Robust Security Framework for Mitigating Cyber Threats in Banking Payment System: A Study of Nepal

Rajib Dongol[1] and Jyotir Moy Chatterjee[2]

[1]Research Scholar, LBEF Campus
[2]Faculty Member, LBEF Campus

ABSTRACT

Today, customer needs, technical capabilities, management preconditions, socio-economic and financial problems have become an urgent innovation development and transformation of technology. With the spread of technology, especially the internet, banks increasingly rely on technology for online bank online payment system. Unfortunately, bank-related cybercrime is also becoming more and more worrisome. The trend of cybersecurity attacks on the banking sector in Nepal is much higher than in any other sectors. Common cyber security attacks include banking phishing, cross-site scripting, cybersecurity, botnets, spoofing, etc. This will cause huge losses to customers and banks, which will reduce the reputation of the bank and reduce the user's confidence in the bank.

In this study, we analyzed the new challenges in terms of bank security and Privacy of banks assets. Security control mechanisms for the deployment of the commercial banking sector have identified. The security and privacy issues are recognized by the financial sector for payment system and are especially prevalent in cybersecurity attacks. The survey focused on banks security practice based on their perception on cyber security. The questions were based upon banks staff knowledge about cyber security and awareness of common threats in payment system of banks. The results obtained support the argument that there is weak practice on security implementation for the cyber threats in the payment systems and gap between banks perception and practice related to payment system.

Finally, the proposed framework provides banks protection against cyber-attacks and provides a powerful security baseline/framework to deter intruders from attacks and opportunistic malicious threats.

Keywords*: Information Security, Cyber Threats, Vulnerabilities, Banks, Malware, Incident Response Plan, IT Risk Management Framework, Security Awareness, Payment system, Payment security flaws, cyber security attacks, confidentiality, Integrity, and Availability.*

I. INTRODUCTION

Background

In a world, technology driven more and more by information system, online transaction, social networks, and data transmission, stored or managed via networks. More and more organizations especially banking sectors are highly depended on Information processing and on payment system. Automated payment process perform with payment systems, information security, and data privacy are permanently facing risks of cyber threats, frauds and vulnerabilities. With the development of new tools and techniques, cyber threats and vulnerabilities are consistently increasing in terms of number of attacks and level of damage to its infected victims.

Today customer desires, technological competences, administrative prerequisites, socioeconomics and financial matters are as one making an urgent change in innovation development. This prompts the requirement for banking institution to give out the challenges and hold a proactive way to deal with security for different threats. There is a visible move in the financial banking sector in the manner in which customers deal with online transactions from different online payment systems. There is a quick increment in the usage of digital channels, for example, online banking, e- wallets, versatile banking, ATM. This increases in exposure on internet and thereby cyber-attacks, which further may lead to financial losses in banking sectors.

Problem Statement

The increasing risks of cyber threats and vulnerabilities, banks payment system of Nepal exposing an exceptional challenge of data privacy and security breaches and therefore hard to follow proper security assessments framework/baseline for strengthening their cyber security landscape.

The biggest challenges facing banks' all around the world today is information security and protecting it. Whenever we think of cybersecurity, "cybercrime," is the first things which is growing. Governments' & private companies' are taking many steps to avoid these cybercrime. In addition to various measures, cybersecurity is still a matter of great concern to many people. This article focuses on the cybersecurity faces in the latest technologies. The latest network security technologies, ethics & trends' in changing network security (G.NIKHITA REDDY, 2014).

Aim of the Research

This main aim of this research to organize a bigger and precise picture of cyber threats and vulnerabilities in banks payment system of Nepal with intent to understand the current posture of cyber security issues and hence use it to establish a strong security IT risk assessment baseline/framework to stops intruders attack and opportunistic malicious adversaries. Through this report, banking sector in Nepal look forward to assisting in the attainment of more cyber secure Nepal.

Research Objectives

The objectives of this study are:

- To determine landscape of threats and vulnerabilities facing commercial bank in Nepal.
- To determine the mitigation and securing strategies building a security assessment framework which banking in Nepal could use to manage the information security threats and vulnerabilities
- To propose the security assessment framework for preventing the risks of threats and vulnerabilities.

