorized access and misuse.
- Personnel security: - top protect the individual or group of individuals who is authorized to access the organization and its operations.
- Operations security: - to protect the details of a particular operation or series of activities.
- Communications security:- to protect communication media, technology and content
- Network security: - to protect networking components, connections and contents.
- Information security: - to protect the confidentiality, integrity and availability of information assets whether in storage, processing or transmission. It can be achieve via the application of policy, education, training and awareness and technology.

2.2 Information Security

The definition of information security varies from scholars and/or institutes based on their different understanding perspective. Fredrik (2005) define information security as “protecting information from a wide range of threats in order to ensure business community, minimize business damage and maximize return on investments and business opportunities.” Annene and Annette (2007) define information security as “the application of any technical methods and managerial processes on the information resources (hardware, software and data) in order to keep organizational assets and personal privacy protected.” Whitman and Mattord (2009) define information security as “the protection of information and its critical elements including the systems and hardware that use, store and transmit that information”. Information security refers to the process and methodologies that are designed and implemented to protect print, electronic, or any other form of confidential, private and sensitive information or data from unauthorized access, use, misuse, disclosure, destruction, disruption and modification” (SANS Institute). As a result, many scholars define information security as protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

Whitman and Mattord (2009) also identify several critical characteristics of information that give it value in the organization. These characteristics or aspects of information security includes the confidentiality, integrity and availability of information (Alexander, et al, 2016).

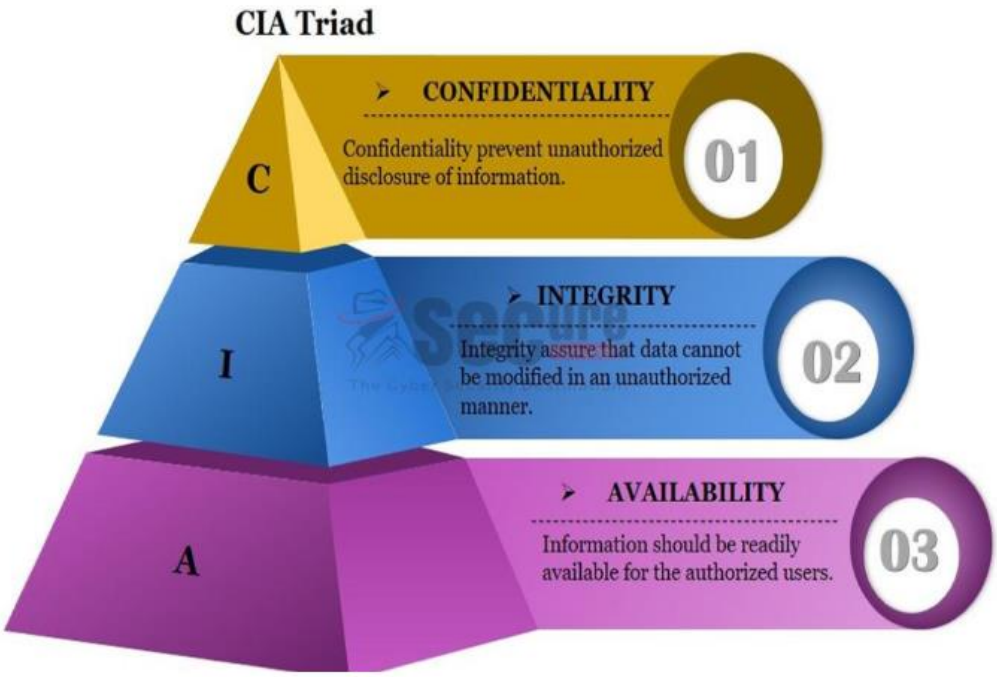


Figure 2-1 CIA Triad

Confidentiality (being safe from unauthorized access):- it refers to limiting information access and disclosure to authorized user and preventing access and disclosure from unauthorized ones.

Integrity (correctness and comprehensiveness of data):- integrity refers to the credibility of information resources. It involves maintaining the consistency, accuracy and trustworthiness of data over its entire life cycle. Data must not be changed in transit, and steps must be taken to ensure that unauthorized user cannot alter data.

The risk of violating the confidentiality of information is provided by the following factors (Alexander, et al, 2016).

- Degree of reasonableness of algorithms and reliability of system authentication of users who have the right to access the data stored in it.
- Possibility of having undocumented features in the software.
- Noncompliance with standards in the system design, production or operation phase
- Imperfection of the organizational structure of IS (information systems)
- Human factor

Availability (resources are always available to authorized user):- availability refers to the accessibility of the information resources. It ensures that information must be available to authorized user when the access.

Information security includes a number of essential terms and concepts, some of them will be discussed below (Michael, et al, 2012).

- Access: - a subject or objects ability to use, manipulate, modify or affect another subject or object. Authorized users have legal access to the system whereas hackers have illegal access to the system. Access controls regulate this ability.
- Asset: - the organizational resource that is being protected. An asset can be logical, such as website, information or data, or an asset can be physical, such as person, computer system or other tangible object. Assets and particularly information assets are the focus of security efforts, they are what those efforts are attempting to protect.
- Attack: - an intentional or unintentional act that can cause damage or compromise information systems. Attacks can be active or passive, intentional or unintentional, direct and indirect. Someone casually reading sensitive information, which is not intended for his /her use, is a passive attack. A hacker attempting to break in to an information system is an intentional attack. Lightning strike that causes a fire in a building is unintentional attack. A direct attack is a hacker-using personal computer to break in to the system. An indirect attack is a hacker compromising a system and using it to attack other system.

- Control, safeguard, and countermeasure: - security mechanisms, policies, or procedures that can successfully counter attacks, reduce risk, resolve vulnerabilities, and otherwise improve the security within an organization.
- Exploit: - a technique to compromise a system. Threat agents may attempt to exploit a system or other information asset by using it illegally for their personal gain. On the other hand, an exploit can be a documented process to take advantage of a vulnerability or exposure, usually in software, that is either inherent in the software or is created by the attacker. Exploits make use of existing software tools or custom-made software components.
- Exposure: - a condition or state of being exposed. In information security, exposure exists when a vulnerability known to an attacker is present.
- Loss: - a single instance of an information asset suffering damage or unintended or unauthorized modification or disclosure. When organizations information stolen, it has suffered a loss.
- Protection profile or security posture: - the entire set of controls and safeguards, including policy, education, training and awareness, and technology, that the organization implements (or fails to implement) to protect the asset.
- Risk: - the probability that something unwanted will happen. Organization must minimize risk to match their risk appetite the quantity and nature of risk the organization is willing to accept.
- Subjects and objects:- a computer can be either the subject of the attack an agent entity used to conduct an attack or the object of an attack the target entity.
- Threat: - a category of objects, persons, or other entities that represents a danger to an asset.
- Threat agent: - the specific instance or a component of a threat.
- Vulnerability: - a weakness or fault in a system or protection mechanism that opens it to attack or damage. Some well-known vulnerabilities have examined, documented, published and others remain latent (undiscovered).

2.3 Threats to Information Security

With the development of information and communication technologies and increasing accessibility to the internet, organizations become vulnerable to various types of threats, which

can cause different types of damages that might lead to significant financial loss (Michael et al, 2012). Information security damages can range from small losses to entire destruction of information system.

According to many scholars, information system threats classified in to three categories as natural, physical and human threats. Natural threats include natural disasters such as earthquake, hurricane, floods or any other nature created disasters that cannot be stopped. Information damage or lost due to natural threats cannot be easily prevented as no one knows in advance that these type of threats will occur. Physical threats may include loss or damage of the system resource through fire, theft, water and physical impact. Human threats include threats of attacks performed by both insiders and outsiders. Insider attacks refer to attacks performed by disgruntled or malicious employees. Outsider attacks refers to attacks performed by malicious individuals or group outside of the organization. Insider attacks can be the biggest threat to information systems, as they may know the security posture of the information system, while outsider attacks apply many tricks to learn the security posture of the information system (Abeselom, 2013). Attackers have matured from using hacking skills to show that they can circumvent the authentication process to access each other's file to use them in the theft of confidential information (Dlamini, et al, 2009).

2.4 Banking and Financial Services Cyber Threat Landscape Report

The financial services sector faces a constant stream of cyberattacks levied by threat sectors seeking to infiltrate corporate defense networks. IntSights provides a comprehensive overview of the current cyber threat landscape in the financial services and banking sector based on key threat data collected in the IntSights enterprise threat intelligent and mitigation platform. Threat researchers analyzed the most significant action in attack types, attack vectors, and regional trends facing these organizations, and offer commentary on best practices to defend against the latest trends and attack vectors.

Banks and financial service organizations targeted in 25.7% of all malware attacks in 2019, it is more than other 27 industries tracked and there is 212% increase in instances of compromised credit cards (IntSights, 2019). Credential leaks increase in 129% and 102% increase in malicious applications including fraudulent mobile banking apps has reported. Financial organizations based in developing countries namely Latin America, south Asia and Africa were attacked more

frequently because many lack the external facing security systems that are common in more developed regions of the world (IntSights, 2019).

2.5 Most Common Attack Types

Cyber criminals have a constantly expanding collection of TTPS used to exploit banking and financial service organizations (IntSights, 2019). Hacking tools enable faster campaigns, social media and mobile devices give threat actors new ways to target customers and data leaks from thousands of external sources are costing banks billions of dollars each year in fraud costs. New attack vectors emerge constantly, leaving organizations scrambling to cover any newfound weaknesses or attack strategies.

The following are some of the most types of attacks leveraged against financial institutions over the past years (IntSights, 2019).

2.4.1.1. Vulnerabilities in SS7

In February 2019, United Kingdom based metro bank become the first publicly reported victim of a new attack vector. The codes sent through text messages to customers to verify transactions. Cybercriminals were able to exploit flaws in SS7- a protocol used by telecommunication companies to coordinate how they route SMS around the world- to interpret messages that authorize payments from accounts. This scheme enabled the attackers to empty some of the customer's bank account.

2.4.2.2. Malware

As 5G network is rolling out, the use of IOT devices will accelerate dramatically and this will increase network vulnerability to large scale, multi sector cyber-attacks (Cyber security risk report, 2020). IOT devices and their connections to networks and clouds are a weak link in security. It is

hard to get visibility of these devices that can have complex security requirements. The more IOT devices the more risk.

Banks and financial service organizations were the main targets of malware attacks in the last years than any other industry. Trojan viruses are among the more common types of malware attacks. Some of the most known banking Trojans in 2018 were Adload, ATRPAS, and Emotet. Adload is a tool that opens backdoor on the targeted system, where it downloads and installs programs to gather usernames and computer name information to send to the attacker's server. ATRPAS is a Trojan targeting window that steals information from infected computers and sends to the attacker's server. Emotet is a modular banking Trojan that is primarily used as a downloader or dropper of other banking Trojans.

2.4.1.3. Ransomware

In recent years, sophisticated ransomware were reported across the world. Specific industries were highly victimized, including local and state government and health care institutions. The new stark reality is that attackers are spending more time to gather intelligence on the target systems, achieving maximum disruption and scale up ransoms (Cyber security risk report, 2020). Cyber criminals use ransomware to hold banks hostage until they pay. Attackers are in essence executing a denial of service that can host banks millions of dollars each day as the attack continues. A bank cannot function under ransomware attack, since most of its key data is encrypted. Businesses may need to evaluate their options in order to protect their stakeholders, customers, employees, and information assets from attacks.

2.4.1.4. ATM Attacks

ATM malware: since the start of 2018, more than 20 type of ATM malware families have hit banks around the globe. FASTCash and ATMJackpot are two of the malware applications that caused the greatest damage in 2018 through 2020. The notorious hacking group Lazarus has used FASTCash in dozens of ATM hacks. The attackers inject a malicious executable file in to the switch application server of the ATM network. FASTCash allows attackers to transmit fake messages that approve fraudulent withdrawal requests.

