YANGON UNIVERSITY OF ECONOMICS

DEPARTMENT OF COMMERCE

MASTER OF BANKING AND FINANCE PROGRAMME

MITIGATING SECURITY RISKS OF DIGITAL BANKING IN AYEYARWADY BANK

AUNG SOE MOE

(MBF- 6th BATCH)

DECEMBER, 2019

MITIGATING SECURITY RISKS OF DIGITAL BANKING IN AYEYARWADY BANK

A thesis submitted as a partial fulfillment towards the requirements for the degree of Master of Banking and Finance (MBF)

Supervised by:	**Submitted by:**
Daw Khin Nwe Ohn	Aung Soe Moe
Associate Professor	Roll No – 4
Department of Commerce	MBF 6th Batch
Yangon University of Economics	Yangon University of Economics

ABSTRACT

This study focus on investigating security practices using in Ayeyarwady Bank (AYA BANK) Digital banking services whether policies, procedures and framework are in line with industrial best practices to prevent the potential data breaches. The study focuses mainly on potential security risks that may happen in AYA Bank environment and figure out the security mitigation points to alleviate security risks. This study indicates the concepts of security risks in detailed and explain types of security risks especially the importance of insider risks. Study reveal that the rising of data breach happening in everywhere due to the internet usage surge. In the theory background, this study extract the unexpected loss caused by the technology misuse in the organization. Findings from analysis also shows that insider threats may harm AYA Bank services if the mitigation plans are not effective in place. Study explain AYA Bank security controls and measurement process with four different independent variables such as planning and engaging with security experts from industries to do security assessments, identify the weakness in the AYA Bank Digital Banking systems environment, controlling the access to internal information system and monitoring the services by physical human or using the automation tools. In the analysis part of the study, the questionnaire result reflect the current security practices of AYA Bank and give the findings, suggestions and recommend for further study. There is a need for AYA Bank services to define the high level security policies and practices. Findings of the study recommend AYA Bank to give the security awareness trainings and technical refreshment sessions to bank staff occasionally.

ACKNOWLEDGEMENTS

Foremost, I would like to express my sincere gratitude to Prof. Dr. Tin Win, Rector, Yangon University of Economics, for his concern, motivation, enthusiasm and encouragement to the participants of the Master of Banking and Finance (MBF) Programme.

I also would like to express my sincere thank to Prof. Dr. Nilar Myint Htoo, Pro-Rector, Yangon University of Economics, for her concern, motivation, enthusiasm and praise to the participants of the Master of Banking and Finance (MBF) Programme.

My deepest gratefulness goes to Prof. Dr. Soe Thu, Programme Director of the Master of Banking and Finance (MBF) Programme, Department of Commerce, Yangon University of Economics, for her guidance throughout the course of the study.

A debt of gratitude is also owed to my supervisor Daw Khin Nwe Ohn, Associate Professor, Department of Commerce, Yangon University of Economics, for her insightful comments, guidance and constant supervision through out the thesis period.

I also wish to thank my respected professors and lecturers of MBF program who shared their time and valuable knowledge during the course of MBF student tenure at the Yangon University of Economics. I would like to thank my MBF colleagues, friends, and classmates for their encouragement, support and knowledge sharing during my studies. Last but not least, I would like to heartfelt thanks to my family for giving the time, chance and support.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS

APP	Application for Mobile Phone/Tablet
AYA Bank	Ayeyarwady Bank
BYOD	Bring Your Own Device
e-Wallet	Electronic Wallet Application
FIs	Financial Institutions
HTTPS	Hypertext Transfer Protocol
IB	Internet Banking
IS	Information System
IT	Information Technology
MB	Mobile Banking
Netizen	Internet users
OTP	One Time Password
Pen test	Penetration Testing
PII	Personally Identifiable Information
PHI	Protected Health Information
SIEM	Security Information and Event Management
SOC	Security Operations Center

CHAPTER I

INTRODUCTION

In the 21st century, every citizenships in their respective countries are using modern banking services digitally or using usual way of brick-and-mortor services by making the relationship with banks. Banks are working hard to improve their customer experience and to adapt to emerging technologies and trends by digitizing their services, product and processes, and utilizing their data in a more meaningful way. In Myanmar, some banks are leapfrogging in technologies to serve better products and services to their customers while competing with other rivalry banks. The Leapfrog effect sometime help banks as fruitful service that grows the profit and customers in term. However, it may go wrong badly while the effect is go beyond the reach of the bank expectation. A few forward thinking bank are shifting away from legacy systems toward emerging technologies such as cloud based solutions and services on the cloud.

Trust is the mutual benefit between bank and its consumers for having the strong relationship for long term investment. Banks now a day in Myanmar are offering multiple ways of giving self managing services which reduce the dependency relying on the human resource of Bank Services. With digital banking and the need for personalization, the amount of personal data increases enormously. However, to optimize the protection of this data is a real challenge, as attackers have become incredibly smart. Data breaches or weak securities in internal systems can cost the millions of money, Bank it self is at the risk of bad reputation for handling the customer information. Bank are increasing spending on security products to get stronger security standard and policies implemented within the organization, get all the stakeholders involvement to collaborate on solutions to mitigate the potential frauds. Financial criminals are smatter than before and use sophisticated ways. Bank and FIs need to find the best way as a effort to mitigate risk of fraudulent activity in their system, facilities.

Most of the breach activities are found as the post incident result after the incident happened. Securing the software development internally is the one way of creating robust breach response model. In this model, many IT savvy required to work their structural daily routine in the Bank. Some bank has a team for remote monitoring and they can efficiently act in the event of data breach or security emergency case.

Bank established well organization structure to provide clear instructions on how to identify hazards and the process for managing these hazards, with regard to risk assessment. This is time taking and long process of involving multiple parties in the organization. Bank senior management and Head of IT personnel should take the overall responsibility for Corporate security, including Risk Management and, based on internal assurances guidelines implemented in the bank.

1.1 Rationale of the Study

Digital banking services in Myanmar started developed in 2014 although internationally it was started since mid and late 1990s. In 2000, 80% of United States Banks offered e-Banking service online. In 2001, Bank of America became first bank of having top 3 million online e-Banking users which is more than 20% of Bank of America customers.

People usually understand that the electronic banking conform with Internet banking, Mobile banking channel whereby bank account holder can register with their accounts and do transactions without any delayed nor disturbance of any factors. Individual bank customers can perform fund transfer within same bank or 3rd party bank, bill payments to 3 parties organization, cash in / cash out through ATM/CRM machines, Airtime top-up and credit card payments through all available electronic channels. As long as the electronic banking channel services surge with the fast pace, the concern on the stabilities of securities also up high parallel. In fact, it is very risky to expose the customer's information such as account information, account balance, transaction history, payment history available on bank channel via online. Therefore, bank are practicing the security guidelines, procedures and policies issued by well-known security organizations and associations in the world such as PCI Security Standards Council, etc.

More and more cyber crimes become more sophisticated, financial institutions (FIs) have to discover the best way to use time and money in an effort to mitigate the risk of fraudulent activity in their facilities. Bank should always aware what are the most recent security outbreak in other countries and plan ahead to prepare security fix that would cover for loop hole in bank system, internal discussion for standard operating procedures implementation, lab test, simulation test and explore more on the current trending. Bank should be more proactive in educating their consumer base, because Internet scams undermine the benefits of online commerce for everyone, regardless of whether that risk is directly related to a bank's actions or not. Bank should distribute the security awareness hand-out, handful information and do-and-don't things to its all bank staff effectively and efficiently.

This paper discover what are the best practice that AYA Bank is adhere to follow the standard guideline, policies and procedures for security risks, the way that AYA Bank prevent the potential frauds and abnormalities in their digital banking environment and then to explore and suggest the better ways in providing more secure and risk free approach in modern digital banking in the bank world.

1.2 Objectives of the Study

This study conduct with two objectives:

1) To identify current security practices in Digital banking operation of Ayeyarwady Bank and
2) To investigate mitigation process of the security risk in Ayeyarwady Bank Digital banking.

1.3 Scope and Methods of the Study

This study shows mitigating security risk factors in AYA Bank. This study used descriptive research method. In order to fulfil the study objective, both primary data and secondary data have collected. The primary data collected from 80 out of 140 AYA Bank's internal IT staff (57 % of total IT staff) with structured survey questionnaires. The secondary data was collected from various published sources as journals, articles, relevant text books, survey reports, previous research papers and website and so on.

1.4 Organization of the Study

This study include five chapters. The Chapter one describe the introductory chapter with rationale, objectives, scope and method, and the organization of the study. The Chapter two cover the theoretical background of security risks. The Chapter three present the profile of AYA Bank and it's digital banking and online services. The Chapter four focus the analysing of questionnaire data gathered from respondents. The Chapter five describe the conclusion of findings, suggestions and recommendation for further research.

CHAPTER 2

THEORETICAL BACKGROUND OF SECURITY RISKS

The internet has become an important means for users to complete business transactions. Information Technology (IT) systems aid in the advancement of banking operations, customer service, and stakeholder value. Financial institutions adopt IT innovations within operations to drive business efficiencies and increase profitability. Although IT services have a positive effect on businesses, IT services introduce data security and privacy issues in large corporations, banks and financial institutions. Depending on such technology brings security compromises that have become a global threat and produce unexpected financial losses. Business leaders have serious concerns as they work to respond creatively to new challenges and risks to ensure survival in this highly competitive environments.

Relying on technology drives a participatory democracy and cultivates organizational innovation, with a associated threat of digital piracy. The potential knowledge gained through this study could facilitate economic empowerment, expand awareness, and ensure the strong information security in organizations. The rapid changes of computing power and information technology continually initiate new risks expose to security of information assets. Such changes make the violation of information security easier, and in some cases, undetectable.

2.1 Concept of Security Risks

Understanding and analyzing the various risk factors to network security is of the utmost importance in information technology. Categorizing various risks, implementing control types, and identifying threat vectors are all concepts that information security experts must master to protect own networks against malicious threats from externals. Security policies establish guidelines and procedures for securing the valuable information against malicious threats and often involve encryptions for passwords and sensitive data, policies for configuring antivirus software and configuring firewalls. There are three main types of security control.