Research Question

- How information ethical hacking and cyber security is being practice in Banking of Nepal?
- What are the solution to the issues of hacking and cybercrime in Nepal Banking industry?
- What assessments need to use to reduce current cybersecurity vulnerabilities and threats in banking payment system in Nepal?
- What types' of cybercrime are risks' specific to the financial sectors' & what steps are taken to mitigate these risks?

Scope of the Research

The scope of this research is to organize a bigger and precise picture of cyber threats and vulnerabilities in banking payment system of Nepal with intent to understand the current posture of cyber security issues and hence use it to establish a strong security assessment baseline/framework to stops intruders attack.

Significant of the Research

The following are the significant of this study:

- The finding from the study will aware the stakeholders/employees/department in the banking industry and the public on how robust security framework and assessment can be used in cyber security to protect against trending vulnerabilities and threats in payment systems.
- This report provides a clear, organized approach to dealing with potential threats to computers and data, and takes appropriate action in response to bank cybersecurity incidents when third party payment system intrusions or incident sources are traced back to the bank and describe the overall plan.

- It identifies structures, roles and responsibilities, types of common events, incidents and methods of preparing, identifying, including, eradicating, restoring and implementing lessons learned to minimize the impact of security incidents.

II. LITERATURE REVIEW

Research Background

In this Chapter, the related articles, books, research papers and previous researches similar to the research topic of this study have been reviewed and presented. The related cyber security framework for the payment systems and its mitigation approaches for the threats and vulnerabilities are reviewed and presented

Theoretical Review

Significant growth in cyber attacks often steals confidential data and serious consequences because of the exponential growth in the use of Internet interconnection and malicious applications. For emerging technologies, malware is the primary choice for weapons that exploit existing vulnerabilities to carry out malicious activities in cyberspace (jang, 2014). According to (Elena Sitnikova, 2014), 205/5000

Internet for transmitting critical information and trading between different systems. These systems extend from one business organization to the customer and supplier communities. Therefore, today, the Internet's vulnerabilities and threats in different networks are as important as systems integrated in enterprise networks, and use risk management methods to check Internet security. The independence measured by the Audit Committee, financial expertise and technical expertise were not significantly negatively correlated with the cybersecurity of the Nigerian banking industry. The audit committee currently established in Nigeria will not be able to provide control and oversight functions for the banking industry's cybersecurity, which is the most sensitive sector in the economy (Stephen A. Ojeka, 2017). Check out the security aspects of mobile banking applications. In addition, we use workflow technology to simulate real-world scenarios related to mobile banking application attacks' and summary insights designed to help banks' & consumers reduce the security risks of mobile banking applications (Wu He, 2015). The study assessed the main aspects and basic concepts of social engineering attacks and their impact on New Zealand's banking industry. The study further identified the attack phase and provided a user response model to mitigate the engineering attack cycle at each stage. The result of the study is a model that provides users with a process of reacting to their participation in online activities (David Airehrour, 2018). According to (Anna Sapienza, 2017), automated alerting systems for current cyber threats have introduced the spread of different malicious sources on dark networks, as well as the activities of cybersecurity experts on social media. Between September 2016 and January 2017, the Auto-Trigger System approach generated 661 alerts, of which approximately 84% were related to current or upcoming cyber threats that could be registered in the security assessment. After recent attacks on financial institutions, cybersecurity risks have become a threat to financial stability. Document cyber risks for global financial institutions by analyzing different types of network events (data breaches, fraud and business disruptions) and using various dataset, identification models (Bouveret, 2018). The threat cyberspace poses to security can jeopardize specific lifestyles, build on key functions of information technology and infrastructure, and have less direct attention to humans. The solution to this dilemma is the cybersecurity strategy, which is anti-vulnerability and on the basis strong considerations of privacy and data protection. This security must base on the ethics of the information domain, which based on the dignity of information related to humans (Cavelty, 2014). The following below are the base papers for this study, which are shown in tabular form.

III. RESEARCH METHODOLOGY

Research Methodology

Research Methodology is one amongst important section in the study, which determines the method of research methodology. It establishes components of research structures such as strategies, methods and methods. Research methods are important tools for identifying problems, need to be explored, and achieve set goals in research (Mohamed Al Kilani, 2016). According to (Solms, n.d.) , research methods play a very important role in ensuring the quality of research & determining whether the results' of one study can be meaningfully integrated with the results of another.