ATM Card Skimmers: organized cybercriminal group installs payment card skimmers on ATM machines around the world, with new stories emerging daily about perpetrators being arrested. For this technique, attackers put a small device on the ATM's card swipe mechanism. When customers swipe their cards through the skimmer, the device captures the card information, including the card number, expiration date, and full name. These attackers also put an undetectable camera on the ATM to record the pin number of the customer's card. The groups that installs the skimmers later use the information stolen to make fraudulent charges.

2.6 Information Security Measurement

Security measurement matters to every stakeholder in network security and involves all the stages and aspects of the entire lifecycle. There would be no effective security awareness and actions without accurate security measurement. The existing security measurements mainly focus on the relationships between exploits and system vulnerabilities, their security measurements of unknown threats like zero day loophole are very limited (Lihua, et al, 2018). An increasing number of hackers, motivated by their persistent love for technology or tempted by profits are attempting to discover and propagate zero day exploits.

2.7 Vulnerability, Threat and Risk

In order to have a strong handle on data security issues that may potentially affect your organization, it is imperative to understand the relationship of three components, threat vulnerability and risk (Stephen, 2020).

Figure 2-2 Threat, Vulnerability and Risk (Stephen, 2020)

2.7.1 Vulnerability

vulnerability is, "the quality or state of being exposed to the possibility of being attacked or harmed, either physically or emotionally." This is a very broad term. Yet, somehow, in InfoSec, we've come to narrowly associate a vulnerability with unpatched software and misconfigurations (Rich, 2020).

Vulnerability is the level of exposure to being harmed or attacked. Vulnerabilities will probably exist in large and complex software systems, at least with today's software methods, techniques and tools. It seems to be impossible to eliminate all flaws (Stephen, 2000). Vulnerability defined as any flaw or hole in a system that presents the opportunity for malicious exploitation, there by posing a threat against network resources and information (SANS, 2000-2002). Vulnerability is a flaw or weakness in a system security procedure, design, implementation or internal controls that could be performed (accidentally triggered or intentionally exploited) and result in a security

breach or a violation of the systems security policy (William, 2006). Vulnerabilities are easily detectable by hacker for breaches and attacks, this will led to the entry of hacker to the system which may lead to breaches in security such as confidentiality, integrity, availability, nonrepudiation, authentication, authorization and access control (Sushilkumar, 2014). The USA national institute of standards and technology (NIST) defines vulnerability as a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source". Thus, a vulnerability is a weakness that can be exploited by adversaries to advance their goals (ISACA, 2017). It is impossible to remove every technical vulnerability from a given environment and there are a number of reasons for this. Some vulnerabilities are latent until they discovered and publicly disclosed called zero days. Other vulnerabilities might persist due to challenges associated with patching certain devices. The vulnerability in a system or network may be due to design flaws, poor security management, incorrect implementation, internet technology vulnerability, the nature of intruder activity, the difficulty of fixing the vulnerable systems, the limits of effectiveness of reactive solutions, and social engineering (Satish, 2016). The cause of vulnerabilities are misconfigurations, policy violations, and system flaws. Majority of design flaws are due to software design and there are reasons behind it. Human factors, software complexity, and trustworthy software sources. The human factor includes forget to add or remove or verify some code, finish product in urgency, overconfidence, malic behavior of developer and overlook certain tests (Satish, 2016).

There are many causes for security vulnerabilities. Among those some are listed below (Rich, 2020).

- **Unpatched Software –** Unpatched vulnerabilities allow attackers to run a malicious code by leveraging a known security bug that has not been patched. The adversary will try to probe your environment looking for unpatched systems, and then attack them directly or indirectly. –
- **Misconfiguration –** System misconfigurations (e.g. assets running unnecessary services, or with vulnerable settings such as unchanged defaults) can be exploited by attackers to breach your network. The adversary will try to probe your environment looking for systems that can be compromised due to some misconfiguration, and then attack them directly or indirectly.

- **Weak Credentials** – An attacker may use dictionary or brute force attacks to attempt to guess weak passwords, which can then be used to gain access to systems in your network.
- **Phishing, Web & Ransomware** – Phishing is used by attackers to get users to inadvertently execute some malicious code, and thereby compromise a system, account or session. The adversary will send your users a link or malicious attachment over email (or other messaging system), often alongside some text/image that entices them to click.
- **Trust Relationship** – Attackers can exploit trust configurations that have been set up to permit or simplify access between systems (e.g. mounted drives, remote services) to propagate across your network. The adversary, after gaining access to a system, can then proceed to breach other systems that implicitly trust the originally compromised system.
- **Compromised Credentials** – An attacker can use compromised credentials to gain unauthorized access to a system in your network. The adversary will try to somehow intercept and extract passwords from unencrypted or incorrectly encrypted communication between your systems, or from unsecured handling by software or users. The adversary may also exploit reuse of passwords across different systems.
- **Malicious Insider** – An employee or a vendor who might have access to your critical systems can decide to exploit their access to steal or destroy information or impair them. This is particularly important for privileged users and critical systems.
- **Missing/Poor Encryption** – With attacks on Missing/Poor Encryption, an attacker can intercept communication between systems in your network and steal information. The attacker can intercept unencrypted or poorly encrypted information and can then extract critical information, impersonate either side and possibly inject false information into the communication between systems.
- **Zero-days & Unknown Methods** – Zero days are specific software vulnerabilities known to the adversary but for which no fix is available, often because the bug has not been reported to the vendor of the vulnerable system. The adversary will try to probe your environment looking for systems that can be compromised by the zero-day exploit they have, and then attack them directly or indirectly.

2.7.2 Threat

A threat refers to a new or newly discovered incident that has the potential to harm a system or overall of your company (Stephen, 2020). Worms and viruses are categorized as threats because they could cause harm to your organization through exposure to an automated attack, as opposed to one penetrated by humans. Most recently, on May 12, 2017, the Wannacry ransomware attack began bombarding computers and networks across the globe, and since been described as the biggest attack of its kind (Stephen, 2020).

2.7.3 Risk

Risk is the potential loss or damage when a threat exploits a vulnerability like, financial loss, loss of privacy, damage to your reputation, legal implications, even loss of life (Stephen, 2020). Information security risk comprise the impacts to an organization and its stakeholders that could occur due to the threats and vulnerabilities associated with the operation and use of information systems and the environments in which those systems operate (Stephen, et al, 2013). Information security risks should be mitigated through implementation and continuous monitoring of preventive and detective information security controls to safeguard the infrastructures from unauthorized access or loss.

2.8 The National Vulnerability Database

The NIST vulnerability database (NVD), launched in 2005, and it is the largest collection of technical vulnerabilities in the world 93,361 in 2017. The NVD is a superset of the common vulnerabilities and exposure (CVE) vulnerability list, established in 1999 and maintained by MITRE with input from dozens of organizations worldwide, the NVD adds analysis, a database and searching capabilities. The CVE provides a taxonomy to describe vulnerabilities and enable information security tools to refer to vulnerabilities through standard identifiers that named as CVE IDs. CVE numbering authorities (CNAs), the organization that assigns CVE IDs, interact with the CVE dictionary directly, however most information security practitioners work with

CVEs through reference to the NVD, results presented in vulnerability scanners and other information security tools or advisories.

2.9 Vulnerability Assessment

A vulnerability assessment is the process of identifying and analyzing those security vulnerabilities that might exist in the information systems. Vulnerability assessment can be defined as an examination, discovery and identification of system and applications security measures and weaknesses (IpSpecialist, 2018). Systems and applications examined for security measures to identify the effectiveness of deployed security layer to withstand attacks and misuses (ISACA, 2017). Vulnerability assessment also helps to recognize vulnerabilities that could be exploited, need of additional security layers and information that can be revealed by scanners. ISACA declared that vulnerability assessments are typically conducted through network or host based methods by using credential or non-credential scanning type to discover, test, analyze and report systems vulnerabilities. It should be noted that vulnerability assessments alone do not prevent incidents (ISACA, 2017). Conducting an assessment does not necessarily improve security in its own; instead, it reflects the snapshot of the environment at a particular point of time, and its goal is simply to identify and analyze weaknesses present in a technical environment. To set a net benefit to security, the enterprise must regularly conduct vulnerability assessment (to track net improvement or failure to improve) and act on the results of those assessments.

Vulnerability scanning is the art of using one computer to look for weaknesses in the security of another computer. So that you can find and fix the weaknesses in your systems before someone else finds that there, is a security weakness and decides to break in. It is a bit like a shop keeper making sure all the doors and windows are closed and locked, the money is in the safe and the alarm is set, before closing up for the evening (Ken Houghton, 2003).

Vulnerability assessments are not exploitative by nature compared to ethical hacking or penetration tests. In conducting a vulnerability assessment, practitioners or the tools they employ will not typically exploit vulnerabilities they find. Instead, vulnerability assessment serves an altogether different purpose. It allows an enterprise to focus on reconnaissance and discover weaknesses in its environment.

NIST special publication 800-115, “technical guide to information security testing and assessment” is a practical guide to techniques for information security testing and assessment. The standard discusses the following four vulnerability assessment activities based on asset groups.

2.9.1 Network Based Scans

Network based scans combine host and service discovery with vulnerability enumeration. The discovery component of network-based scan allows the assessor to identify the devices on a network and for each device, determine its type and potential points of attack. To learn the type, the scanning tool probes a target and analyzes its behavior and responses to a fingerprint that includes information about the system and allows the tool to determine the characteristics of the host. Because hackers are almost certain to scan internet connected systems new servers typically scanned within minutes of coming online. Hackers who gain a foothold on an internal network can “land and expand” by using compromised host to identify more vulnerable targets, to move literally throughout the network, and to attack other systems using the compromised host as a beachhead. To the extent that scanning can help reduce this possibility, internal scans can help prevent attacks from spreading quickly inside an enterprise.

2.9.2 Host Based Scans

Network based scans may sometimes miss weaknesses that can be exploited only by a user who is logged onto the system because they may only have the capability or be configured only to look for remotely exploitable vulnerabilities. Host based scans, by contrast are executed from the target computer or remotely controlled with authenticated account access to the target computer. These scans provide greater visibility in to systems configuration settings and patch details, while covering ports and services that are also visible to network based scans, however that breadth typically increases their overhead and makes them harder to setup and operate.

2.9.3 Wireless Network scans

Wireless scans of an enterprise’s WI-FI networks focus on points of attack in wireless network infrastructure. One aspect of wireless network testing is validating that an enterprises networks are securely configured. Although any benefit of disabling SSID broadcast to hide a network has long since passed, scanning validates that strong encryption is enabled and default settings are changed.

Another purpose of wireless testing is to identify rogue access points, which pose as legitimate wireless networks of either an enterprise or a hotspot, such as a local coffee shop, to trick victims in to joining an attacker's network.

Network based scans should also be used on wireless networks to detect vulnerable systems. Enterprises should be aware that internal systems might connected to guest wireless networks, an attacker can target systems connected to a guest network and jump to internal networks from there. Guest networks may be isolated, but compromised systems connected to these networks really are isolated, network infrastructures may inadvertently allow guest network traffic inside internal networks and access to sensitive networks and systems.

2.9.4 Application Based Scans

Application scans typically focus on websites to discover and enumerate software vulnerabilities and misconfigurations. Software Centric Dynamic Application Security Testing (DAST) tools help to identify vulnerabilities that are unique to web software, such as SQL injection, cross-site scripting (XSS), insufficient input validation and sensitive data exposure. Many network vulnerability-scanning tools also include web application security testing, although they have fewer features that focus on web application testing than DAST tools. Application security testing can be risky because scanning software may make changes to the databases and delete content during testing, so enterprises should restrict testing to nonproduction environments or exercise caution in scanning production environments.

2.10 Types of Vulnerability Assessment

- Active Assessment: - it is a process of vulnerability assessment, which includes actively sending requests to the live network and examining the responses. In short, it is the process of assessment, which requires probing the target host.
- Passive Assessment: - it is the process of assessment, which usually includes packet sniffing to discover vulnerabilities, running services, open ports and other information. However, it is the process of assessment without interfering the target host.
- External Assessment: - it is a process of hacker's perspective to find out vulnerabilities and to exploit them from the outside.

- Internal Assessment: - it is discovering vulnerabilities by scanning internal network and infrastructure from the inside.