Technical Control Types can be thought of regarding controlling access in information system. This control type focuses on using technology and considers elements such as authenticating and controlling who has valid access, what type of access allowed in the system, as well as the specific resources that are allowed to be accessed. Moreover, technical control types emphasize how systems are securely protected, and how communications between systems are well protected. Some important elements of technical control are encryptions to protect the confidentiality of data, antivirus software, and firewalls.

Policies and procedures for securing physical or virtual networks are essential to management control types. It is not enough to simply install a firewall device in the existing networks. Information technology professionals must also understand the policies and procedures for correctly configuring firewalls. Thus, planning and assessment methods are used to manage and reduce security risks. This management control type deals with risk assessment procedures. Additional management control types involve vulnerability tests, which seeks to test for weaknesses in systems, and pen tests, which actively attempt to exploit vulnerabilities and give recommended remediation.

Operational control types make sure that the daily organizational operations fall in line with the organization's overall security plan. A significant difference between operational control types and technical control types is that operational control types are performed by internal staff of an organization on a day to day basis and not performed by technology. Some operational controls include network security training, planning for contingencies, and configurations and changes management training. Organizations and people that use computer system can describe their needs for information security and trust in systems in terms of three major requirements: *Confidentiality*: controlling who gets to read information; *Integrity*: assuring that information and programs are changed only in a specified and authorized manner; and *Availability*: assuring that authorized users have continued access to information and resources. These three requirements cab be emphasized differently in various applications.

2.2 Types of Security Risks

Most of the financial institutions are aware of the importance of information security. An Organizations security of the building, security for employees and financial security are all in high priority; however, company comprises many other assets that require security and its IT infrastructure. Every organization's network is the lifeline that employees rely on to do their jobs and subsequently make money and growth for the organization.

Therefore it’s important to recognize that IT infrastructure is a must that it require as top security. Common types of security risks are :

Data Exfiltration, it happens when there is unauthorized copying, transfer, or retrieval of data from either organization server or an individual’s computer. Organizations with high-value data are particularly at risk of these types of attacks, whether they are from outside threat actors or trusted insiders.

Third-party Service Providers (Vendor risk), as technology becomes more specialized and complex, organizations are relying more on vendors and outsources to support and maintain stable systems in it environment. Vendors or third-parties typically use remote access tools to connect to the organization's network, but do not always adhere security best practices and potential data breach incident may happen.

Risks from Viruses, program or code that replicates itself onto other files with which it comes in contact. Virus can infect another program, or a document that supports macros by inserting itself or attaching itself to that medium. Most viruses only replicate, although many can do damage to a organization computer or to the valuable data as well. Viruses generally require human action to propagate to another environments.

Bring own devices (BOD), data theft is at high vulnerability when employees are using own devices rather than organization's devices such as mobile, laptop, tablets, to share data, access organization information, or careless to change mobile passwords. Many enterprise organization has BYOD or BOD policy, they face risk exposure from those devices on the corporate network in the event an app installs malware or other Trojan software that can access the device's network connection and can get restricted information through those devices.

Network vulnerabilities, enterprise networks are getting ever-more complex, and it means the number of potential vulnerabilities within network is on the rise. Issues such as zero-day attacks, SQL injections and advanced persistent threats all seek to take advantage of weaknesses in code that can allow hackers to gain access to a network in order to plant malware, exfiltrate data or damage systems. One of the main ways hackers do this is by taking advantage of outdated and unpatched software.

Phishing attack, it is a type of information security threat that into breaking normal security practices and giving up confidential information, including names, addresses, login credentials, Social Security numbers, credit card information and other financial information. In most cases, hackers send out fake emails that look as if they're coming from legitimate sources, such as financial institutions, eBay, PayPal -- and even friends and colleagues. In phishing attacks, hackers attempt to get users to take some recommended action, such as clicking on links in emails that take them to fraudulent websites that ask for personal information or install malware on their devices. Opening attachments in emails can also install malware on users' devices that are designed to harvest sensitive information, send out emails to their contacts or provide remote access to their devices.

2.3 Causes of Security Risks

For large organization, data breach can be a disaster. The compromising of secure customer information and internal business data such as financial information, transaction history, and other privileged information is an event that no business wants to experience. Beyond the immediate financial impact of fraudulent order placements and bank transfers, the loss of customer faith can cripple a business' operations.

Organizations continue to develop a combination of technical, administrative, and physical controls to reduce information security risk. Administrative measures include the development of information security policies. The development of policies included outlines of the duties and responsibilities of the employee to safeguard the information technology resources of their organizations. Most security violations are a result of insiders using IT in an inappropriate manner. Employees using IT (Information Technology) inappropriately present a significant security threat to businesses and it can cause the reputation risk in the future. Information security policy provisions incorporate guidelines for employee reference, when interacting with IS (Information Security) to secure the data and technology resources of their employer. Unfortunately, there are documented cases of employee intentional and no intentional non-compliance with information security policies. Security experts concluded through documented cases that employees are the weakest link in information security defenses. Evidence suggests that a majority of information security incidents occur driven by trusted employees 'actions. However, popular media tends to headline the exploits of hackers or crackers.

Detecting insider threats is not straightforward task for security teams. The insider already has valid access to the organization's information system and assets and distinguishing between a user's normal activity and potentially malicious activity is a challenge. Insiders typically know where the sensitive data lives within the organization and often have elevated levels of access.

Cyber security often is synonymous with the term information security are not exact equivalents. Cyber security expands beyond the limits of information security to encompass other assets beyond information resources to include people as possible targets of cyber attacks. Additionally, cyber security includes people as unwitting participants in cyber attacks. Typically, information security only considers the human factor as it relates to their roles in the security process.

This additional measurement has moral ramifications for society in general since the assurance of certain susceptible groups could take shape as a societal responsibility. Criminal activities and security breaches often referred to as attacks do not only represent technological threats.

Economically developed societies are increasingly becoming information societies which are followed by rising security threats to information that negatively impact the core of these societies. Although no one disputes the importance of protecting cyberspace from criminal activities, our understanding of cybercrime and its consequences, both economic and social, is still limited.

The literature on cybercrime is huge but still theoretically thin and underdeveloped. Undeveloped literature exists because there are still many different perspectives on the topic, leading to a lack of consensus regarding many fundamental aspects of cyber crimes. As the internet becomes the essential tool for businesses, continued growth in e-commerce becomes a leader in the network economy. The expansion of cyber functionalities opens new opportunities for people to carry out online criminal activities. Unethical use of the internet has led to serious security concerns. The use of point of sale for business transactions becomes the primary information source for retailers.

The advantages of the internet come with risks, as people use the innovative tool as a medium for criminal objectives. Security risks of e-commerce transactions influence consumers, retailers, payment processors, banks, and card issuers. Retailers bear the cost for fraudulent, card-not-present (CNP) transactions, motivating them to reduce fraud in order to avoid damage to their reputation which impact revenue. Criminal activities often referred to as attacks, do not only represent technological threats but creates issues with individuals also.

Acceptance of modern economically developed societies continues to increase, transforming them into information societies. Security attacks on privacy and information threatens the core of these societies. Although no one disputes the importance of protecting cyber space from criminal activities, our understanding of cybercrime and its consequences, both economic and social, remains limited. The literature on cybercrime is vastly under developed because currently there are many different perspectives on the fundamental aspects of cyber crimes.

One of the major challenges faced by organizations is the response time to internet threats. Business leaders must act promptly while accurately predicting the period and severity of threats. The internet takes on a network capability that is a vital part of current business transactions. The internet has become an essential and indispensable means for users to complete relevant business. The network economy is born based on commerce. Referred to as e-commerce, such internet activity has expanded both foreign and domestic businesses. Networks and IS have inherent disadvantages such as the vulnerability to threats they present. These disadvantages make network security an important part of the country and national defense security and are a critical bottleneck, restricting the further development of the network economy. The influence of the internet enhances the popularity of computer network systems. Network security becomes more critical as security threats arise.

Security techniques, such as user authentication, data encryption, and firewalls, that used to improve security networks in banking system network; however, there are still many unsolved security problems. With limits placed on standard security techniques, researchers began to focus on building systems called intrusion detection systems (IDS). Detection of unexpected and emerging new threats have become a necessity for secured internet communication with absolute data confidentiality, integrity, and availability. To detect internet attacks in advance, the importance of intrusion forecasting in a network intrusion system is growing rapidly.

Advanced detection approaches from combining or integrating multiple learning techniques have shown better detection performance than general single learning techniques. Implementation of such detection systems proved to be not only accurate and fast, but also helpful for increasing effectiveness of the surrounding network. As technology continues to evolve rapidly, new security risks and challenges arise.

Companies and individuals are expanding consideration of cloud computing technology through marketing as a cost-effective method for small businesses to innovate. The concern regarding this shared environment directs attention to standards, regulations, and the capability consistent with technological evolution. The gap between the rapid technological evolution and the supporting standards and legislation regarding assurance, reliance, and information security. The distributed and open structure of cloud computing services becomes an attractive target for potential cyber attacks by intruders. Increased intrusion exists in part because IDS are largely inefficient for deployment in traditional cloud computing settings, as open structures in shared environments make it a lucrative target for cyber attacks.

The cyber security situation is worse than most people imagine. An accelerating pace of technological change causes the future to be more difficult to predict with each passing year. The lack of security of the internet and the devices connected to it results in serious vulnerabilities. Undeniable challenges exist, as internet dependence continues to increase. Concern about the security of computing systems has existed for over 40 years and that concern has intensified with the widespread global inter connectedness enabled by the Internet.

In the last 20 years, the proliferation of the internet brought about e-commerce, which lends itself to the coining of the term network economy. The Internet enters the market as an essential tool for many businesses both foreign and domestic. Given the world’s dependence on the network economy, the lack of inherent security present in network and IS makes for less than ideal market conditions for business. The result is a need for security at both a local and national level to mitigate security risks. While security is a major issue, at the same time, the need to remove barriers to the growth brought about by the network economy is relevant. Technology from web data mining provides the blending of both historical and new data technologies to increase security while propelling necessary market growth. Web data mining is an advanced technology that offers the possibility and feasibility of enhanced performance of network information security.

2.4 Loss Caused by Low Security Standards

Technology has played a significant role in changing the way human interact with each other. Most of financial institutions will increase internal efforts to innovate, with many businesses embracing the disruptive nature of FinTech. Losses resulting from identify fraud and fraudulent account takeovers have reached new peaks in recent years and it is not predictable. The general business problem is that technology dependence causes operational security risk, which results in financial losses. The specific business problem is that some small business leaders lack risk management strategies to prevent and mitigate operational security threats, producing unpredictable financial losses.