2.11 Vulnerability Assessment Life Cycle

Vulnerability assessment phase refers to identifying vulnerabilities in the organizations infrastructure including operating systems, web services etc. it helps to identify the category and criticality of the vulnerability in an organization and minimizes the level of risk. The ultimate goal of vulnerability scanning includes scanning, examining, evaluating, and reporting the discovered vulnerabilities in the organization information systems. In order to choose a good vulnerability assessment life cycle two different samples developed by (SANS and EC-Council) has been discussed.

Vulnerability assessment life cycle includes the following five phases (SANS, 2013).

1. Preparation

To prevent being stunned by thousands of vulnerabilities identified in the first scan, it is recommended to start with a small scope. This can be achieved by starting out with a small number of systems or by limiting the number of vulnerabilities obtained by vulnerability scanner. It is important to have an agreement on which systems will be included or excluded from the vulnerability assessment. Besides the scope of systems, the organization should determine the type of scans. Informing IT, specifically teams managing firewalls, IDS, or other security monitoring systems should be part of vulnerability assessment process.

2. Vulnerability scan

Once the preparation phase is complete, vulnerability-scanning phase begins. Most vulnerability scanning tools offer a wide range of reporting options to visualize scan results. It is necessary to use them to create a various number of reports, which has technical information about detected vulnerabilities as well as recommendations for mitigation and improvement.

3. Define Remediating Actions

The asset owners with the cooperation of security officers will define remediating actions. IT departments will analyze the vulnerabilities from a technical perspective and answer questions such as if patches are available or whether the configuration should be tough? The recommendation also should include feasibility of the remediating actions such as whether installing a certain patch will result in the application not supported by the vendor. In short, term remediation is not possible, compensating controls should be identified in order to mitigate/remove the risk without correcting the vulnerability. In case asset owners decide to accept the risk, it should be documented trough a risk acceptance process. Usually high risks can only be accepted by the organization whereas asset owners can accept small risks.

4. Implement Remediating Actions

The planned remediating actions should be executed in line with the agreed period. If a problem occurs with implemented remediation, it should be recorded. The asset owners based on the recommendations from IT department and security officer should define alternative actions. These new or other remediating actions should be implemented. The security officer should track the status of the remediation action.

5. Rescan

Once the vulnerability is remediated, a rescan has to be scheduled to verify the remediation actions have been implemented properly. This scan should be performed with the same vulnerability-scanning tool and identical configuration settings as initial scan. This phase is very essential to prevent inaccurate results due to configuration results.

EC-Council in 2018 has grouped vulnerability assessment life cycle in to the following six phases.

1. Creating Baseline

Creating baseline is a pre assessment phase of the vulnerability assessment life cycle in which pentester who is performing vulnerability assessment identifies the nature of corporate network, applications and services. He/she creates an inventory of all resources and assets, which help to manage, prioritize the assessment. Furthermore he/she also maps the infrastructure, learns about the security controls, policies and standards followed by the organization. In the end baseline helps to plan the process effectively, schedule the task, and manage them with respect to priority.

2. Vulnerability Assessment

It focuses on assessment of the target. The assessment process includes examination and inspection of security measures such as physical security as well as security policies and controls. In this phase, the target is evaluated for misconfigurations, default configurations, faults and other vulnerabilities by either probing each component individually or using assessment tools. Once the scanning is complete, findings ranked in terms of their priorities. At the end of this phase, vulnerability assessment report shows all detected vulnerabilities, their scope and priorities.

3. Risk Assessment

Risk assessment phase includes scoping these identified vulnerabilities and their impact on corporate network or on an organization. The tasks in this phase includes perform risk characterization, assess the level of risk impact, and determining the threat and risk level.

4. Remediation

Remediation phase includes remedial actions for these detected vulnerabilities. High priority vulnerabilities should address first because they can cause a huge impact. It refers to the steps that should be taken to mitigate vulnerabilities, locating risks, and designing response for the vulnerabilities. It is important for the remediation process to be specific, measurable, attainable, and relevant and time bound. The tasks performed in the remediation phase include-

- ✓ Prioritize recommendations
- ✓ Develop an action plan to implement the action plan
- ✓ Perform root cause analysis
- ✓ Apply fixes/patches
- ✓ Capture lessons learned
- ✓ Conduct awareness training

5. Verification

Verification phase ensures that all vulnerabilities in an environment are eliminate and it helps the security analyst to verify whether all the previous phases are perfectly deployed or not. The tasks in the verification phase includes performing dynamic analysis and attack surface area.

6. Monitor

Monitoring phase includes monitoring the network traffic and system behaviors for any further intrusion. It includes implementing continuous security monitoring, policies, procedures and controls to prevent ever-evolving threats.

Figure 2-4 Vulnerability assessment life cycle (EC-Council)

Many organizations have used these two different vulnerability assessment life cycles, but a life cycle provided by EC-council is more preferable due to its detail clarification on every phase and monitoring is included as essential, which is not listed under SANS life cycle. This phase includes monitoring the network traffic and system behaviors for any further intrusion. It also includes implementing continuous security monitoring policies, procedures and controls to prevent ever-

evolving threats. EC-council's life cycle includes all the phases under SANS life cycle with brief contents and explanations, which is essential for successful vulnerability assessment process. Due to this, a life cycle provided by EC-council is used as a basis for this study.

2.12 Vulnerability Assessment Tools

Vulnerability assessment tools used to test hosts or applications for vulnerabilities. Several vulnerability assessment tools available include port scanners, vulnerability assessment scanners and OS vulnerability assessment scanners. Typically, vulnerability scanning tools search network segment for IP enabled devices and enumerate systems, operating systems and applications. Vulnerability scanning software scans the computer against the common vulnerability exposure (CVE) index and security bulletins provided by the software vendor.

In this era of modern technology and advancement, finding vulnerabilities in an existing environment is becoming easy using different tools. Various tools are available to help in finding weaknesses, problems and holes in an operating system, network, software and application. These scanning tools perform deep inspection of scripts, open ports, banners, running services and configuration errors.

2.13 Related works

Researches regarding to information security and vulnerability assessment in different organizations has been done a broad.

Author $ Title	Objective	Methodology	Finding	Gap
Stephan (2000) Observations on operating system security vulnerabilities	To investigate intrusions in operating systems in order to find and model the underlying weaknesses.	Collects data on 3 different operating systems UNIX, Novell NetWare, and windows NT. Data generated from practical	Operating systems have a number of vulnerabilities Provides a powerful basis for improving security of	The researcher only focuses on operating systems vulnerabilities

		experiments and security analysis	operating systems	
Osiro (2011) a vulnerability assessment of information system security at the National Bank of Kenya (NBK)	To assess vulnerability of the information security systems	Uses questionnaire to collect data and analyzed with statistical tool Uses census	Effective security measures are in place to safeguard information systems	The study seems like more focused to physical security vulnerability assessment.
William (2006) Development of malicious insider vulnerability process	Provide methodology to determine an organizations malicious insider vulnerability level	Attack tree method Content analysis Multidimensional approach	Improve an existing insider Threat taxonomy model and develop a composite vulnerability assessment process	Focuses only to malicious insider threats, the researcher doesn't consider misconfiguration, weak accounts, operating system, application etc.
Charles D. Lybrand (2013) The use of vulnerability assessment: A survey	Investigate vulnerability assessment and the security of data in a small organization	Collect survey from five third party vulnerability assessment organizations.	Develop methodology Show the common weaknesses faced by small organizations and make recommendations on common countermeasures	

Table 2-1 Related works

Table 1 illustrated that researchers have conducted a study on vulnerability assessment from different perspective in different organizations and they identified gaps and recommendations for future work.

Stefan (2000) has studied an intrusion investigation on operating system security vulnerabilities. The researcher has conducted his study on three different operating systems UNIX, Novell Netware, and Windows NT. he uses the data for UNIX and Novell Netware that was generated from a number of practical intrusion experiments that was done by Masters Students while Windows NT data resulted from a security analysis performed by the researcher. Based on the analysis, the researcher clarified that Windows NT has a number of vulnerabilities and a comparison with earlier UNIX analysis indicates that the security differences between the systems are related more to the factors such as time on market and security by obscurity than to inherent security performance. In addition, the investigation result of Novell Netware systems shows that, even if some efforts have been made to improve the security, no significance difference has achieved, due to compatibility requirements. The researcher describes towards a full understanding of the generic weaknesses and vulnerabilities that impair commercially available operating systems, but the researcher does not cover issues about application and network vulnerabilities.

Osiro (2011) has studied an assessment on vulnerability of information systems security. The researcher conducted his study at National Bank of Kenya (NBK) aimed on establishing security systems as well as assessing how vulnerable these systems are to threats from either internal or external. The researcher collected data from NBK ICT division and 10 branches in Nairobi using questionnaire and analyzed with statistical tool. He also used census to ensure that the collected data is not biased. The researcher puts on findings that effective security measures are in place to safeguard information systems at NBK, smart cards are widely used to gain access to almost all sensitive areas and properly installed CCTV cameras are in place to offer all around surveillance with in the bank. Automatic vulnerability assessment tool mostly used by the bank, which enables for effective detection of systems, capable of updating automatically for new threats and scanning periodically based on predefined schedule. From the findings, the study seems like more focused to physical security vulnerability assessment.

Charles (2013) conduct a study to investigate the vulnerability assessment and security of data in small organizations. The researcher collected the survey from five third party vulnerability assessment organizations; make the analysis to verify the weaknesses of small organizations and the safeguards that vulnerability assessment can provide. Based on findings the researcher recommends on countermeasures to protect the data of the organization.

Even though some studies have been conducted on information systems vulnerability assessment, it will not be the same for all organizations. Hence, it is vital to study information systems vulnerability assessment from diverse perspective in different organizations. As per the knowledge of the researcher, local researchers do not study information systems vulnerability assessment either in financial sectors like banks or non-financial organizations. This research is intended towards improving information systems vulnerability assessment practice and suggest strategies for improvements in Bank ABC.

2.14 Chapter summary

This chapter discussed the detail concept of information systems, vulnerability assessment, and the research related literatures. Many scholars are paying attention for vulnerability assessment issues. On top of that, this chapter discussed about internationally accepted vulnerability assessment life cycle, which was provided by EC-Council, as experts develop it. Due to this, this research relies based on this life cycle.

CHAPTER THREE

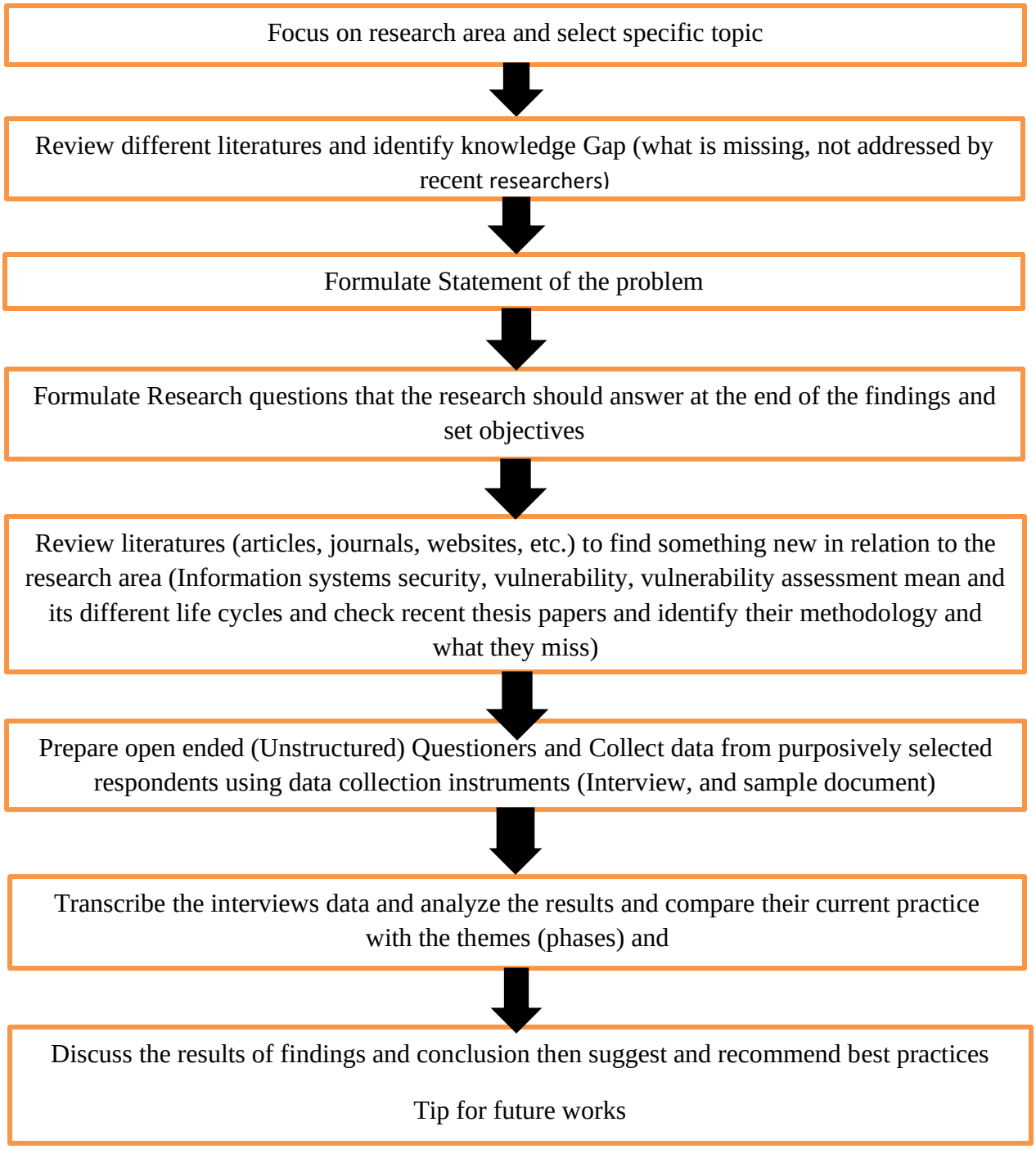
RESEARCH DESIGN AND METHODOLOGY

This chapter describes the way enquiries of the study obtained. It consists of the research processes, research design and method, and source of the relevant data's, participant's selection mechanism, data collection methods and its analysis.

3.1 Research design

Research designs are plans and procedures for research that span the decisions from broad assumptions to detailed methods of data collection and analysis (Creswell, 2009). It provides the framework that specifies the type of information to be collected, its sources and collection procedures. Research design is the blueprint of the research process used to complete the study, as it ensures that the study is relevant to the problem and will use economical procedure (Churchill, 2005). The selection of the research design is based on the nature of the research problem or issue being addressed, the researcher's personal experience, and the participants for the study. Hence, this research is qualitative which intends for improving information systems vulnerability assessment in bank ABC.

The research design for this research in diagram



3.1.1 Qualitative Research

Qualitative research is a means for exploring and understanding the meaning individuals or groups describe to a social or human problem (Creswell, 2009). The process of research involves emerging questions and procedures, data typically collected in the participants setting data analysis inductively building from particulars to general themes and the researcher making interpretations of the meaning of data. When compared to quantitative research, a researcher is the main actor for data collection and analysis than in qualitative research. Qualitative research adopts the inductive approach and its effectiveness depends on the skills and knowledge of the researcher because the outcomes mostly come from the researcher's judgment and interpretation. This research conducted to understand the current practice of information systems vulnerability assessment in bank ABC with a small and purposely selected respondent. The data collected with open ended response from the interviewees and observation of sample documents in order to identify the relevant themes. The role of the researcher plays a vital role to transcribe the collected data and finalize the report without changing and bias of the respondent's idea. This process inflicts that the research has a qualitative research characteristic.

3.1.2 Case Study

Case study method enables the researcher to closely examine the data with in a specific content. In most cases case study selects a small geographical area or a very limited number of individuals as the subject of the study. Case studies in their true essence explore and investigate contemporary real time phenomenon through detailed contextual analysis of a limited number of events and their relationships (Zaidah, 2007). Yin (1984) defines the case study research method "as an empirical enquiry that investigates a contemporary phenomenon within it real life context when the boundaries between phenomenon and context are not clearly evident, and in which multiple sources of evidence are used."

3.1.3. Analytic Frame CE-council

EC-council describes vulnerability assessment life cycle with six phases. The first phase is creating baseline, which includes activities such as identifying and prioritize critical assets to create a good

baseline for the vulnerability assessment process. Vulnerability assessment phase is the first operational phase, which enables to identify vulnerabilities and weaknesses in an organizations information systems or infrastructures with the help of scanning tool. In the risk assessment, phase all serious uncertainties those are associated with the system are assessed, fixed, and permanently eliminated to have a flaw free system. It summarizes the vulnerabilities risk level of selected assets. Reducing the severity of vulnerabilities after the successful implementation of baseline and assessment steps incorporated in remediation phase. Verification phase provides a clear visibility in to the firm and allows the security team to check whether all previous phases are perfectly employed or not. The last phase is monitoring phase, which is implementing continuous security monitoring, policies, procedures and controls to prevent ever-evolving threats. SANS, NIST, ISACA and many other technology institutions provide standards for vulnerability assessment, which can be used as a base by organizations to improve their assessment strategy. Hence, EC-Council life cycle is used as a basis for this research to explore the current information systems vulnerability assessment trend at bank ABC and looking forward for improvements.

3.2 Research Approach

Research approaches are plans and procedures for research that span the steps from broad assumptions to detailed methods of data collection, analysis, and interpretation (Creswell, 2009). Inductive approach was followed for this study. Inductive approach enables researchers to build their patterns, categories, and themes from the bottom up by organizing the data in to increasingly more abstract units of information. This inductive process illustrates working back and forth between the themes and the database until the researcher have established a comprehensive set of themes. It may also involve collaboration with participants interactively, so the participants have a chance to shape the themes or abstractions that emerge from the process. Even if this approach has weaknesses on some aspects but it is appropriate for small number of samples.

3.3 Data Collection Methods

Data collection is the process of gathering and measuring information on variables of interest, in an established systematic fashion that enables one to answer the stated research questions, test

hypothesis, and evaluate outcomes (Syed, 2016). Qualitative research uses different data sources and techniques. For the purpose of this research, face-to-face semi structured interview and document analysis were the main sources of data gathering methods. Interview questions were open ended and it enables the respondents to provide a detail explanation and information about the topic. Collection of interview data involved interaction between researcher and the respondents, which needs to be documented. For the purpose of this study, the interviews were tape-recorded and I took short notes at the same time. After the interview, I reviewed the tape and notes and wrote down direct quotes that were found to be relevant. These interview questions were adapted from different literatures, journal articles and international standards.

3.4 Data Source

A research whether it is qualitative or quantitative should have a data source and the data source will be different based on the type of research and its content. In order to collect the required data that meets the research objective, sampling technique is applicable to identify the exact data source from the whole unit. The idea behind qualitative research is to select participants or sites (or documents or visual material) purposefully that will help best the researcher understand the problem and the research question (Creswell, 2009). This does not necessarily suggest random sampling or selection of a large number of participants and sites, as typically found in quantitative research. Sampling is a process of selecting units or individuals from a population with the intention of representing the particular population for study purposes. Hence, purposive sampling was preferable to identify data sources for this research. Purposive sampling is the most important type of non-probability sampling. Researchers rely on their experience, ingenuity and/or previous research findings to purposely obtain units of analysis in such a manner that the sample they obtain may be regarded as being representative of the relevant population (Creswell, 2009). The interviewees for this study were selected from members of Vulnerability assessment, Cyber Security Operation Center, Server and Network Management employees in bank ABC. Eight interviewees have been participated for this research the respondents has been selected based on their experience on vulnerability assessment operation and participation in each vulnerability assessment lifecycles.

3.5 Validity and Reliability

Validity in research is about the accuracy and trustworthiness of findings. Valid research should demonstrate what actually exists and valid instruments should measure what it is supposed to measure. Validity is the degree to which the interpretations and concepts have mutual meanings between the participants and the researcher. Bias can be overcome by several strategies such as triangulation and member checking. Data triangulation means using several methods for collecting evidence, such as interviews, document analysis and observation. This allows for studying a phenomenon from different perspectives and increases data quality (Yin, 2009). Member checking involves returning data material to the respondents for review and shows that their contributions are valued.

Reliability is the degree to which the findings of the research are independent of accidental circumstances and concerned with the consistency, stability and repeatability of the informant's account as well as investigators ability to collect and record information accurately. It is closely related to assuring the quality of field notes and guaranteeing the public access to the process of the publication of the research result (Creswell, 2009). It refers to the ability of a research method to yield consistently the same results over repeated testing periods.

In order to reduce the risk to the validity and reliability of this research, the researcher has performed the following tasks.

- To reduce sample bias, sample selection was based on the ability of the respondents to provide data, which is relevant to the research questions. The researcher judgment based upon the best available evidence to choose interview participants who knows enough was applied.
- The researcher clarified the nature of the research, why the research conducted in their bank, how the data is going to be collected, and for what purpose the study is used. This creates a trust relationship between the participants and the researcher.
- Since the subject matter of the research is sensitive, the interpersonal context under which the data gathered was taken in to consideration by the researcher. Interview was conducted in comfortable, secure, and private surroundings preferably in the interviewee's office, which was convenient for them.

- The researcher's observation of the real environment and practical experience on the subject matter was crucial. The data collected from face to face interview and document analysis was analyzed using triangulation

3.6 Data Analysis

This study used thematic analysis and the researcher transcribed interview recordings and used coding techniques. Initially the researcher read and re-read the transcripts from the recorded interview in order to filter out or identify the themes. And then review different initial codes to produce sub- themes. Next the sub themes were reviewed to define and name the themes. After the themes finalized the write up of the report has begun. The analysis has provided the following themes namely: - Creating baseline, vulnerability assessment, risk assessment, remediation, verification and Monitoring security and network traffics.

Thematic analysis is a method of identifying, analyzing and reporting patterns (themes) within data (Ashley, et al, 2018). Thematic analysis is a type of qualitative analysis used to analyze classifications and present themes (patterns) that relate to the data. Thematic analysis allows the researcher to determine precisely the relationships between concepts and compare them with the replicated data. By using thematic analysis, there is the possibility to link the various concepts and opinions of the learners and compare these with the data that has gathered in different situations at different times during the project (Alhojailan, 2012). Thematic analysis of open-ended responses from surveys or transcribed interviewees can explore the context of teaching and learning at a level of depth, that qualitative analysis lacks. While allowing flexibility and interpretation when analyzing the data, but it should be carryout with special care and attention to the transparency of the method in order to ensure confidence in findings (Ashley, et al, 2018). The flexibility of thematic analysis allows it to be used in both deductive and inductive approach (Alhojailan, 2012). A thematic analysis process analyzes the data without engaging preexisting themes, which means that it can be adapted to any research that relies only on upon participant's clarification.

Thematic analysis has the following phases (Lorellie, et al, 2017).

- Familiarization: - this phase involves reading and rereading the data to become immersed and intimately familiar with the data.

- Coding - this phase involves generating succinct labels (codes) that identify important features of data that might be relevant for answering the research question. It involves coding the entire dataset and after that collecting all the codes and relevant data extracts for later stage of analysis.
- Generating initial themes: - this phase involves examining the codes and collected data to identify significant broader patterns of meaning or potential themes. It then involves collecting data relevant to each candidate theme.
- Reviewing themes: - this phase involves checking the candidate themes against dataset, to determine the convincing story of data and the one that answers the research questions.
- Defining and naming themes: - this phase involves developing a detailed analysis of each theme, working out the scope and focus of each theme, determining the story of theme. It involves deciding on an informative name of each theme.
- Writing up: - this final phase waves together the analytic narrative and data extracts, and contextualizing the analysis.

Thematic analysis data investigation and generating theory is combined with its analytical element. This is particularly appropriate when the researcher aims to examine the data in order to discover common themes and to convey their experience. Thematic analysis provides the opportunity for researchers to move beyond calculating unambiguous words or statements.