When a personal data breach occurs in an organization, the cost and consequences can be severe. The organization is required to notify the regulatory authorities rapidly. Organization need to make a public announcement, and to notify each individual affected.

Some regulations require a written communication to every person. The organization may need to handle large numbers of enquires from concerned people who want to know if they have been affected. Individuals who have had their personal data compromised are entitled to credit monitoring services for a period of time in case they suffer identity theft. Those who suffer loss will require being compensated. Some may elect to bring a lawsuit against the company. Regulators typically impose fines on the company for its failure in the duty of trust. The organization also face internal costs from dealing with the breach, including a forensic investigation to identify any IT system vulnerability that was the cause of the breach, installation of higher levels of security, and disruption to its business practice while it deals with the immediate aftermath of the event. These direct costs can be significant. The type of data stolen is important: for a breach of 10,000 records, it will cost a company 1.5 times as much for PCI records than for personally identifiable information (PII), and 5.5 times as much for protected health information (PHI) records (solving the cyber risk, Andrew Coburn).

Others factors increasing the costs of a data breach may include delays in discovering or announcing the event, high losses being suffered by the victims, poor media management, and litigation costs. The average cost per record of a data loss of more than 100,000 records more than doubled from 2010 to 2016. This reflects increasing regulatory fines and procedures, growing costs of compensation, and escalation of legal complexities in dealing with identity loss. The reputational damage causes customer desertion, revenue dip, market share is lost, executives resign, share price fall and suppliers and counterparties suffer in turn. Credit ratings are downgraded and the viability of a company can be threatened. The impact of experiencing a data breach can go far beyond the direct costs, and can impact the brand, the reputation, and the viability of the organization itself.

2.5 Security Risks Mitigation

Prevention is sometimes included with risk mitigation, which involves actively taking steps to reduce the level of risk. Implementing layers of security on a network is one part of risk mitigations, but it can also include cyber security training for users. Anything that reduces risk can be referred to as risk mitigation. Information security is a major concern of risk management for business leaders in financial institutions. Due to the frequency of changes in system environments, and information technology in general, new risks are always inherent to information security assets. These risks potentially make it easier to compromise the security of information assets of customers and such compromises may even go unnoticed. Security solutions based on the technical aspect alone are not sufficient to protect operational information of businesses.

Financial institutions and banks must develop their capabilities to respond to and mitigate risks. Developed capabilities are a strategic strength in highly competitive areas, as well as essential to the permanence of the organization. While organizations have developed, implemented, and enhanced security controls over time to time, the current information security controls and practices may not be sufficient to protect organizations because security must take into account people as a potential threat, in addition to technical security.

As businesses provide employees with access to IS and the frequency and sophistication of security threats grows, the need to provide security assumes greater importance. Successful information security is dependent on the behavior of the employee, or user, while operating the backend system of the bank. User satisfaction is widely used to measure the success of Information System. Studies by Montesdioca and Maçada (2015) indicated that the achievement of a strong information security presents itself through a combination of technical and socio-organizational investments that considers the user as an active agent. User satisfaction is one of the most relevant variables to assess the success of IS. The user satisfaction variable in conjunction with the information system is important because it suggests business leaders are investing in the decision-making process of the user.

Security risk mitigation can alleviate by decreasing the threat level by eliminating or intercepting the adversary before they attack, blocking opportunities through enhanced security, or reducing the consequences if an attack should occur. Without question, the best strategy for mitigating risk is a combination of all three elements, decreasing threats, blocking opportunities and reducing consequences. Logically, risk mitigation strategy ties assets to threats to vulnerabilities to identify risks. Solutions for the identified risks typically enhance three facets of security: Policies, Procedures and Training; Physical or electronic security systems and security personnel. A statement from TAG(Threat Analysis Group, LLC) security consulting firm, a sound mitigation strategy maximizes existing security resources and prioritizes as policies first, systems second, and personnel third.

Pen testing is commonly used to address the problem of cyber risk mitigation, instead of more empirical and scientific practices. Although pen testers know what to charge for their professional services, most pen testers cannot put a price on their success or failure. Pen testers can make recommendations, remediation on how to close the security gaps with those are on high security risks, and how to prioritize the necessary tasks. But no two pen testers go about their assignment in the same way, and pen testing is usually done on a limited set of targets.

Accordingly, pen testing is not strictly a risk management exercise. To provide another perspective on security risk management, consider the pen testing analog of red-teaming in counterterrorism studies. Red teaming exercise are particularly valuable in identifying gaps in security that would make a location or event a comparatively soft target relative to other alternative targets. By hardening any one potential target, e.g., deploying additional perimeter security guards and installing CCTV, the risk may be transferred to another soft target. This tactic should extend to cyber risk as well. Hackers follow the path of least resistance in their targeting, and if an attractive designated target for a cyber attack has been hardened, others lacking the benefit of pen testing or red-teaming knowledge may become more likely to be attacked.

The risk mitigation strategy should be both proactive with the aims of preventing or reducing security incidents and reactive with detect and investigate security breaches in order to contain, minimize the damage, and/or recover and restore services and data. Doing a structured security risk assessment helps in building such a picture of a security architecture that is related to the existing risks. Based on that, a portfolio of organizational and technical actions can be defined in which the selected technologies work together to build a layered security infrastructure. Behavioral anomalies help security teams identify when a user has become a malicious insider or if their credentials have been compromised by an external attacker. Assigning risk scores also gives security operations center (SOC) teams the ability to monitor risk across the enterprise whether it be creating watch lists or highlighting the top risky users in their organization. By adopting a user-focused view, security teams can quickly spot insider threat activity and manage user risk from a centralized location instead of manually piecing disparate data points that individually may not show the full picture.

The setting of security policy is a basic responsibility of management within an organization. Management has a duty to preserve and protect assets and to maintain the quality of service. It must assure that operations are carried out prudently in the face of realistic risks arising from credible threats. This duty may be fulfilled by defining high-level security policies and then translating these policies into specific standards and procedures for selecting and nurturing personnel, for checking and auditing operations, for establishing contingency plans, and so on. Through these actions, management may prevent, detect, and recover from loss and mitigation can be affective.

2.6 Governance of Information Security

The process of establishing and maintaining a framework and supporting management structure and processes to provide assurance that information security strategies are aligned with and support business objectives, are consistent with applicable laws and regulations through adherence to policies and internal controls, and provide assignment of responsibility, all in an effort to manage and mitigate the risks.

The supervision and making of decisions necessary to achieve business objectives through the protection of the organization's information assets. Management of information security is expressed through the formulation and use of information security policies, procedures and guidelines, which are then applied throughout the organization by all individuals associated with the organization.

Von Solms (Von Solms and Von Solms (2004) published the 10 Deadly Sins of information Security Management) suggested that management use the 10 points as a checklist to ensure the introduction of a comprehensive plan is defined. If not taken into account while developing a governance plan, could cause the plan to fail, or at the least, cause serious flaws in the plan. Not realizing that information security is a corporate governance responsibility. Not realizing that information security is a business issue and not a technical issue. Not realizing the fact that information security governance is a multi dimensional discipline. Not realizing that identified risks are the foundation for an information security plan. Not realizing and leveraging the important role of international best practices for information security management. Not realizing that a corporate information security policy is absolutely essential. Not realizing that information security compliance enforcement and monitoring is absolutely essential. Not realizing that a proper information security governance structure of organization is absolutely importance. Not realizing the core importance of information security awareness among the users. Not empowering information security managers with the infrastructure, tools, and supporting mechanisms to properly perform their responsibilities.

Addressing all ten issues could be useful for implementing or evaluating an existing information security plan in a business like Financial institutions and banks that seems to be having problems in being effective.

The growing emergence of security threats call to be integrated into the organization’s corporate governance, and treated as high importance, as other critical corporate governance area by executive management. While senior level management have leading roles, the findings point to other significant actors such as outsourcing partners and lower level management.

A concept to enforce information security derived from corporate accountability and information governance attempts to make corporate level executives aware of their responsibility in the protection of data. Information security is an integral feature of information governance. Business leaders at the strategic level establish strong alignment between the business and information security with the aim of ensuring that security delivers business value through appropriate policies of risk management, resource management, and performance measurement. Business leaders must improve strategic alignment attributes in order to attain effective information security governance.

The foundational understanding of information security governance and the effectiveness governance based on: (a) the commitment of the organization’s stakeholders with the purpose of aligning key stakeholder’s interest with business objectives, (b) availability of resources with the aim of strategically manage resources and competencies to achieve organizational goals, and (c) the responsibility and accountability of the agents to ensure that performance through monitoring and measurement is efficient and effectively monitored in order to minimize risks.

Internal security incident reports and global vulnerability reports from various sources help define the threat and level of risk that the organization faces in protecting its information assets. The numerous standards and best practices documents provide guidance on managing risk. User feedback comes from both internal users and external users who have access to the organization’s information assets. This feedback helps improve the effectiveness of policies, procedures, and technical mechanisms. Depending on the organization and its cyber security approach, each of the three factors plays a role to a greater or lesser extent at each level.

Staff negligence or ignorance of information security policies are the cause of many of the recent security breaches. Such negligence results from significant financial losses for businesses. Business leaders strive to implement influential policies and procedures to improve information security. The impact of policies and procedures bare close examination as compliance with information security continues to be problematic for business leaders.

The internet and information technology continue to have an enormous influence on human life. Information security continues to be a decisive concern for both users and organizations. Technology cannot solely guarantee a secure environment for information. In addition to technology, the human factor of information security must be considered. The lack of information security awareness, ignorance, negligence, apathy, mischief, and resistance are the root of user mistakes. Compliance with information security policies creates procedures that aid in risk mitigation of staffs' behavior. Information security culture engages the identifications of security-related ideas, beliefs, and values of the business.

Information security knowledge sharing, collaboration, intervention, and experience all have a significant effect on staffs' attitude towards compliance with organizational information security policies. The presence of business leader commitment and personal norms affect staff attitudes. Employee attitude towards compliance with information security organizational policies also have a significant effect on the behavioral intention regarding information security compliance. Internal auditors and information security management play important roles in protecting an organization's assets. The two groups are not always supportive of one another. There are definite benefits of the two groups working together. One of the key activities for data loss prevention is an audit. Roratto and Dotto added the importance of having reliable records of activities in order to be able to audit a system. Systems store critical data, whether financial or operational and must have features such as audit log, also called audit trail, which records all activities on data. Recording critical data activity enables the identity of harmful actions that can be internal or external, intentionally or unintentionally caused.