3.7 Chapter Summary

This chapter has discussed about research design and methodology used for this study. Detail explanation for qualitative research and inductive approach was presented. Data sources and collection methods like interview and document analysis were presented in this chapter. In addition, thematic analysis discussed which used for the analysis of the collected data.

CHAPTER FOUR

DATA PRESENTATION ANALYSIS AND DISCUSSION

In this chapter, data from Face to face interview, document analysis and findings of the collected data presented. Findings are described in relation to the research questions prepared by the researcher. The findings obtained from the interviewees and document analyses described separately but the theme or information bases on the six-vulnerability assessment phase of EC-Council.

4.1 Respondents Information

The respondents of this research were Technical staffs with managerial and expert/officer level individuals those who play major role in vulnerability assessment tasks. Even if vulnerability assessment is the responsibility of vulnerability assessment team, but the task needs the involvement of other teams in order to have a secure information system. From the teams Cyber security operation center, Vulnerability assessment, server management and Network management managers including senior experts from each subunit were the main participants for this research.

4.2 Challenges in data collection process

The researcher submitted cooperation letter from AAU to Bank ABC and HRM office accepted the letter and write the interdepartmental memorandum letter to Vulnerability assessment manager to be cooperative with the researcher without compromising the bank policy and confidentiality. During this time, the manager was hesitated to accept the letter and he mentioned that vulnerability is a weakness in the banks information systems. Due to this, I am not going to accept this letter and allow you to collect such sensitive data because it is against the banks security policy. The researcher explains how it is possible to collect the data without mentioning the exact name of the bank and identity of interviewees in any aspect. The manager was confused that, how the

researcher is doing the research without mentioning the exact research area and would it be acceptable by the school. The researcher explained that he has agreed with his advisor to make the name of the bank represent as Bank ABC. After a long discussion, the manager has accepted the idea and willing to give the required information's without compromising the banks security policy and his identity. However, Covid 19 was one of the challenge to conduct interview and collect the required data. Since the research is qualitative and needs face-to-face interview with the selected interviewees, it was difficult to interview them due to their fear of sitting close in a small room will spread Covid. The researcher asked the interviewees to meet before working hour early in the morning and they were ready to cooperate. Even if there was so many challenges and took too long, the researcher has collected the information's from each of the interviewees.

4.3 Data Presentation

4.3.1 Data from Face to Face Interview

Among the data collection methods for this study, this section presents data's obtained from face to face interview The interviewees were Vulnerability assessment, server management, network management and cyber security operation center managers and some selected staffs from those departments.

Creating baseline

All Interviewees have almost the same understanding about information systems vulnerability and vulnerability assessment. The vulnerability assessment manager defined that, Information systems vulnerability is a weakness or hole in information system infrastructures, like network devices, security devices, applications, workstations etc. whereas Vulnerability assessment is finding or discovering of those weaknesses using scanning tools before attackers use this holes to break in to infrastructures. All managers define information systems vulnerability and vulnerability assessment the same as Vulnerability assessment manager described, they said vulnerabilities are weaknesses that outsiders or hackers can penetrate easily to disrupt the entire information systems of organizations. Vulnerability assessment manager said "… Vulnerabilities are weaknesses of information systems and this hole can happen due to Misconfigurations, outdated operating systems. Vulnerability assessment manager and staffs said,"… vulnerability assessment is a newly

established information systems sub unit in the last year's bank structure arrangement the bank has a plan for vulnerability assessment based on quarterly term but the plan may be changed based on the request of asset owners. Due to this, plans are not practical and tasks will be performed out of plans". The interviewees said there is no defined pre assessment task put in place by the bank.

Vulnerability assessment manager said:

"*... Even if we don't have a defined pre assessment task, we are doing many things before starting the scan which is collecting assets from asset owners and identify those assets based on their significance and device type*."

After identification of assets, we select the scanning tool that fits to the device type and schedule the scan. He also said vulnerability assessment team identifies the corporate network, applications, services and the whole infrastructure assets that the bank is using to provide effective service and protect the information systems from cyber security attacks. Vulnerability assessment manager mentioned that the bank doesn't have a documented procedure, policies and defined terms for vulnerability assessment because the department is newly established, but now the vulnerability assessment team is preparing the policies and procedures including for risk assessment policies and procedures said the IS officers of Vulnerability assessment team. Asset owners and monitoring team complains that vulnerability assessment team in not informing us when they start scanning and they schedule based on their own interest.

Vulnerability assessment

some interviewees have a common understanding about vulnerability assessment in the bank and described that vulnerability assessment is one of the main task in the IT sector of the bank and it is discovering the vulnerable holes or weaknesses of the banks infrastructures which is performed by specifically with vulnerability assessment team. Vulnerability assessment team were asked about how frequent the bank conduct vulnerability assessment said" … yes, the bank performs vulnerability assessment to the information systems and infrastructure to identify the vulnerable holes and weaknesses of information system and devices. The team performs the assessment until all vulnerabilities are fixed and be confident that our systems are secured. They said that, the targets of the assessment identified by the asset owner group and their service priority. During vulnerability assessment network and security devices, applications, operating systems and every

infrastructures vulnerabilities will be discovered either with credential or non-credential type of vulnerability assessment.

IS officer of the vulnerability assessment team member describes what credential and non-credential vulnerability assessment and their differences.

He said:

"*…credential and non-credential vulnerability assessments are the types of vulnerability assessments and differs with their authentication. Non-credential scans do not require trusted access to the system they are scanning and we are currently using to scan the vulnerabilities of our information systems. Credential scan requires credentials or admin privileges and does not need a trusted access to the system we are scanning. This scan type requires management and system owners' decision because it may bring system interruption and failure to the scanning system*."

The interviewees mentioned that they are using three licensed vulnerability-scanning tools Nessus, Nexpose Rapid 7 and a built in module vulnerability scanner on IBM Qradar SIEM. These tools has multiple options of reporting format to visualize the scan results. One of the interviewee said the scanning tools have a limit on the number of assets they can carry out based on their license agreement. Having three different vulnerability scanning tools helps us to choice the fittest scanning tool for different infrastructure assets and it enables us to address a number of information systems with in license. Cyber Security Operation Center Manager said, "The primary task of Qradar SIEM is for monitoring purpose which enables us real time visibility of banks information security systems, but vulnerability assessment team is using this device as a scanning tool to discover vulnerabilities or weaknesses of information systems. The scanning brings additional task for the SIEM that is causing monitoring tool interruption and exceeds its EPS limit. We sometimes inform them to pause the scan whenever the SIEM is unable to display information security incidents during scanning. The scan alert notification makes the monitoring team busy and hides the real attack alerts. We have customized the CRE of SIEM to consider the scan alerts from vulnerability assessment team as false positive.

Network and server management managers also complain about the time schedule that vulnerability assessment team is scanning the systems and devices during working hour and it causes system performance degradation and slowness. Vulnerability assessment manager highly concerned about the lack of formal trainings for his staffs, this can improve the skill of employees to understand the scanning tools feature and to make a deep analysis on the discovered vulnerabilities. The management simply requests the final remediation result and current vulnerabilities status without interaction with the processes and our challenges. The team has knowledge gap some scanning tool features and vulnerabilities.

IS officer said:

"….We are scanning vulnerabilities from the local network and we have never tried to scan from the external network".

Risk assessment

The interviewees believes that risk assessment is essential for organizations and it should be a concern for financial sectors. Vulnerability assessment and Cyber security Operation Center managers define risk assessment as:

"*… It is identifying the risks that vulnerabilities will cause and looking forward to remove or minimize the risks before it happens*".

Server and network management managers also define risk assessment as the process of projecting what will happen in the future on the business and technology side of the organization if something wrong happens. The also said Bank ABC is conducting a risk assessment regularly but it is mostly from business side. Vulnerability assessment team is preparing a risk assessment procedures and policies but still it is not practical. The interviewees said the only thing that we take as a risk assessment is that the Impact level and severity of vulnerabilities from scanning report. At the beginning of 2021, there was a discussion to begin technical risk assessment but not yet.

Remediation

As interviewees pointed out remediation of vulnerabilities is the core component of vulnerability assessment. Server management and network management managers said "…the identified vulnerabilities coming from vulnerability assessment team distributed to the responsible organ or asset owners based on vulnerability type groups. The asset owner assigns dedicated individuals to interact and communicate with vulnerability assessment team for remediation follow up and prepares an action plan. Most of the time remediation of vulnerabilities requires the involvement and support of product vendors in order to have common understanding and possible patches. They also mentioned based on our support request the vendors quickly react on the discovered vulnerabilities and recommends us the best option if it can be fixed by our side unless, the vendor requests a remote access to the vulnerable servers.

IS officer said that:

"*….Sometimes our devices does not support the latest patches due to hardware compatibility issues and we face difficulties to remediate such vulnerabilities." Vulnerability assessment manager said even if remediation of vulnerabilities is the responsibility of asset owners, our team supports them when they request our involvement. Asset owners are responsible and accountable for remediating actions to the discovered vulnerabilities and systems. He also said there are many vulnerabilities, the bank can remediate without the support of product vendors. These vulnerabilities needs policy change and access control list on network and security devices to make secure the way admins access to critical devices. The IS officer said, system admins use a telnet connection for remote access to different infrastructures, which is not secure puts usernames and passwords as plain text and unencrypted. This telnet remote access will allow attackers to sniff the passwords and usernames of critical infrastructures. We have discussed with the technical teams and recommend to use a secure SSH remote connection during access to information system assets. Now almost all system admins are using a secure SSH remote access because telnet access is deactivate on selected devices. Network management manager declare the vulnerabilities on network and security devices mainly requires change of policy and procedures. He also said the previous network topology has many routing problems and many unmanaged devices. By 2020, we upgraded the entire LAN and this project fixes many vulnerabilities*".

Server management manager said our team mainly focuses on remediating OS and certificate vulnerabilities. If the vulnerabilities are application, database, or webserver software related we communicate with those teams and they would react to remediate. These teams communicate with product vendor customer support team and shares the issue. The interviewees also added if these vulnerabilities are critical and needs immediate action, the remediation action should be informed to the change management team and prepare a plan for remediation. The change management makes the assessment announces to asset owners with time of downtime during remediation including all the necessary requirements. The vendor sometimes requests to run a credential scan on the device in order to check the reality of the discovered vulnerabilities and it is a challenge for remediation of vulnerabilities with in short time. Cyber security operation center manager said:

"…vulnerability assessment team discovers vulnerability on our Monitoring tool on Jan 2021, and we have requested the vendor to support us. After their deep analysis on the vulnerability, they request to run a credential scan but the management were not willing to allow the scan. In the last, they recommend us to upgrade our SIEM to the latest version but the hardware appliance is not compatible with the latest version. Even if we request the management to purchase the new appliance not delivered yet. Such type of challenges are making the vulnerability assessment process running out of time".

Some remediation actions require down time in order to deploy the patches, and the down time of a single device will affect the business operation. On financial sectors, a minimum time of business interruption will cause a huge financial loss and fail to their competitive advantage. However, security breach by attackers through the vulnerabilities will cause a huge financial loss and the infrastructures will be under the control of attackers.

Vulnerability assessment manager said assets owners take remediation of vulnerabilities as their extra job responsibility and sometimes they do not accept the scan reports. We know that every team have a job description and considers this task as additional and they do not give attention. He also mentioned a meeting was held regarding to this issue with asset owners and our team explains the impacts of vulnerabilities and they agreed to do their best but still there is a problem on remediation of vulnerabilities.

Verification

Interviewees understood that remediation of vulnerabilities should be verified in order to know how much the remediation is successful. We made a rescan in order to check that assets owners fixed the vulnerabilities or not as interviewees said. After asset owners take remediation action for vulnerabilities, they report to vulnerability assessment team with remediation report.

Vulnerability assessment manager said that:

"*… we don't have any other option of verifying that the vulnerability is fixed or not rather than scanning the system again with the same tool scanned previously and it makes our task repetitive and causes system performance degradation". He also said that a rescan does not consume our scanning tools license because the tool once captures the assets*".

As interviewees mentioned that most of the time not all of the vulnerabilities on a single system may be remediated at once because the nature of vulnerabilities varies with their impact level and way of remediation. Vulnerability assessment team rescans the system using the same vulnerability-scanning tool, they use during the initial scanning process and compare the current scanning result with that of the previous scanning result. A rescan and communication with assets owners continues until all the discovered vulnerabilities gets a solution.

Monitoring

.Interviewees declare that monitoring system and network traffics regarding to cyber threats is the major responsibility of cyber security operation center team. Network traffics in and out to the globe are monitoring by cyber security operation center team by using different monitoring tools. The manager of cyber security operation center said that:

"*…in the bank's cyber security operation center room, we monitor the information systems 24/7 using security information and event management tool called Qradar SIEM*".

Security analyst also said that:

"*… We were using Imperva WAF and DAM tool to monitor web servers and databases but now those tools are outdated and now they are on purchase order stage to upgrade the tools*."

Interviewees define Qradar SIEM as one of the most highly effective monitoring tool that many international organizations are using to monitor their information systems." As the interviewees

stated that all the assets are integrated with Qradar SIEM to send different logs to Qradar. Qradar has CRE, which analyzes the incoming logs and classify based on their attack category and creates an offense. Qradar SIEM collects events from devices by using DSM file. For windows OS type devices an agent is installed on servers and Linux OS devices needs only traffic redirection permission on checkpoint and firewalls. Based on the collected logs the security analysts review the logs and identify the real attempts and false positive alerts. If the offenses are real attacks/attempts, the security analyst escalates the incident for the respective either to block the attackers IP or isolate the infected client from the network. Interviewees described that the detected incidents may be escalated through ICD, Phone, and Company mail, which depends, based on the incidents priority. The cyber security operation center manager described that; those offenses detected by the Monitoring tool (Qradar) will assign to the security analyst and register to incident handling tool called ICD.

Many security devices are in place to protect the banks information systems from cyber threats. Among these, FTD is the one, which used to filter the network traffic and blocks the suspicious activities based on the ACL and policy rules. Check point which act as internal firewall and filters network traffics with in the intranet. Symantec AV is installed on every client and server to protect assets from malicious threats. There is a regular automatic scan scheduled on every client and server to scan for infected clients. The interviewees said Qradar SIEM has a threat intelligence feed which checks the detected IPs profile from the globe and it enables us to easily identify the previous history of the IP whether it is suspicious or not. If such IPs have a malicious or scanning activity before the threat intelligence feed groups the IP as malicious with high-risk score. Cyber security operation Center manager said:

"…. *One of the major incident we are detecting is the Wannacry Ransomware, starting from May 2017 and it infects many clients worldwide. Wannacry infects devices of many organizations and encrypts file on the machine then requests the organization to pay in order to decrypt those files*."

Interviewees worried about Wannacry because its impact can cause a huge damage to the banks infrastructures. It causes system performance degradation, uses high network bandwidth and may bring loss of banks reputation. Server manager also said Wannacry is our biggest attack attempt to our information assets but still we can resist by installing the latest Symantec AV on every devices and disabling the worm transmission ports on firewalls. Wannacry is not successful to ask payment

but it may cause system interruption by consuming the highest network bandwidth of the organization. IS officer from monitoring team noted that using of a single client for data and internet line interchangeably might enable attackers to intrude our systems easily. We have notified this issue to the management and still there are clients using in such a way. Proxy server does not filter their internet access and this may allow attackers to drop malicious files to client. Many organizations are requesting and visiting the monitoring room and we are sharing the best practices of cyber security operation center. This will initiate other organizations to build a best cyber security operation center and monitor their infrastructures network traffics and assets security.

4.3.2. Data from Document Analysis

Most of the interviewees noted that Bank ABC does not have a defined document for the responsibilities they carried out. Each technical team is preparing their own document format related with their tasks. Vulnerability assessment manager said our team is established one year ago but still they have no a defined policy or procedure for vulnerability assessment. The scanning tools generate the reports and the team customizes based on the sample-reporting format they use. The researcher refers some documents prepared by IS personnel and they are using as a temporary standard for reporting and monitoring activities. The following table illustrates the document of the scanning result, which is customized by vulnerability assessment team to forward for asset owners for their remediation action.

As table, 4-1 below shows, it is the reporting format of vulnerabilities to asset owners. The document has a detail vulnerabilities report with their, vulnerability name, scan date, severity, and impact of vulnerabilities, proposed solution and the IP address of the asset. Vulnerability assessment team describes the vulnerabilities and clarifies in order to make the remediation process easy for the asset owners. Asset owners only required to remediate the vulnerabilities based on the proposed solutions and impact level.

Description	**Scan date**	**Vulnerability**	**Severity**	**Concern**	**solution**	**Asset IP**
An Obsolete Version of Oracle	Sat, Jan	Oracle Linux Obsolete Version	Critical	Unsupported versions of Oracle Linux may contain	Upgrade to a supported	Intentionally left blank

Linux Running.	16th, 2021			unpatched security flaws. It is recommended to upgrade to a supported version.	version of Oracle Linux	
The server's TLS/SSL certificate is self-signed.	Sat, Jan 16th, 2021	Self-signed TLS/SSL certificate	Medium	Self-signed certificates cannot be trusted by default, especially because TLS/SSL man-in-the-middle attacks typically use self-signed certificates to eavesdrop on TLS/SSL connections.	Replace TLS/SSL self-signed certificate	
The server supports one or more weak key exchange algorithms.	Sat, Jan 16th, 2021	SSH Server Supports Weak Key Exchange Algorithms	Medium	It is highly advisable to remove weak key exchange algorithm support from SSH configuration files on hosts to prevent them from being used to establish connections.	Disable weak Key Exchange Algorithms	
The prime modulus offered when diffie-hellman-group1-sha1 is used only has a size of 1024 bits.	Sat, Jan 16th, 2021	SSH Server Supports diffie-hellman-group1-sha1	Medium	The prime modulus offered when diffie-hellman-group1-sha1 is used only has a size of 1024 bits. This size is considered weak and within theoretical range of the so-called Logjam attack.	Remove ssh-diffie-hellman-group1-sha1 from the Kex Algorithms list specified in ssh d_config.	

Table 4-1 Vulnerability Reporting Format

Monitoring team has their own incident handling process but the management level officials do not approve it. Even if they have a temporary incident handling process standard it is difficult to apply on their environment. Lack of skilled and professional employees on Tier -3 is a challenge

to perform the incident handling process successfully. Tier-3 analysts are required to perform a detail analysis for the attack attempt and prepare threat-hunting mechanisms. The incident handling process of information security incidents in cyber security operation center, which is not approved by the management used as a guide document, looks like as below.

Incident handling over all Work Flow process

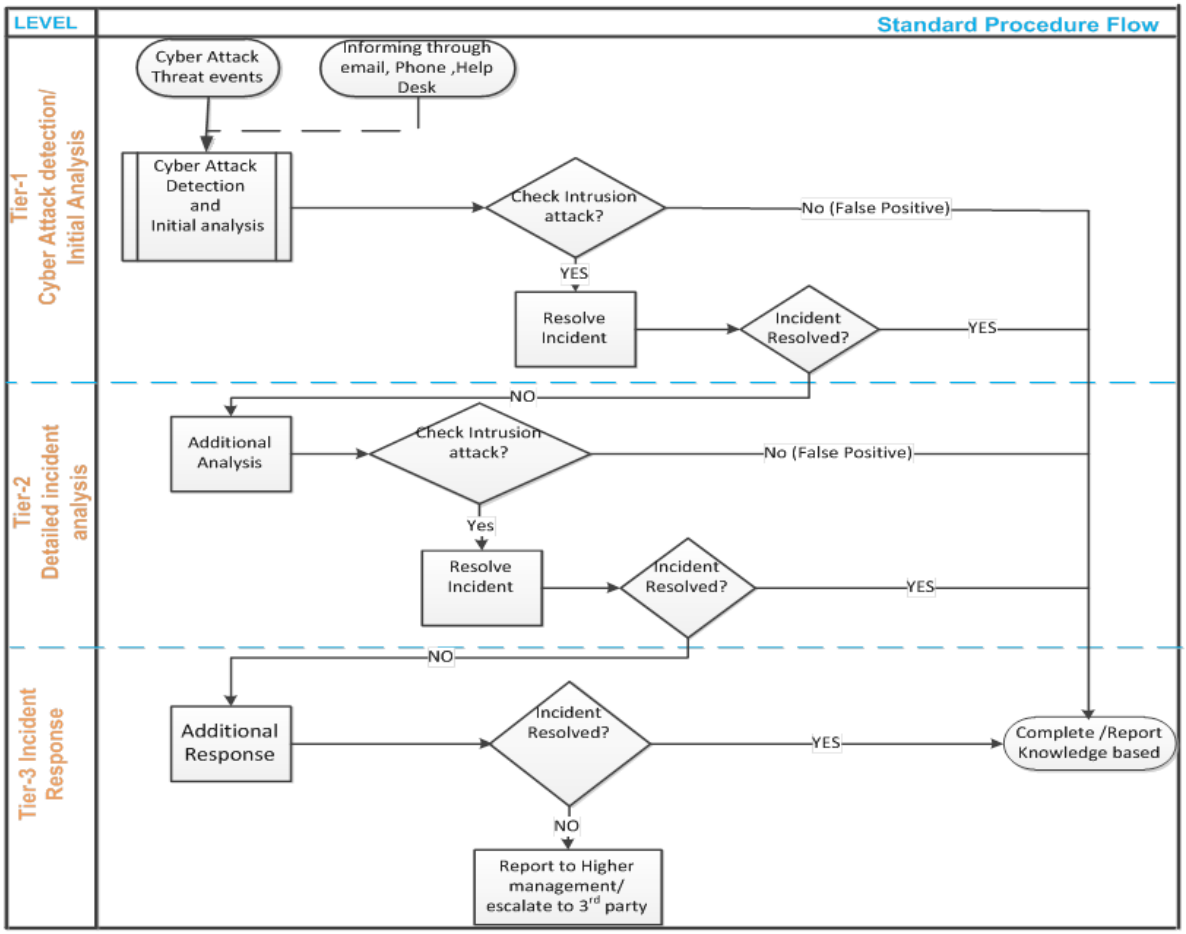


Figure 4-1 Incident handling process

Steps for incident handling during monitoring of information security incidents at Cyber Security Operation Center illustrated in figure 4.1.

- Cyber security operation center team Monitors incidents 24/7 using Qradar SIEM.
- SIEM collects all the incidents and display on the dashboard
- Tier 1 analysts detect and make initial analysis and check the attack behavior whether it is real attack or false positive. If Tier 1 can handle the incident analyst takes an action either escalate or change rules, if not sent the case to Tier 2 analysts.

- Tier 2 makes additional analysis on the detected incident and either closes the incident with reason or escalate to the next Tier 3 analyst
- Tier 3 analyst make further analysis and communicates with respective organs either with management or with third party support teams.

4.4 Discussion

Information security is becoming a big concern for many organizations and they use security devices to protect their information assets from security breach. However, organizations are still a target for criminals and this implies they need to check their security devices are in the right posture. It brings the idea of vulnerability, which is the weakness or vulnerable hole in their information systems. Many researchers have studied on information security and vulnerability assessment topics from different approaches. Even if those researchers focus on information security areas, no local researcher has addressed vulnerability assessment issues for financial sectors yet.

How Bank ABC is performing information systems vulnerability assessment?

Many scholars and international technology institutions have described the importance of doing vulnerability assessment for the sake of keeping organizational infrastructures from cyber-attacks. SANS, NIST and EC-Council have stated that having a well-defined vulnerability assessment procedure is becoming a mandatory for organizations. SANS has a life cycle consists of five phases namely preparation, vulnerability scan, implement remediation actions and rescan. Whereas EC-Council published a vulnerability assessment lifecycle, which consists of six phases namely, Creating baseline, vulnerability assessment, risk assessment, remediation verification and monitoring. The life cycle by EC-Council is most accepted and widely used standard by many organizations. All the interviewees noted that Bank ABC has established vulnerability assessment team since 2020, but it does not have a defined vulnerability assessment policy and procedure yet. In addition, the bank is not compliant with EC-Council's vulnerability assessment life cycle, which composed of six phases. Technical scholars claim that companies should conduct vulnerability

assessment and promptly remediate vulnerabilities before security breach occurs through these weak security holes. Vulnerability assessment team has their own plans but top-level management officials do not approve it. Scheduling the scan frequently enables the organization to discover vulnerabilities and take remediation actions in a timely manner. IS officer said, *"….even if there is a temporary action plan the scan and remediation actions will not be performed based on their schedule due to several issues"*.