The level of technical expertise possessed by internal auditors and the extent of the internal audit review of information security relate to information's security assessment. The quality of the relationship between the internal audit and information security functions is positively associated with perceptions of the value provided by internal audit and, most important, with measures of overall effectiveness of the organization's information security endeavors. Therefore, special care must occur to protect the integrity of sensitive data adequately. The use of an audit log, also called audit trail, records all activities on critical data which allows for the identity of harmful actions that can be internal, external, intentionally, or unintentionally caused.

2.7 Theory Reference of Other Studies

In the figure (2.1), it illustrates the risk management cycle of IT system and the main activities to handle the security risks. The cycle contain four phases (a) Identification, (b) Quantification, (c) Controlling and (d) Monitoring.

(a) Identification, within the scope of the identification phase, the security risks are identified and classified. Security in ICT covers the wide range from the physical protection of the hardware to the protection of personal data against deliberate attacks. In an open information system like the Internet, one cannot assume, that all parties involved trust or even know each other. Therefore, the analysis of security risks requires not only the observation of external attackers but also the inclusion of all parties involved as potential attackers. The concept of multilateral security considers the security requirements of all parties involved. The security risks result from the threat of the so-called four protection goals of multilateral security as confidentiality, integrity, accountability and availability.

(b) Quantification, the identified security risks are measured by the use of different methods within the quantification phase. No quantification model has been developed for the measurement of the security risks, defined above. For the measurement of this subset of operational risk the Basel Committee on Banking Supervision (2004 Basel Committee on Banking Supervision) suggests five different quantification methods in order to determine the economical capital charge. The methods reach from simple, actor-based approaches to complex stochastic loss distribution models based on the Value-at-Risk (2004 Basel Committee on Banking Supervision). Beyond that, further methods exist for the quantification of operational risks, as for instance questioning techniques or causal methods.

Controlling, based on the identified and quantified operational risks, decisions on carrying, decreasing, avoidance as well as the transfer of the security risks are made within the controlling phase. There are internal and external controlling instruments for operational risks. The model aims to solve the described trade-off between the expected losses and the opportunity costs of the economical capital charge on the one hand and the investments in security mechanisms and insurance policies on the other. Thereby, the amount to be invested in security mechanisms and insurance policies will be optimized.

(d) Monitoring, The monitoring phase encompasses all procedures and techniques, which are necessary for a continuous monitoring of operational risk. Thereby it is analyzed, if all the occurred events have been prior identified as possible events, the distribution of probabilities of occurrence of events and the distribution of severities of losses have been anticipated within the quantification phase, the selected controlling measures have lead to the desired results.

Figure (2.1) Theory Reference of Risk Management Cycle

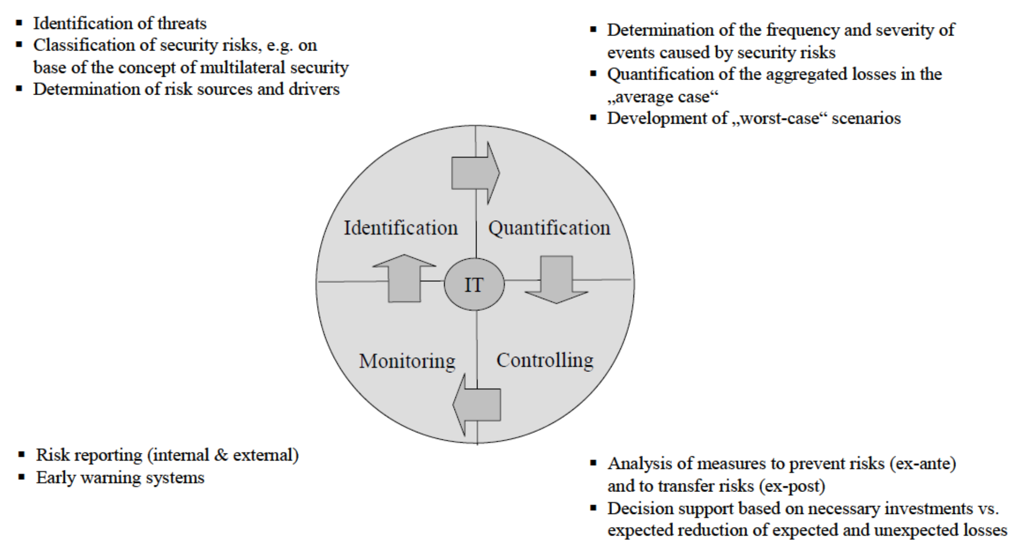

▪ Identification of threats
▪ Classification of security risks, e.g. on base of the concept of multilateral security
▪ Determination of risk sources and drivers
▪ Determination of the frequency and severity of events caused by security risks
▪ Quantification of the aggregated losses in the „average case"
▪ Development of „worst-case" scenarios
Identification
Quantification
IT
Monitoring
Controlling
▪ Risk reporting (internal & external)
▪ Early warning systems
▪ Analysis of measures to prevent risks (ex-ante) and to transfer risks (ex-post)
▪ Decision support based on necessary investments vs. expected reduction of expected and unexpected losses

Fig. 1. The risk management cycle

Source : Ulrich Faisst & Oliver Prokein - Management of Security Risks - A controlling model for banking companies

Taking the reference factors from Figure (2.1) , Four main processes (a) Planning (b) Identification, (c) Controlling and Measurement and (d) Monitoring, are practicing in AYA Bank IT department to serve the digital banking services to customers.

Planning process describe how AYA Bank engage with security experts to conduct the Pen tests, vulnerability assessments to mitigate the potential security threats.

Identification process describe how AYA Bank identify the weakness of their system, find the security loop holes so that security team can handle and fix the weak points in the system. This can evaluate hard facts relating to impacts and frequency of events that are difficult to come by. Having identified the impacts for each threat, AYA Bank need to assess the likelihood or probability of each occurring.

Controlling and measurement process illustrate that after low level of security standards figure out in digital banking services, AYA bank need to implement the action plan to patch the environment, update the systems, get the resolution from vendors to fix the issues. This process also prevent the vendor risks that may interrupt the bank services.

Monitoring process describe that AYA Bank has established Network Operation Centre (NOC) facilities to watch and monitor the security threats, attacks and other abnormalities in the digital banking services. NOC gather information through automated or manual means, alerting or reporting on information relevant to intended purposes for risk monitoring, and providing inputs to ongoing risk assessment and response processes.

CHAPTER 3

HISTORY OF AYEYARWADY BANK

On 2 July 2010, the Central Bank of Myanmar issue banking license to AYEYARWADY Bank and allow to operate banking services in Myanmar. Upon receiving banking license, AYEYARWADY Bank started operations on 11 August 2010 at Naypyitaw HO branch. According to Financial Institutions Law 2016, AYEYARWADY bank relicensed as a full service universal bank. Across the years, the bank will continue to expend its branch network capabilities throughout Myanmar while concurrently investing in state-of-the-art Core Banking system, Fintech and Digital Banking platforms as well as human resources. AYA Bank mission is to provide uniform Omni-channel interface offering innovative products and services across all customer levels.

3.1 Vision and Mission of AYA Bank

AYA Bank continue to extend its branch network throughout Myanmar. Bank continue to focus on providing excellent customer service, building relationship with customers and leverage on technology as the enabler to enhance its customer's base. AYA Bank aims to strengthen its governance, risk and compliance structure as a measure to ensure balance and to sustain growth.

To be recognized as the leading bank in Myanmar through pursuit of excellent and long term sustainable growth for the bank and its stakeholders. AYA Bank is the bank of choice for anyone who is looking for fast, reliable, honest banking relationships at reasonable cost. AYA Bank offers the full range of retail and commercial banking products and services and is in tune with domestic customs and international standards in its governance and operations.

AYA Bank seeks highly-motivated individuals who share our passion for growth and success; and who would like to make a difference. AYA promote a learning culture within the organization and engage in excellent learning opportunities, reward high performers and provide our employees with career mobility opportunities across our different business units.

3.2 AYA Bank Branch Networks

AYA Bank has opened 258 branches in Myanmar as of December 2019. There are 110 branches in Yangon region, 27 branches in Mandalay region, 11 branches in Naypyitaw, 11 branches in rest of lower Myanmar and 99 branches in rest of upper Myanmar. All the branches are using the centralized core banking system to serve the banking services to customers.

3.3 Products and Services of AYA Bank

AYA Bank is giving the nine main types of products to its customers. Products are deposit, loan and advances, remittances, cash management, card payment, eBanking, trade product, AYA rolay banking and safe deposit box products. Well known services are education loan, home loan, auto loan, SWIFT telegraph transfer, Western Union money remittance, debit card, credit card, POS and foreign exchange services.

As a first step of Digital banking service, AYA iBanking Service has published to AYA Bank customers on 27-Jun-2014 for customers to manage their financial transactions over the internet. on 16-Jan-2015, AYA Bank released mBanking mobile application for managing customers money at AYA Bank from anytime, anywhere. Customers can manage their accounts, credit cards, transfer money, pay bills at ease with a few simple steps. By then, AYA Bank digital banking customers count has been improving to 580,000 users as of December 2019.

AYA Bank published new version of mBanking 2.0 on 28 Oct 2019 with new features such as *Request Money*: Customers request money from other AYA account holder by sending a QR code of his/her bank account and ask payee to simply scan and pay

Fast Pay (Billing Organization): Customers can make payment by easier and faster way via AYA mBanking less than normal transfer steps.