As a pre-assessment task before vulnerability assessment, it is required to study the nature of corporate network, infrastructures, learn about security policies, procedures and inventory of all assets. Informing the teams managing Firewalls, checkpoint, network and security devices including all information assets should be part of planning phase before vulnerability scan starts (Tom, 2013). Depending on the mandate of asset owners, it is necessary to get formal approval form respective technical staffs before vulnerability scan. This can help asset owners to check their requirements such as not scanning production systems outside of maintenance or only during business hours. Bank ABC does not address all the tasks on this phase, only collecting list of infrastructures from asset owners is the primary task. The bank has three vulnerability scanning tools namely IBM Qradar SIEM, Nessus and Nexpose Rapid 7 and the interviewees cleared that these tools are licensed. Even if the bank uses those tools to scan the vulnerabilities, the procedure does not fit with best practice of EC-Council vulnerability assessment life cycle.

Before initiating the scan, the team selects the scanning tool, which fits the device in order to get the best result and for successful vulnerability discovery. Some Organizations in Ethiopia are not aware of vulnerability assessment and its relevance to their entire information systems security and it is the same in Bank ABC due to lack of common understanding between vulnerability assessment team and other technical and management level staffs. EC-Council mentions that risk assessment enables to determine the impacts that vulnerabilities could bring to the information assets and actions to remove or mitigate the risks. As vulnerability assessment manager said a well-defined technical risk assessment procedure is not yet available, the team is trying to prepare by themselves without approval of management officials. The security personnel should analyze the vulnerabilities from technical perspective and answer questions such as, if patches are available or whether the configuration could be hardened? (Tom, 2013). However, in bank ABC the vulnerability assessment team forwards the scanning result to the asset owners with form of

reporting template. Asset owners checks the feasibility of remediation actions whether installing a certain patch will result in the device with no longer support from vendor. They prepare their own action plan for remediation of vulnerabilities but a clearly stated deadline is required. If short term is not possible, restricting network access to the vulnerable service should be implemented in order to remove the risk without correcting the vulnerability. However, this is not happening in Bank ABC, asset owners do not take temporary solutions until the discovered vulnerabilities on systems gets a remediation. Interviewees said there is a vulnerability discovered on a single system on January 2021 but still remediation action is not taken because the vendor requires us to upgrade the application and the current hardware is not capable to carry out the latest version of the application. Asset owners implement the remediation action based on their own action plan. They forward their remediation result to vulnerability assessment team and the team schedules a rescan in order to verify whether the remediation action performed perfectly or not. Vulnerability assessment manager said that

"*… we don't have any other option of verifying that the vulnerability is fixed or not rather than scanning the system again with the same tool scanned previously and it makes our task repetitive and causes system performance degradation*".

Using the same scanning tool during the first scan and on rescan helps to compare the scanning results. Information sharing and communication with asset owners enhances the remediation and verification processes to make accurate. From the six phases of vulnerability assessment gibe provided by EC-Council, Bank ABC is better on monitoring and vulnerability scanning phases, but on creating baseline, risk assessment, remediation and verification lacks consistency. The overall vulnerability assessment process of Bank ABC is not partially compliant with EC-Council's vulnerability assessment lifecycle.

What challenges exist in vulnerability assessment of Bank ABC?

Bank ABC has established vulnerability assessment team in 2020. The team is doing the assessment as much as they can. However, the interviewees has mentioned they are facing different challenges to perform effective vulnerability assessment and discover vulnerabilities. Even many of technical staffs and management official does not have a common understanding what value adds the assessment to the banks information security posture. Lack of defined standard and procedure makes the vulnerability assessment to be considered as a non-existent. Employee's lack of trainings about the scanning tool makes difficult to analyze the scanning results. Scanning the information assets and devices during business hour makes the system performance degradation and busy. This leads the asset owner not to accept the requests from vulnerability assessment and brings postponement on the remediation actions. The management level officials also require the result of the remediation action without creating suitable conditions and procedures for vulnerability assessment process. Vulnerabilities will not remediate with in short time because some patches have compatibility problem with the current hardware and this has its own purchase process. Vulnerability assessment team does not have privilege for systems and devices to take remediation action and follow the progress. Many scholars declare that having effective vulnerability assessment enhances the security posture of the organization in addition with different control mechanisms and measurements.

4.5 Chapter Summary

The data gathered from participants and documents for this study discussed using EC-Council, 2018 vulnerability assessment life cycle guide. The respondent's information, challenges during data collection, data presentation and analysis of the collected data using interview and document analysis, gaps and challenges of information systems vulnerability assessment at the bank has been discussed.

CHAPTER FIVE

CONCLUSION AND RECOMMENDATIONS

This chapter concludes the whole study. It revises and discusses the summary of key findings, presents conclusions and recommendations. Suggestions for further studies have been forwarded for future study to help other researchers further extend this study.

5.1 Conclusion and Findings

Most organizations have realized that security breaches can have a negative influence on the business process continuity, public image, cause financial lose or create problems with legal authorities in case of noncompliance. Banks are among the operators in the financial sector in Ethiopia and bank ABC is the one in financial ecosystem. Due to the nature of its business, bank ABC needs to have strong security systems in order to protect its information asset from highly increasing threats. Securing information systems from current and future threats requires abroad and unbiased view of system vulnerabilities, as well as creative consideration of security and stability options in the face of resource constraints. Many researchers have studied on information security and vulnerability assessment topics from different approaches. Even if those researchers focus on information security areas, no local researcher has addressed vulnerability assessment issues for financial sectors yet. Therefore, the researcher aims this study towards improving information systems vulnerability assessment practice at bank ABC and come up with suggestions for improvement standing from the current practice and identifying the challenges exist during vulnerability assessment process in the bank.

Efficient way of conducting vulnerability assessment gives successful scan results and contributes for discovering weaknesses of the information systems before it is prone to attackers. Many international standards, policies and procedures of vulnerability assessment are considering vulnerability assessment as a part of information security mechanisms with the help of security devices. Bank ABC does not have a defined vulnerability assessment policy and procedure that

could help them to discover vulnerabilities, remediate and minimize the risk impact of vulnerabilities. Vulnerability assessment team has a responsibility of identifying vulnerabilities in networks, applications and servers and asset owners handle the remediation action of the vulnerabilities. However, interviewees mentioned that the misunderstanding and lack of attention on vulnerabilities makes the remediation process difficult and takes too long. Whereas all interviewees complain about lack of trainings and the management has promised many times to facilitate the opportunity but still they are not satisfied with management decision. Employees should have enough understanding about the scanning tools to make a deep analysis on vulnerabilities and to select suitable patches for security holes. This imposes to rely on the product vendor's suggestion and their involvement in every remediation action. Trainings for the employs plays a vital role to create a secure environment and skilled human power.

Nonexistence of a dedicated team for remediation makes the vulnerability process as an additional assignment for IS officers. Vulnerability assessment team only have the privilege of scanning the systems using a defined tool and forward the scan results for remediation to asset owners. Asset owner's main concern is managing the information systems; check the service availability and other responsibilities appointed for them on job description. They also complain that vulnerability assessment team is not informing us when they initiate the scan. There is lack of awareness sessions regarding to vulnerability assessment advantage and requirements for IT personnel's, asset owners and management level officials, which can improve their understanding and expectations about vulnerability assessment team. Vulnerability assessment requires a collaborative action from IS personnel's and management side, their skill and experience matters a lot for the successful process. Introducing vulnerability assessment to organizations and employees will have a challenging aspect, attention should be paid and responsibilities clearly assigned. The accuracy of the vulnerability assessment process is in doubt because of nonexistent procedure and plan, the team only checks during verification or rescan.

This study has shown that Bank ABC has many challenges to conduct a successful vulnerability assessment process. Some of the challenges are IS personnel's and management officials lack of attention and understanding to vulnerability assessment, lack of skilled professionals to analyze the vulnerabilities, asset owner's negative perspective about the scan and remediation responsibilities, lack of a predefined standard and procedure etc.

Organizations must have policies, processes and tools in place to not only defend against attacks but also strengthen their security posture by reducing organizational risk. Vulnerability assessment processes are foundational in managing cyber security risks, but for a variety of reasons, vulnerability assessment processes often stall or break down. The following best practices will improve the vulnerability assessment practice of the bank.

- ✓ **Scan hosts more frequently than networks:** network based scanners add significant overhead as they scan through network services. They also require attention such as configuration settings, opening firewall ports etc. host based scans on the other hand do not traverse the network, they eliminate network overhead and allow more continuous scanning.
- ✓ **Use multiple factors and context based risk assessment to prioritize the remediation:** a variety of internal and external sources should be correlated to understand the severity of vulnerabilities with in organizations environment. CVSS scores, thereat intelligent repositories, banks asset management and change management systems to understand the business criticality and security posture of the asset threatened by the vulnerability.
- ✓ **Use vulnerability assessment metrics that improve and fine tune detection, prioritization, and remediation processes**
- ✓ **Maintain single source of truth for all relevant teams:** many teams may interact in vulnerability assessment process and effective collaboration and common understanding between teams results a successful remediation
- ✓ **It is not all about patching:** vulnerability remediation must take shape in a reality where patches are not the only solution. Other remediation approaches including configuration management and compensating controls, such as shutting down a process, session, or module. It requires a knowledge base to match the best remediation solution to vulnerabilities based on the Banks's cumulative vulnerability process experience.
- ✓ **Use remediation playbooks:** to minimize the impact of vulnerabilities, remediation should be automated as possible. Once the IT personnel's define playbooks for remediation, the playbooks can remediate vulnerabilities automatically. The following flowchart show a simple playbook, which can perform remediation by its own.

5.2 Recommendations

Organizations are becoming highly dependent on information technology and it brings both positive and negative impacts on the connected devices. The technology brings simplicity to the day-to-day activity of individuals using technology. However, the technology also makes these devices to be a target for attackers from everywhere. By considering the current practice and challenges of information systems vulnerability assessment in Bank ABC, the researcher recommends the following for bank ABC and other organizations for a better way of vulnerability assessment process.

- The management with the help of technical personnel should prepare information systems vulnerability assessment procedure and policy, which helps to ensure vulnerabilities discovery, risk assessment and their remediation.
- Establish a dedicated team for vulnerability assessment with full privilege and responsibility of vulnerability assessment process, which is composed from different IT departments.
- Vulnerability assessment team with the support of management officials should create awareness sessions regarding to vulnerability assessment advantage and requirements for IT personnel's, asset owners and management level officials, which can improve their understanding and expectations about vulnerability assessment team.
- The management should make suitable opportunities for IT personnel to get formal Trainings; this can improve the skill of employees to understand the scanning tools feature and to make a deep analysis on the discovered vulnerabilities.
- Before starting the scan, Vulnerability assessment team should inform individuals managing infrastructures, which helps them to check their requirements of not scan the assets and time of scan.
- Vulnerability assessment team should perform external scan, it can provide overview of vulnerabilities, which are visible from outside the local network.
- Vulnerability assessment team should schedule the scan frequently, typically on a weekly or monthly basis out of working hour and Perform detail risk assessment for the vulnerabilities and identify their impact level.

- Vulnerability assessment team should start with small scope of scan and set clear deadlines for remediation of vulnerabilities. Delay in remediation action will increase the probability of vulnerabilities to be discovered by the intruders.
- Asset owners should give attention for vulnerabilities and minimize remediation delay; make the assigned team responsible and accountable for their responsibilities.
- The management and vulnerability assessment team should check the accuracy of vulnerability assessment processes based on the defined plan and procedures.

5.3 Limitation and Future Work

The aim of this study is towards improving information systems vulnerability assessment in Bank ABC. Through this, the bank's current practice of vulnerability assessment assessed and challenges identified. The intention of the researcher was to know the most common vulnerabilities but with confidentiality policy, the respondents hesitate to mention except some. To enhance the security of information systems in an organization studying more on vulnerability assessment can bring advancement. Further studies can be conducted on the following areas.

- Many technology companies suggest different vulnerability assessment methodology composed of different phases; however, future researchers can develop a new vulnerability assessment methodology or life cycle, which is more preferable than current existed lifecycles.
- Organizations security posture differs with their type of security device, personnel's capacity, scope and so on. Therefore, conducting the same study on other financial institutions and business sectors would bring some additional knowledge on vulnerability assessment.
- By selecting two different organizations, the one performs vulnerability assessment and the other not, conduct a study on vulnerability assessment and show the visibility and value the assessment adds to the organizations. This will clarify what organizations benefited from vulnerability assessment

- Vulnerability assessment also can be conducted from physical vulnerability aspect, and this will elaborate how organizations keep their information assets, data centers and critical infrastructures from being vulnerable to physical attacks or damage.

REFERENCES

Abselom, N. (2015). Practices, Challenges And Prospects Of Information Security Policy In Ethiopian Banking Industry. *(Masters Thesis)*. Addis Ababa University, Addis Ababa, Ethiopia.

Acunetix. (2020). *Web Application Vulnerability Reoprt* .

Alexander, A. (2016). Main Reasons of Information Systems Vulnerabilities. *Global Journal of Pure and Applied Mathematics*.

Amanda, K. (2008). Technical Guide to Information Security Testing and Assessment. *Recommendations of The National Institute of Technology (NIST)*.

Ankita Gupta, K. K. (2013). Vulnerability Assessment and Penetration Testing. *International Journal of Engineering Trends and Technology*.

Aon. (2019). *2019 Cyber Security Risk Report.*

Ashley, A. (2018). Thematic Analysis of Qualitative Research Data: Is It As Easy as It Sounds? 807-815.

Atreyi, K. (2003). An Integrative Study of Information Systems Security Effectiveness. *International Journal of Information Management*, 139-154.

Brian, S. (n.d.). Vulnerability Assessment for Security in Aviation Cyber Physical Systems.

CEH v10: EC-Council Certified Ethical Hacker Complete Training Guide. (2018). In EC-Council, *Certified Ethical Hacking Workbook.* EC-Council.

Chanchala, U. (2016). Security Testing and Assessment of Vulnerabiltiy Scanners in Quest of Current Information Security Landscape. *International Journal of Computer Applications (0975-8887)*.

Charles, D. (2013). The Use of Vulnerability Assessments: A Survey. *Masters Thesis*.

Creswell, J. W. (2009). Research Design Qualitative, Qualtitative and Mixed Method Approaches. SAGE Publications.

(2020). *Cyber Security Report* . Check point Research.

Daniel. (2004). Security in Modern Business: Security Assessment Model for Information Security Practices. *Pacific Asia Conference on Information Systems.* Association of Information Systems.

EC-Council. (2018). CEH V10 Module. *Ethical Hacking and countermeasures, Vulnerability Analysis*.

Fariborz, F. (2004). Developing a Risk Management System for Information Systems Security Incidents. *(Dissertation)*.

Girum, A. (2016). Assessment Of Information Security Culture In The Banking Industry: The Case Of Development Bank Of Ethiopia. *(Masters Thesis)*. ST. Mary University, Addis Ababa, Ethiopia.

Goddign, I. (2020). *2020 MidYear QuickView Data Breach Report.* Cyber Risk Analytics.

Hiran. (n.d.). Vulnerability Assessment Methods- A Review. *TIFAC CORE in Cyber Security Centre*.

Houghton, K. (2003). Vulnerabilities and Vulnerability Scanning. *Information Security Reading Room.* SANS Institute.

INSIGHTS. (April, 2019). *Banking and Financial Services Cyber Threat Landscape Report.*

Isabel, S. e. (2017). Evaluation of Vulnerabilities in Computer Systems Users.

ISACA. (2017). *V ulnerability Assessment.*

Jai Narayan Goela, B. M. (2015). Vulnerability Assessment & Penetration Testing as a Cyber Defence. *3rd International Conference on Recent Trends in Computing 2015 (ICRTC-2015)*, 710-715.

James, E. (2009). First Principles of Vulnerability Assessment.

Jean, F. P. (2019). A Review of Information Systems Security: Types, Security Issues, and Main Systems Affected. *International Research Journal of Engineering and Technology (IRJET)*.

Jeffry, I. (2006). Extracting Useful Information From Security Assessment Interviews. *Proceedings of the 39th Hawaii International Conference on System Sciences*.

Jonas, J. N. (n.d.). Modeling and Assessment of Systems Security. *Swedish Defense Research Agency*.

Kelmie, T. (2013). Information Security Managment Framework For Banking Industry In Ethiopia. *(Masters Thesis)*. Addis Ababa University, Addis Ababa, Ethiopia.

Lihua, & Yanwei. (2018). Security Measurement for Unknown Threats Based on Attack Preferences. *Security and Communication Networks*.

LLP, K. P. (1998). Vulnerability Assessment Framework 1.1. Critical Infrastructure Assurance Office.

M.Madhusduhanan, M. (2015). Web Security Vulnerability Assessment and Recovery Mechanism. *International Journal Of Engineering Sciences and Research Technology*.

Malahat, N. Z. (n.d.). Review of INformation Security Vulnerability: Human perspective.

Mastewal, G. (2020). Proposing Information Security Risk Assessment Methodology For Commercial Bank of Ethiopia.

Matunda, N. (2005). Enterprise Vulnerability Management and Its Role in Information Security Management. *Information Systems Security*.

Michael E.Whitman, H. J. (2012). *Principles of Information Security, Fourth Edition.* Kennesaw State University.

Milkiyas, B. (2018). Proposing Information Security AwarnessS Program For Enat Bank. *(Masters Thesis)*. Addis Ababa University, Addis Ababa, Ethiopia.

Mohammed, A. (2015). Cybersecurity And The Internet of Things: Vulnerabilities, Threats, Intruders And Attacks. *Journal Of Cybersecurity*, 65-88.

Nebyou, E. (2018). Assessment Of Information Security Maturity LevelL On Ethiopia Public UniversitiesS. Addis Ababa University, Addis Ababa, Ethiopia.

Nida, T. (2018). Impact Of Cyberattacks On Financial Institutions. *Journal of Internet Banking and Commerce*.

NIST. (2008). Technical Guide to information Security Testing And Assessment.

Omar, S. (2016). Information Systems Security Threats and Vulnerabilities: Evaluating The Human Factor in Data Protection. *Masters Thesis*. Kwame Nukurumah University.

Osiro, C. (2011). A Vulnerability Assessment Of Information Systems Security At The National Bank Of Kenya (NBK). *(Masters Thesis)*. KENYA.

Petter, T. (2005). Creating a Patch and Vulnerability managment program. *Recommendations of the national institute of standards and technology (NIST)*.

Rich, C. (2020). *Types of Security Vulnerabilities.* Retrieved from Balbix Blog: https://www.balbix.com/blog/the-9-types-of-security-vulnerabilities/

Said, N. (2019). A Review of Cybersecurity Measuring and Assessment Methods for Modern Enterprise. *International Journal of Informatics Visualization*, Vol 2 157-176.

Sasko, M. A. (n.d.). Security Vulnerability Assessment of OpenStack Cloud.

Satish, K. (2016). Information Security Threats, Vulnerabilities and Assessment. *International Journal of Adnanced Research in Computer Engineering & Technology*.

Shushilkumar, C. (2014). Secured Techniques for Vulnerability Assessment and Penetration Testing. *International Journal of Computer Science and Information Technologies, Vol. 5 (4)*, 5132-5135.

STEFAN, L. (2000). Observations on Operating System Security Vulnerability assessment. *(Masters Thesis)*.

Tesfaye, A. (2018). Cyber Security Auditing Framework (CSAF) For Banking Sector In Ethiopia. *(Masters Thesis)*. ST. Mary University, Addis Ababa, Ethiopia.

Tewodros, G. (2018). Cyber Security Practices and Challenges at Selected Critical Infrastructures in Ethiopia: Towards Tailoring Cyber Security Framework. *Masters Thesis*. Addis Ababa University, Addis Ababa, Ethiopia.

Tsedale, Y. (2018, JUNE). Assessment Of Information Security Incident Managment Practice In Ethiopia Bank. *(Masters Thesis)*. Addis Ababa University, Addis Ababa, Ethiopia.

Usman, I. (2010). Information Security Risk Assessment for Banking Sector- A case Study of Pakistan Banks. *Global Journal of Computer Science and Technology*, 44-55.

William. (2006). Development of an Malicious Insider Composite Vulnerability Assessment Methodology. *(Masters Thesis)*.

Xinhu Caoa, J. S. (2019). A fast reaction-based port vulnerability assessment: Case of Tianjin. *Transportation Research Part A*.

Yasasin, E. (2019). Forecasting IT security vulnerabilities – An empirical analysis. *Computers & Security*.

APPENDICES

Appendix A: Interview protocol/guide

Dear Respondent

My name is Abeje Abay and I am conducting thesis paper with a title "Towards Improving Information Systems Vulnerability Assessment practice in an Ethiopian Bank" for the partial fulfillment of requirement of Master's degree in information Science (information Systems Track). Your participation is highly required for the success of this study.

Your response will help a lot to know the information systems vulnerability assessment current practice and identify the existing challenges. Based on your responses, the researcher will recommend strategies to improve the vulnerability assessment in your bank.

The following interview questions are selected as relevant in order to answer the research questions. Therefore, this is to kindly request you to be interviewed for a short time.

Thank you for your cooperation!

Abeje Abay
0920-767462
abejeabay12@gmail.com

Basic Information

1. What is your job title?
2. Would you explain your main job responsibilities?
3. For how many years you have worked on this job.

Creating baseline

4. What does information systems vulnerability and assessment mean in your understanding?
5. Does your organization have existing plan for vulnerability assessment? Yes/ no
6. If yes, are those plans been properly practical? If not, why?
7. Is there an established information systems vulnerability assessment team in your organization? Yes/no if not why?
8. Does your organization has a defined pre assessment task?
9. If yes, do you use these tasks? If not, why not?
10. Is there a predefined down time during vulnerability scan?
11. What tasks you perform before starting vulnerability assessment?
12. How you identify the assets and prioritize the assessment?
13. How you plan, schedule and manage the tasks to make the assessment process effective?

Vulnerability assessment

14. Does your organization perform vulnerability assessment and how frequent it is?
15. How do you identify the targets of vulnerability assessment?
16. Which parts of information systems your scan address?
17. What type of vulnerability assessment tool you are using and why you choose the tool (criteria)?
18. Which type of vulnerability scan do you use, Credential or non-credential?
19. How do you generate and prioritize the findings after the scanning is complete?
20. Would you tell me the recent vulnerability on a single system?

    Does it successfully patched? Yes/no

    How the process looks like?

21. Do you have any success practice in relation to vulnerability assessment that you want to share for others?
22. What is the most challenging part of vulnerability assessment in your organization?
23. Anything you want to say about vulnerability assessment process.

Risk Assessment

24. What is risk assessment mean in your understanding?
25. Does your organization conduct risk assessment of vulnerabilities? If yes, how you determine the impact, threat and risk level of those vulnerabilities?
26. Which type of risk do you tolerate?

Remediation

27. What do you say about remediation of vulnerabilities?
28. Who is responsible in remediation of those vulnerabilities?
29. Would you describe additional works, which are performed when vulnerabilities patched?
30. What are the challenges you experienced during remediation of vulnerabilities?

Verification

31. How do you verify that vulnerabilities are fixed?
32. What will you do if there are vulnerabilities not fixed?

Monitor

33. How do you monitor network traffics and system behavior?
34. Is there a dedicated team for monitoring?
35. What type of monitoring tool you are using?
36. Could you describe the workflow from incident detection to the response?