Scan QR & Pay:For Easy Payments, QR allows a simple scan of Codes for every transactions

ATM Withdrawal: Customers can withdrawal money at any AYA ATM without card in hand by initiating ATM Withdrawal straight from AYA mBanking app

Foreign Exchange Transfer: Customers can transfer to other AYA USD accounts or own USD accounts followed by the exchange rate of transfer time

Biometric Login: Convenience and secure by biometric login, Verified by customer finger print or face ID provided by device by setting up at your phone setting and enable at the AYA Mobile Banking app

Push Notification: Customer will receive notifications for adding payee list and every financial transactions of customer account

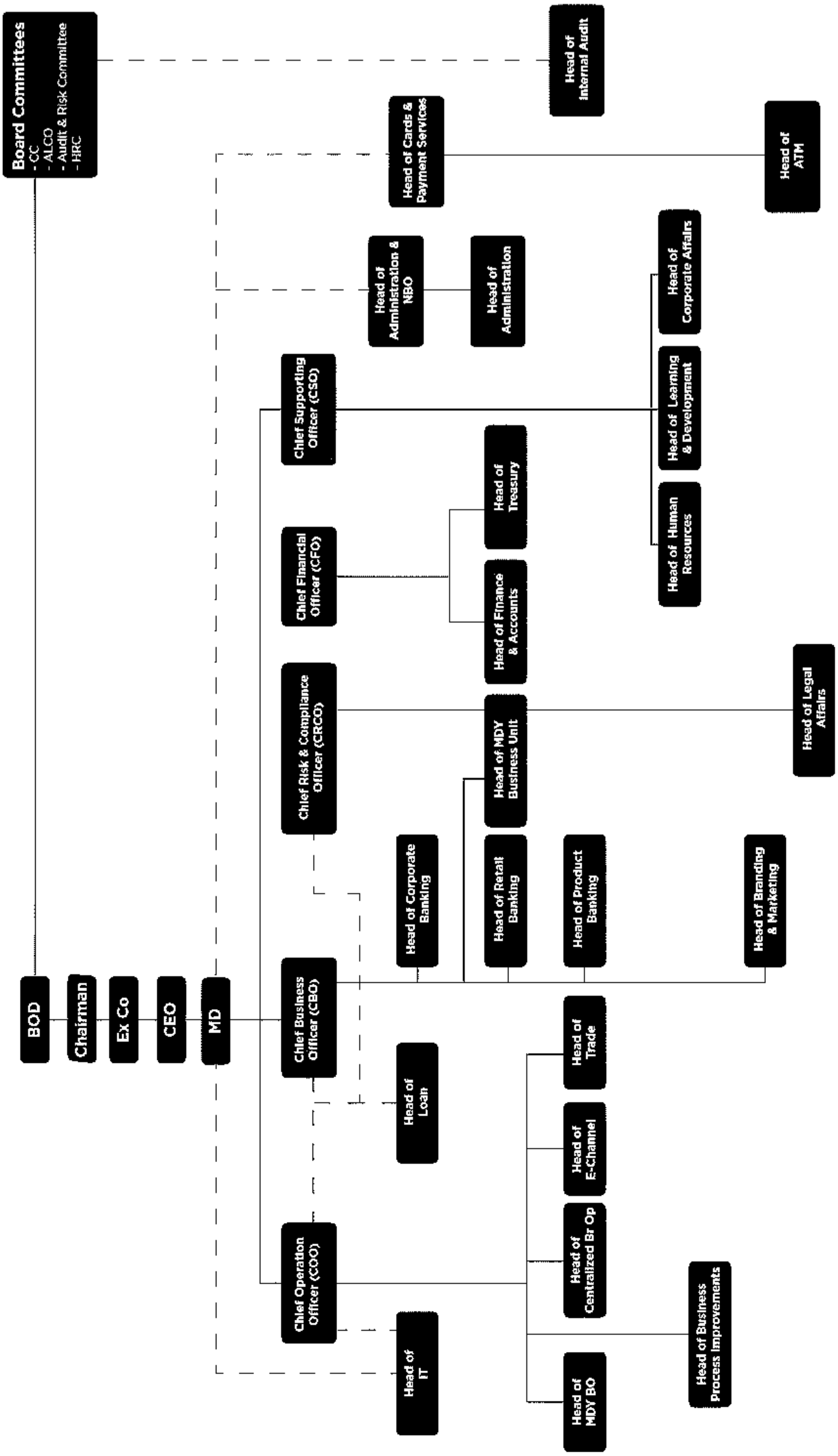
AYA Bank published another Fintech application, AYA Pay (e-Wallet), on 16th Dec 2019 to Google play and App store. This subscriber app is designed to bring convenience payments and money transfers into customers everyday life.

Feature of AYA Pay application such as Top up mobile phone with 5 Telco: MPT, Mytel, Ooredoo, Telenor, Mec-Tel, Cash in your Wallet at Agents or by verified AYA Bank account, Cash-out money at Agents or at ATMs, Simply transfer money to Wallets, to Unwallet by OTP/NRIC or request transfer to receive money, Easy bills payment at any time with 3 billers: Steam, Ananda, Canal+, Quick payment in Merchant stores by scanning QR code or accepting the payment request, Conveniently move money between Agent's Wallet and linked AYA Bank account, Transaction management review wallet balance, all transactions history over time and receive transaction notifications.

3.4 AYA Bank Organization Structure

The organization structure of AYA bank consists of people department, administration department, finance department, core banking department, corporate banking department, treasury department, credit department, international banking department, digital banking department, marketing department, PMO department, banking operation department, information and technology department, strategic and planning department and risk management department. Board of Directors decide the strategic decisions and spread out strategic plans to respective departments. Figure (3.1) illustrate the organization chart of AYA Bank.

Figure (3.1) AYA Bank Organization Chart

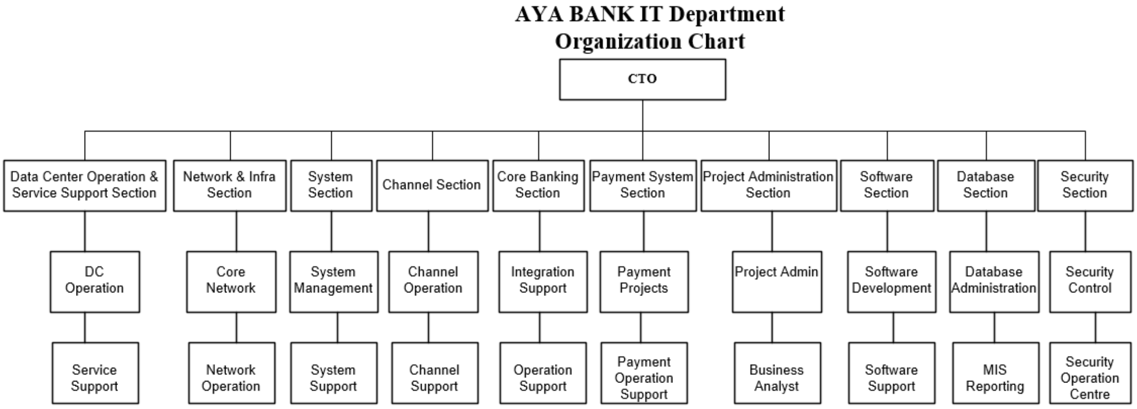

Board Committees
- CC
- ALCO
- Audit & Risk Committee
- HRC
Head of Internal Audit
Head of Cards & Payment Services
Head of ATM
Head of Administration & NBO
Head of Administration
Head of Corporate Affairs
Head of Learning & Development
Head of Human Resources
Chief Supporting Officer (CSO)
Chief Financial Officer (CFO)
Head of Treasury
Head of Finance & Accounts
Chief Risk & Compliance Officer (CRCO)
Head of MDY Business Unit
Head of Legal Affairs
Head of Corporate Banking
Head of Retail Banking
Head of Product Banking
Head of Branding & Marketing
BOD
Chairman
Ex Co
CEO
MD
Chief Business Officer (CBO)
Head of Loan
Head of Trade
Head of E-Channel
Head of Centralized Br Op
Head of Business Process Improvements
Chief Operation Officer (COO)
Head of IT
Head of MDY BO

Source: AYA Bank Financial Statement (2016-2017)

3.5 AYA Bank IT Department Organization Structure

AYA Bank IT department has 140 IT staff as of 2019 December. There are ten sections established in IT department such as Data Center Operation & Service Support Section, Network & Infrastructure Section, System Section, Channel Support Section, Core Banking Support Section, Payment System Section, Project Administration Section, Software Section, Database Section and Security Sections. Chief Technology Officer (CTO) is the executive in charge of the IT department and oversee across ten sections. CTO develops policies, procedures and guidelines and uses latest technology to enhance products and services that focus on external or internal customers. CTO also develops IT strategies in the way of using technology to increase revenue of the bank and performs a cost-benefit analysis and return-on-investment analysis. CTO oversee the bank's data, security, maintenance and the infrastructure network, and implement the bank's technical strategy. CTO also manage the bank's high-level technological roadmap.

Figure (3.2) AYA Bank IT Department Organization Chart



Source: AYA Bank

3.6 Functions, Roles and Responsibilities of AYA Bank IT Department

IT department is one of the important department to drive the business strategies of the bank to have affective and efficient. Therefore, IT department is responsible for providing the infrastructure for this automation long term. IT department implement the governance for the use of network and operating systems within the bank environment and across all the branches, the IT department enables the company’s employees to communicate, collaborate and automate routine tasks, and generally provide operation teams with the ease of use functionality and abilities through the systems they need to perform their duties. It's important to take note that although the IT department implements, operate and facilitates the flow of information in bank, it does not create the policy that defines which information is correct or accessible to others. Usually ownership of the information and access comes from respective departments. IT department do not have rights to amend, edit or deletion of any customer information in the bank systems without approval from bank management, however represent as a facilitator or supporting unit instead.

There are four major IT functions in AYA Bank IT department such as IT Governance, IT infrastructure, Functionality and IT system security. IT Governance: refers to the implementation of operational parameters for working operation units and individuals' use of IT systems, architecture, solutions and networks. Governance enact the rules about how AYA employee can use the bank technology and what to use it for. This part make sure the conventional IT security as well as the data assurances and data privacy. IT Infrastructure: This function refers to the hardware components used in bank environment, the network, the circuitry and all other equipment necessary to make an IT system functioning properly in the daily bank operations to serve the bank customers in digital banking services and core related services. Functionality: This part is the most obvious task performed by the IT department within organization, and therefore functional tasks are most commonly associated with in many employee's mind. It refers to creating and maintaining operational applications; developing, securing, and storing electronic data that belongs to the bank and assisting in the use of software and data management to all functional areas of the bank. IT department provides technical support service for all the bank users who has rights to access bank systems. IT System Security: This function covers the data security, data privacy and overall hardware, software securities in bank IT system platform. IT System Security: This function covers the data security, data privacy and overall hardware, software securities in bank IT system platform. This portion assess security plans for existing system vulnerabilities, security strategies prioritizations to cover strategically important data, analyze reports generated by automated threat monitoring systems and run testing for anticipation of future issues to pop up.

AYA Bank IT department take the responsibilities of the core systems to have smooth and stable operation day by day as all of the branch networks and back office systems are using the centralized core system platform. Bank IT has 24/7 schedule rotation assignment to NOC (Network Operation Center) team to watch and monitor the back office services and digital banking services. NOC team monitor the services and convey the system status to respective sections if there is incident, issues or problems in core services and digital banking services. Respective sections then take ownership of the incident, issues or problems for next necessary actions to support the issues, to identify the incidents why it is happened and figure out what are the mitigation plans and prevention plans to fix the incidents with subsequent remediation. Solutions to fix the issues and problems, risk mitigation plans, technical support plans route to CTO from responsible section heads to seek the approval to proceed action plan. Upon the approval, respective section head take the lead and manage the staff resources to perform the necessary actions.

Detail action plans are then share and circulate to each of the sections within IT department to collaborate during the implementation. Clarifications, questions, negotiations and technical suggestions are taken into account as all the responsible IT sections are involved in this steps. After getting the clear check lists, detail steps and post activity monitoring process checklist, AYA Bank IT start taking the action activity and keep CTO informed status. The same information spread to other departments to keep everyone in bank are on same page. As per post activity monitoring procedures, NOC team then watch and monitor the bank transactions, stabilities of the core systems in back end. If there is abnormalities found, the NOC team then route the status to responsible sections depending on the severity level of the abnormalities.

3.7 Security Risks Mitigation Practices in AYA Bank

All the security risk assessments, security issues in bank system, privacy and confidentiality of the data are handled by AYA bank IT security section. There are two main group in security section, security control group and security operation group. Security control group under the security sections play the essential role in IT organization. Typical duties represent as maintaining and creating information security policies and procedures for AYA Bank, researching the new technologies and their impacts, documenting the checklist and guidelines for bank users, enabling new policies and implementing new information security technologies, conducting security training programs and security awareness program for external and internal users, and communicate information security goals and new programs effectively with other department within the bank organization.

Security control group from security section usually engage with external security experts to initiate the security risk assessments to find out the possibilities of risk level and their impact, review the risk assessments scope of work given by third party experts. Then, security control group start the assessment action together with external parties to find out system weakness, severity level of the security risks and find the solutions to prevent or to lower down the severity level.

Security control team then define the necessary security policy, procedures and guideline. Subsequently, security operation group follow up and enforce the guideline in bank environment. Security control team regularly check the internal systems whether sensitive data of customer information are stored in backend system in encrypted format so that customer information are not easily readable by human beings. If the team found lack of using the protection methods such as encryption, hashing or data masking not being used in bank system to protect the customer data, Security control team enforce the respective sections to follow the best practice guidelines to put in place the data protection mechanism as immediate remediation. Bank IT department usually deal with the external auditors to conduct the Information Technology General Control (ITGC) every year to ensure the proper development of applications, implementations, as well as the integrity of programs, data files, and computer operations. ITGC scope cover the logical access controls over application systems, customer data and infrastructures.

Security Operation Center (SOC) team regularly monitor and investigate suspicious activities through automated monitoring tools such as Security Information and Event Management (SIEM). SOC team detect threats, investigate those threats and respond to them in a timely fashion. SOC team receive and analyze alerts receiving from the SIEM, which may contain signs of compromise and related threat intelligence. The team performs triage on the alerts, understands the extent of the threat and responds SOC is working 24/7 and multiple shifts and managing the workflow handoff seamlessly and prudently. SOC team SOC team receiving and analyzing alerts from the SIEM, which may contain signs of compromise and related threat intelligence. The team performs triage on the alerts, understands the extent of the threat and responds. A member of SOC is regularly responsible for auditing systems to meet compliance requirements for central bank regulations and industry regulations. Efficient access to threat information, patch levels, identity and access control data is essential for compliance. Findings and reports from SOC usually goes to CTO of AYA Bank for further IT security strategies and policies.

Chapter 4

ANALYSIS OF SECURITY RISKS PRACTICES AND MITIGATING PRACTICES IN AYA BANK

In this chapter shows presentation of results and findings obtained from the respondents of AYA Bank IT staff. There are 5 sessions in this chapter. The first session represent the demographic characteristic of respondents. Second session focus the analysis in the way of AYA Bank practicing on planning and engaging with security experts for Digital Banking Services. Third session represent the current situation of security weakness and identify them in AYA Bank Digital banking services. Fourth session analyze what are the controlling procedures and measurement practices in AYA Bank Digital banking platform. Last part of the session emphasize the monitoring process used in AYA Bank.

4.1 Research Design

A primary survey data were circulated to AYA Bank IT staffs, targeting 120 of bank IT staff, who are currently working at AYA Bank. Out of 120 targeted AYA Bank Staff, total 108 staff were respondent survey accordingly. The questionnaires were visualized by identifying the variables based on theory reviews. Multi sessions structured questionnaire was designed to collect the primary data from the respondents. Sampling method was used in research design. Reason being used sampling method is that this is fastest, affective and efficient to collect the required information from various respondents. The questionnaire collect the respondent profiles, ease of using online system, technical stack of the AYA Digital banking systems, security level of the system, planning, controlling, maintain and monitoring the quality of service provided by AYA Bank. Likert’s 5-point scale was used for respondents to rate their opinion ranging from skill set of 1,2,3,4,5 as strongly disagree, disagree, neutral, agree and strongly agree respectively. Google form platform was used to distribute and collect the questionnaire to and fro respondents.

4.2 Demographic profile of Respondents

In demographic session, surveyed characteristics are gender, age group, education, occupation, monthly earning and frequency of usage on AYA Bank digital banking services.

(a) Genders of Respondents

Gender classification is the first analysis of the demographic upon responses. Total 108 respondents are shown in Table (4.1). The result from survey showed that there were 63 males and 45 females.

Table (4.1) Genders of Respondents

Gender	No of respondents	Percentage(%)
Male	63	58.3
Female	45	41.7
Total	108	100

Source: Survey data (2019)-Mitigating security risks of digital banking in AYA Bank

(b) Age of Respondents

Another demographic analysis was age group of the respondents. The result from total 100 respondents shown in Table (4.2). The table figures shows that the largest group is 21-30 years of age with 40.7 % of the total respondents. Second major group is 31-40 years old with 39.8 % of total respondents and followed by 41-50 years group is 13%, under 21 years is 4.6% and above 50 years group is 1.9%.

Table (4.2) Age of Respondents

Age	No of respondents	Percentage(%)
Under 21 years	5	4.6
21 to 30 years	44	40.7
31 to 40 years	43	39.8
41 to 50 years	14	13
Above 50 years	2	1.9
Total	108	100

Source: Survey data (2019)-Mitigating security risks of digital banking in AYA Bank

(c) Education level of respondents

Another demographic analysis was education level of the respondents. The result from total 108 respondents shown in Table (4.3). The table figures shows that the graduate level are largest group with 72.2% of the total respondents. Second major group is master level with 23.1% of total respondents and followed by under graduate group with 4.6%. It is observed that there is no doctorate level staff information are not available.

Table (4.3) Education Level of Respondents

Education level	No of respondents	Percentage(%)
Doctorate	-	-
Master	25	23.1
Graduate	78	72.2
Under graduate	5	4.6
Total	108	100

Source: Survey data (2019)-Mitigating security risks of digital banking in AYA Bank

(d) Occupation of respondents

Another demographic analysis was occupation statistics of the respondents. The result from total 108 respondents shown in Table (4.4). The table figures shows that the first 3 group of respondents occupation are IT professional, IT support, bankers and their percentages are 30.6%, 13.9% and 13.9% respectively.

Table (4.4) Occupation of Respondents

Occupation	No of respondents	Percentage(%)
Banker	15	13.9
Consultant	2	1.9
Credit Risk Officer	1	0.9
Executive	11	10.2
HR	7	6.5
Internship	5	4.6
IT Professional	33	30.6
IT Support	15	13.9
IT Technician	13	12
Others	6	5.6
Total	108	100

Source: Survey data (2019)-Mitigating security risks of digital banking in AYA Bank

(e) Monthly Income of Respondents

Another demographic analysis was income level statistics of the respondents. The result from total 108 respondents shown in Table (4.5). The table figures shows that the first 3 group of income levels are 500,000 – 1 million, 200,000 – 500,000 ,1 million – 2 millions, and their percentages are 34.3%, 28.7% and 21.3%% respectively.

Table (4.5) Income Level of Respondents

Monthly Income Level (MMK)	No. of respondents	Percentage(%)
Less than 200, 000	5	4.6
200, 001 – 500, 000	31	28.7
500, 001 – 1,000, 000	37	34.3
1,000,001 – 2,000,000	23	21.3
Above 2,000,000	12	11.1
Total	108	100

Source: Survey data (2019)-Mitigating security risks of digital banking in AYA Bank

(f) Marital Status of Respondents

In the demographic profile survey, the respondents were required to provide their marital status. Table (4.6) represent the result of respondents' marital status analysis. 58.3% of the respondents are single and 41.7% of the respondents are married.

Table (4.6) Marital Status of Respondents

Marital Status	No of respondents	Percentage(%)
Single	63	58.3
Married	45	41.7
Total	108	100

Source; Survey data (2019)-Mitigating security risks of digital banking in AYA Bank

(g) Working experiences in AYA Bank

Table (4.7) Working Experiences in AYA Bank

Experience in AYA Bank	No of respondents	Percentage(%)
Less than 6 months	6	5.6%
6 months – 1 year	11	10.2%

1 year – 1 year 6 months	7	6.5
1 year 6 months – 2 years	21	19.4
Above 2 years	63	58.3
Total	108	100

Source: Survey data (2019)-Mitigating security risks of digital banking in AYA Bank

Table (4.7) states the analysis of the working experience status of respondents with AYA Bank. According to survey data, 58.3 % of the respondents are the largest group with 63 respondents who has been working in AYA Bank more than 2 years. 19.4% of the respondents have been working in AYA Bank 1 year and 6 months. 10.2% of survey respondents are having 6 months to 1 years services each.

(h) Monthly Frequent Usage on AYA Bank Digital Banking Services

Respondents were also requested to answer monthly usage pattern. According to Table (4.8), 44.4% of respondents use AYA Bank Digital banking services more than 10 times per month. The smallest group, 14.8% of respondent says 4 to 6 times usage in a month.

Table (4.8) Monthly AYA Bank Service Usage

Usage frequency	No of respondents	Percentage(%)
1 – 5 times in a month	21	19.4%
4 – 6 times in a month	16	14.8%
7 – 9 times in a month	23	21.3%
10 and above in a month	48	44.4%
Total	108	100%

Source: Survey data (2019)-Mitigating security risks of digital banking in AYA Bank

4.3 Identify the Security Weakness in AYA Bank Digital Banking Services

In this section, there is the analysis using of 5-point Likert scale measurement on survey questions replied from respondents regarding identify the security weakness in AYA Bank digital services.

In table (4.9), the analysis represents that most of the respondent strongly agreed by mean score 4.02 and standard deviation 0.793 shows that AYA Bank IT staff are not allowed to use unsecure Wi-Fi network or free to use network to access the back system from outside network. It is clearly state that IT staff are following the policy not to use unsecure Wi-Fi network.

Analysis on questionnaire shows that most of the bank IT staff inform the IT security team as long as they lost their devices and take action for further prevention so that the other person who got the belonging may not be able to use the stored information saved on the lost device by seeing the mean score 3.95 and standard deviation 0.633.

There is one concerns that IT team need to take action as per survey results from respondent from questionnaire with mean score 3.60 and standard deviation 0.475 shows that AYA Bank IT should follow the security policy guide line regarding the vendor risk. IT person should not allow vendor's remote access usage without having close monitoring. Vendor may amend, change or alter the customer information without bank permission.

With mean score 2.0 and standard deviation 0.705, questionnaire for setting limitation on maximum number of incorrect password submissions to log on to AYA digital banking services, most of the respondent strongly disagree AYA Bank IT system has the bad try limitation with wrong password to log in to systems. Failure to follow this standard procedure to prevent the unlimited trying of bad password, attacker may gain the valid password from authorize user by guessing the correct passwords.

Table (4.9) Identify the Security Weakness in AYA Bank Digital Banking Services

No	Factor	Mean	Std. Deviation
1	Biometric log in feature in AYA Bank mBanking 2.0/AYA Pay is more secure then traditional User ID and password credential log in.	3.78	0.728
2	If bank staff lost the mobile, thumdrive or laptop, Bank staff immediately inform IT security team for further prevention actions.	3.95	0.633
3	AYA Bank offer more authentication choices to customers rather than offering faster application and ease of use.	3.84	0.865
4	AYA Bank has process of sending OTP message to customer mobile phone while using AYA mobile banking, internet banking.	3.95	0.672
5	AYA Bank staff occasionally received email from IT security team to change password, credential and pass phrase on timely basic.	3.25	0.695
6	If vendor support need, AYA Bank IT staff allow the vendors to access the bank systems through remote access without having surveillance of IT personnel.	3.60	0.475
7	AYA Bank do not allow IT staff to use unsecure Wi-Fi network to access the bank system and environment if they are not in office network.	4.02	0.793
8	It is important for security and leadership to take a proactive approach to recognize and address the malicious insider behaviors.	2.67	0.890
9	Putting insider threat defenses procedures in place is one of alleviating security risks in secure bank system.	3.57	0.615
10	There is limitation on maximum number of incorrect password submissions to log on to AYA Digital banking service.	2.00	0.705
Overall Mean		3.46	

Source: Survey data from questionnaire (2019)

4.4 Measuring Security Risks in AYA Bank Digital Banking Services

In this section, there is the analysis using of 5-point Likert scale measurement on measuring security risks in AYA Bank digital banking services. The survey questions were pertaining to measure what are the security risks in the AYA Bank digital banking environment.

Table (4.10) present that most of the bank IT staff agree that schedule penetration testing is ongoing in this year at the time analysis by seeing the mean score 3.86 and standard deviation 0.913. According to survey question of asking existing proper approval process practice in AYA Bank, result shows that mean score 3.78 and standard deviation 0.750, IT staff agree to change the customer information upon the approval process. As per questionnaire response for controlling the back office user access limitation and giving the appropriate user access only after respective approval process done the approval, It seems AYA Bank user access limitation process is taking in control and only give access to appropriate request person by seeing the mean score 3.29 with 0.941 standard deviation. There is another point to take note that AYA Bank management may not enforcedly ask IT security team to initiate penetration testing and vulnerability testing in digital banking system with lowest mean score 3.19 and standard deviation .090, this is far below the overall mean score 3.58. With the lowest mean 2.0 and standard deviation 0.705 shows on the factor that AYA Bank internal IT system may not have bad try limitation process to prevent the guessing the password of the legitimate user account.

Table (4.10) Measuring Security Risks in AYA Bank Digital Banking Services

No	Factor	Mean	Std. Deviation
1	AYA Bank is using the standard security measures put in place to ensure privacy and confidentiality of customer information is protected	3.49	0.840
2	AYA Bank management regularly ask IT security team to do penetration testing and vulnerability testing.	3.19	0.090
3	In a situation that need to change the customer information in, respective AYA Bank IT staff can change the information only after the approval process done.	3.78	0.750
4	Bank IT team conduct the scheduled penetration testing using the same technique and same scope as per last test.	3.86	0.913
5	Every after security risk assessment done in Digital banking services, respective IT sections take a lead to apply the recommended remediation as soon as possible.	3.71	0.792
6	AYA Bank Digital banking services has scheduled maintenances in quarterly/yearly conduct by IT person.	3.49	0.878
7	AYA Bank control the back office user access limitation and giving the appropriate user access only after respective approval process done.	3.29	0.941
8	In the bank system, sensitive customer data are stored in encrypted format.	3.67	0.741
9	AYA Bank internal audit team regularly conduct IT general control audit to IT department.	3.62	0.705
10	Bank must adopt adequate security measures to maintain the secrecy and confidentiality of data. Further, they must use logical access control to implement it.	3.71	0.750
Overall Mean		3.58	

Source: Survey data from questionnaire (2019)

4.5 Mitigating Security Risks Practices in AYA Bank Digital Banking Services

In this section, there is the analysis using of 5-point Likert scale measurement of what are the mitigation practices of security risks in AYA Bank. Questionnaire result are taken from AYA Bank IT staff responses.

Table (4.11) Mitigating Security Risks Practices in AYA Bank Digital Banking

No	Factor	Mean	Std. Deviation
1	In the last twelve months, AYA Bank security team engaged with security experts to do penetration testing.	3.92	0.548
2	System updates and environment patching process are well scheduled.	3.89	0.675
3	AYA Bank IT team has a control mechanism on unauthorized system access.	3.84	0.745
4	AYA Bank IT team has formal request procedures whenever they need access the data and critical systems.	3.84	0.601
5	AYA Bank security operation team has enough resources and perform threats monitoring process as daily job.	3.33	0.648
6	AYA Bank security team can quickly set up emergency response when the significant threat target AYA Bank Digital banking services.	3.70	0.775
7	AYA Banks audit team strengthened internal audit programs to stop intentional entry of bad data into system by employees.	3.44	0.562
8	AYA Bank use firewall to protect hacker attacks and network intrusion from Netizens.	3.94	0.716
9	AYA Bank IT staff know exactly what to do when some hackers are attempting to steal the customer information.	3.70	0.638
10	AYA bank management periodically review the existing monitoring process to keep update.	3.57	0.615
Overall mean		3.72	

Source: Survey data from questionnaire (2019)

In table (4.11), the analysis represents regarding the physical hardware, firewall, using in the AYA Bank. Firewall is the basic infrastructure need for the organizations to block, protect from unwanted sources. It mean value is 3.94 and standard deviation is 0.716.

Another questionnaire result showing that most of the respondent strongly agreed that AYA Bank security team has engaged with security partners and discussed the detail work scope to perform in the testing. It mean value is 3.92 and standard deviation is 0.548.

Most respondent agree on the point regarding formal request procedures in IT Department, mean value is 3.84 and standard deviation is 0.601, represent that AYA Bank IT has formal request procedures when the staff need to access the data from critical systems.

Some IT staff still agree on the questionnaire regarding enough resource in security operation team , by seeing mean value 3.33 and standard deviation 0.648, represent that AYA Bank security operation team may not enough resources and perform threats monitoring process with available resources as daily job . By seeing this, there may have shortage of man power allocation to security operation team and daily security operation may have service lapse.

Chapter 5

Conclusion

In the last chapter of research, study describes findings from analysis done in the previous chapter , give suggestion and recommendation for further research. In order to compete in the ever-changing technological world, leaders must stay informed. The importance of budgeting for the investment in technology and keeping innovation alive within organizations are key priorities. Without effective network-defense and security standard and procedure a business is constantly at risk to protect sensitive and private organization data. The use of more IT security features will not directly solve all operational security breaches happening in industry. However, improving IT security strategies, processes, standard procedures, guidelines and frameworks can help to mitigate and alleviate the most of the security risks. Risk management strategies must be refresh all the time and advanced as technology evolves. To remain competitive, leaders must be proactive and aware of the changes that affect business security and sustainability. Throughout the study, implementation of security standard and policies are the pertaining as the major roles of the AYA Bank Digital Banking services. As shown in objective of the study, the study manage to identify the security practices established in AYA Bank digital banking services. Some practices are in weak position and describe in the findings section. There are a few security mitigation measurement implemented in bank environment. However, measurement still need to improve and enhance further.

5.1 Findings

Survey response point out that most of AYA Bank IT staff are following the guidelines which were circulated to IT staff via email such as not use the bank systems with insecure public Wi-Fi connection when staff are in public area when they need to support the bank.

AYA Bank should have strong security policy for external parties such as outsource labor, vendors and consultants. There is a weak point to prevent and mitigate the vendor risk in the bank environment as some of the services have dependency on vendors.

AYA bank should have periodic security engagement with external partners to do system assessment, multiple vulnerable testing, penetration testing on recent updates happened in the bank systems frequently. Not conducting a security risk assessment regularly can impact the business at risk. All employees in an organization must understand that security policies and procedures exist, that there is a good reason why they exist, that they must be enforced, and that there can be serious consequences for infractions.

Logging, periodic monitoring, and auditing provide an organization the opportunity to discover and investigate suspicious insider actions before more serious consequences ensue. According to survey results, AYA Bank should emphasize more on putting the strong watch and monitoring process on usage of internal systems. There may have employee sabotage, disgruntled employee unhappy with his management maybe trying to damage the information system resources available at his disposal as a display of revenge to management. Although this type of threat is less compared to other threats, it is still forming one of security risks to the bank and it should mitigate as per suggestions. Insider threats are influenced by a combination of technical, behavioral, and organizational issues, and must be addressed by policies, procedures, and technologies. Therefore, it is important that bank management, human resources, information technology, and security staff understand the overall scope of the problems and communicate it to all employees in the organization.

5.2 Suggestions

Bank management should provide periodic notifications to all the relevant parties that serve as a constant reminder of threats, require employees to attend regular scheduled training sessions presenting illustrations of current security breach trends, and provide resources for guidance to combat challenges brought by evolving technologies. It is important to understand that a security risk assessment is not a one-time security project. Rather, it is a continuous activity that should be conducted at least once every other year. Continuous assessment provides an organization with a current and up-to-date snapshot of threats and risks to which it is exposed. Apply mitigating controls for each asset based on assessment results. Highlighting security awareness to employees and customers is essential in financial institutions..

Bank management may benefit from the results of this study by developing in-depth training, monitoring business internet activity, and implementing a risk assessment process to identify and monitor emerging security threats. Furthermore, the need for consistent innovation and proactive security measures might aid in the prevention of security threats. Bank should conduct the awareness trainings, technical refreshment sessions to the new joiners and fresher to get more exposures on risks and compliances.

5.3 Limitation and Need for Further Research

In this research is only focusing on mitigation factors that is practicing in AYA Bank and facts are only based on Digital Banking practices. A limitation of the study was that the findings reflected only the experiences of AYA IT and non-IT personnel who are sharing the knowledge they have in mind. Recommendations for further research include focusing on participants that perform daily operational function lines. Identifying and exploring the experiences of insiders should be beneficial to future research. Future researchers may also consider exploring the relevance of gender and age to insider exposure to operational security threats that may face in future. Further research should cover for the (1) training and awareness program , (2) culture and behavioral effects, (3) policy and compliance in the Bank.

Reference

Book:

AlHogail, A. (2015). *Computers in Human Behavior* (Vol. 49). Elsevier.

Coburn, A., Leverett, E., & Woo, G. (2018). *Solving Cyber Risk:Protecting Your Company and Society* (First ed.). New Jersey, New Jersey, USA: Wiley Publication.

Michael Muckin, S. C. (2019). *A Threat-Driven Approach to Cyber Security*. Lockheed Martin Corporation.

Website:

AYA Bank official website https://www.ayabank.com/en_US/about-aya/about-us-in-brief/

Amutha D.(2016).*A Study of Consumer Awareness towards e-Banking.*| https://www.omicsonline.org/open-access/a-study-of-consumer-awareness-towards-ebanking-2162-6359-1000350.php?aid=77508

Kim, Loy.(2018).*Emerging Risk Management and Security Trends in bnking*.Magazine article. Vanderbilt. https://www.securitymagazine.com/articles/89528-emerging-risk-management-and-security-trends-in-banking

Ulrich Faisst, Oliver Prokein.(2006).*Conceptual framework, Management of Security Risks.*Research Paper. University of Augsburg. https://www.fim-rc.de/Paperbibliothek/Veroeffentlicht/170/wi-170.pdf

William, Stallings.(2018). Understanding Information Security Governance.Electronic article. http://www.informit.com/articles/article.aspx?p=2931571

U Myint Zaw.(2017).*Leap-frogging technology*.World Finance magazine article https://www.worldfinance.com/banking/with-myanmars-economic-future-looking-promising-aya-bank-seeks-foreign-investors.

Gustavo Montesdioca and Gastaud Maçada.(2015).*Measuring user satisfaction with information security practices*.Research article. https://www.researchgate.net/publication/267928690_Measuring_user_satisfaction_with_information_security_practices

Nancy P. Larrimore.(2018).*Risk Management Strategies to Prevent and Mitigate Emerging Operational Security Threats*.Dissertation article.Walden University https://pdfs.semanticscholar.org/8f75/9db5acefbcbd0f7db9c81b2cc641144adb9d.pdf

National Cyber Security Centre.UK.(2018).*10 Steps to cyber security*.Guide line https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary

Siagi project team.(2011).*Risk Assessment*.Electronic article https://siagi.org/our-research/risk-assessment/

Dr. Tejinderpal Singh.(2013).*Security and privacy issues in e-banking* : *An empirical study of customer's perception*.Research report. Indian Institute of Banking and Finance.Mumbai http://www.iibf.org.in/documents/reseach-report/Tejinder_Final%20.pdf

Essays, UK.(2018).*Study On Awareness Of Internet Banking*.Electronic article https://www.ukessays.com/essays/information-technology/study-on-awareness-of-internet-banking-information-technology-essay.php?vref=1

Basie von Solmsa,Rossouw von Solms.(2004).*The 10 deadly sins of information Security management*.(Vol 23).Elsevie https://www.uio.no/studier/emner/matnat/ifi/INF3510/v10/learningdocs/VonSolms-10-Deadly-Sins.pdf

APPENDIX

QUESTIONNAIRES

The following questions are asking for mitigating the security risk practices of Digital banking services of AYA Bank. Please be assured that your responses will be strictly confidential. Please put a (✓) mark to indicate your preference. Thank you and appreciate your participation.

Section A: Demographic profile analysis

(1) What is your gender?

○ Male	○ Female
○ Prefer not to say	

(2) What is your age group?

○ Under 21 years	○ 21 to 30 years
○ 31 to 40 years	○ 41 to 50 years
○ Above 50 years	

(3) What is your highest level of education?

○ Under Graduate	○ Graduate
○ Master	○ Doctorate

(4) What is your occupation?

○ Banker	○ Government Employee
○ Company Employee	○ NGO/INGO Employee
○ Self-employed	○ IT professional
○ Student	○ Other

(5) Marital Status

○ Single	○ Married

(6) Income Per Month (MMK)

○ Less than 200,000	○ 200,001 – 500,000

○ 500,001 – 1,000,000

○ 1,000,000 – 2,000,000

○ Above 2,000,000

(7) How many years are you working in AYA Bank?

○ Less than 6 months

○ 6 months - 1 year

○ 1 year - 1 year and 6 months

○ 1 year and 6 months - 2 years

○ Above 2 years

(8) Do you ever use AYA Bank Digital banking services?

□ AYA iBanking

□ AYA SMS banking

□ AYA mBanking

□ AYA Pay (e-Wallet)

□ AYA mBanking 2.0

(9) How frequently do you use AYA Bank Digital banking services?

○ 1 - 5 times in a month

○ 4 - 6 times in a month

○ 7 - 9 times in a month

○ 10 and above in a month

Section (B): Identify the Security Weakness in AYA Bank Digital Banking Services

(1) Strongly disagree, (2) Disagree, (3)Neutral, (4) Agree, (5) Strongly agree

No	Survey Question Items	1	2	3	4	5
1	Biometric log in feature in AYA Bank mBanking 2.0/AYA Pay is more secure then traditional User ID and password credential log in.					
2	If bank staff lost the mobile, thumdrive or laptop, staff immediately inform IT security team for further prevention actions.					
3	Bank offer more authentication choices to customers rather than offering faster application and ease of use.					
4	AYA Bank has process of sending OTP message to customer mobile phone while using AYA mobile banking, internet banking.					
5	AYA Bank staff occasionally received email from IT security team to change password, credential and pass phrase on timely basic.					
6	If vendor support need, AYA Bank IT staff allow the vendors to access the bank systems through remote access without having surveillance of IT personnel.					
7	AYA Bank do not allow IT staff to use unsecure Wi-Fi network to access the bank system and environment if they are not in office network.					
8	It is important for security and leadership to take a proactive approach to recognize and address the malicious insider behaviors.					
9	Putting insider threat defenses procedures in place is one of alleviating security risks in secure bank system.					
10	There is limitation on maximum number of incorrect password submissions to log on AYA Digital banking service.					

Section C: Measuring Security Risks in AYA Bank Digital Banking Services

(1) Strongly disagree, (2) Disagree, (3) Neutral, (4) Agree, (5) Strongly agree

No	Survey Question Items	1	2	3	4	5
1	AYA Bank is using the standard security measures put in place to ensure privacy and confidentiality of customer information is protected					
2	AYA Bank management regularly ask IT security team to do penetration testing and vulnerability testing.					
3	In a situation that need to change the customer information in, respective AYA Bank IT staff can change the information only after the approval process done.					
4	Bank IT team conduct the scheduled penetration testing using the same technique and same scope as per last test.					
5	Every after security risk assessment done in Digital banking services, respective IT sections take a lead to apply the recommended remediation as soon as possible.					
6	AYA Bank Digital banking services has scheduled maintenances in quarterly/yearly conduct by IT person.					
7	AYA Bank control the back office user access limitation and giving the appropriate user access only after respective approval process done.					
8	In the bank system, sensitive customer data are stored in encrypted format.					
9	AYA Bank internal audit team regularly conduct IT general control audit to IT department.					
10	Bank must adopt adequate security measures to maintain the secrecy and confidentiality of data. Further, they must use logical access control to implement it.					

Section (D): Mitigating Security Risks Practices in AYA Bank Digital Banking Services

(1) Strongly disagree, (2) Disagree, (3) Neutral, (4) Agree, (5) Strongly agree

No	Survey Question Items	1	2	3	4	5
1	In the last twelve months, AYA Bank security team engaged with security experts to do penetration testing.					
2	System updates and environment patching process are well scheduled.					
3	AYA Bank IT team has a control mechanism on unauthorized system access.					
4	AYA Bank IT team has formal request procedures whenever staff need to access the data and critical systems.					
5	AYA Bank security operation team has enough resources and perform threats monitoring process as daily job.					
6	AYA Bank security team can quickly set up emergency response when the significant threat target AYA Bank Digital banking services.					
7	AYA Banks audit team strengthened internal audit programs to stop intentional entry of bad data into system by employees.					
8	AYA Bank use firewall to protect hacker attacks and network intrusion from Netizens.					
9	AYA Bank IT staff know exactly what to do when some hackers are attempting to steal the customer information.					
10	AYA bank management periodically review the existing monitoring process to keep update.					