The main purpose of the research method is to provide crystal knowledge about the method or process to used, and to discuss research questions for resolution. Therefore, it can be defined as a tool for collecting data and analysis that must be compatible with research questions and objectives in order to obtain accurate and effective results.

This chapter contains research methodology used for achieving the objectives. In this section, it is discussed about the research approach, data and study area, research design used, populations' & sample of the study, collection tools' & analysis procedure of data.

Research Approach

During selecting research approach, the following factors should considered:

- the characteristics of the topic and time of the study
- There are three statements of research methods (quantitative methods, qualitative methods and mixed method methods)

However, choosing the appropriate Nepalese bank payment system cybersecurity research is not easy, because cybersecurity allows researchers to choose the appropriate method from different research methods, taking into account the purpose of the research. . The study is based primarily on major data sources and is based in part on secondary sources.

Primary Data Source

- Questionnaires
- Survey

Secondary Data Source

- Internet
- Documents
- Journal

3.3 Population and Sampling

Population is complete set of cases/groups from which a sample is taken. The sample is a subset of a larger population, selected by the researcher to participate in a research project. For this study, all 28 commercial banks operating in Nepal are the total population.

Sample is a sub set or some part of the larger population. The purpose of sampling is to reduce the expenses in terms of money, effort and time. A total of 150 respondents were taken in this study and all of them were IT, Security and compliance department of banks, among them only 100 responded were valid and taken for the study. These respondents were selected using simple sampling technique. The sampling techniques for the study followed non-probabilistic sampling techniques i.e. convenience sampling.

Therefore, the sample size of N=100 will be used for this research. The questionnaires will fill in questionnaires document format from google online form, and findings collected for the security of the organizations and institutions integrity.

Data and Study Area

The study completely based on the primary data & secondary data. The area of the study is all the 28 commercial bank of Nepal along with the department and banks staff. The 28 commercial bank of Nepal are listed below:

S.N.	Name of the Banks'
1	Nepal Bank Ltd.
2	Agriculture Development Bank Ltd.
3	Nabil Bank Ltd.

4	Himalayan Bank Ltd.
5	Nepal Investment Bank Ltd.
6	Standard Chartered Bank Nepal Ltd.
7	Nepal SBI Bank Ltd.
8	Nepal Bangaladesh Bank Ltd.
9	Everest Bank Ltd.
10	Kumari Bank Ltd.
11	Laxmi Bank Ltd.
12	Citizens Bank International Ltd.
13	Prime Bank Ltd.
14	Sunrise Bank Ltd.
15	Century Bank Ltd.
16	Sanima Bank Ltd.
17	Machhapuchhre Bank Ltd.
18	Global IME Bank Ltd.
19	NIC Asia Bank Ltd.
20	NMB Ltd.
21	Prabhu Bank Ltd.
22	Siddhartha Bank Ltd.
23	Bank of Kathmandu Ltd.
24	Civil Bank Ltd.
25	Nepal Credit and Commerce Bank Ltd.
26	Janata Bank Nepal Ltd.
27	Rastriya Banijya Bank Ltd.
28	Mega Bank Nepal Ltd.

Table 1: List of Nepalese Banks

Data Collection Methods

The purpose of this study is to discover, examine and understand the trending state of security of information systems in Nepalese payment systems and a strong security framework to improve future security management and mitigate threats. In order to study the recent cyber threats and vulnerabilities of the Bank of Nepal payment system, data collection methods will applied to research objectives and research issues.

Throughout the study, the samples follows a mixed research approach in which qualitative' & quantitative methods' & techniques' used. Hybrid researches' method enable researchers to take advantage of practical methods and systems that use multiple methods to answer research questions' relatively than limiting or constraining researchers' choices. The research samples were from different banking departments and security consultants in Nepal.

A set of Likert scale issues was prepared for the security perception and practice of banks in the payment system. These questions directed at IT department heads, compliance/risk/audit/ISO (Information Security Officer), & system administrators'. As they manage all information, system functions and operation, including their compliance security, while security consultants' & security officers' ensure that all systems meet the compliance requirements. The questionnaire for the IT/Risk/Compliance/Audit/ISO department based on the NRB (Nepal Rastra Bank) audit checklist and the ICT (Information Communication and Technology) security checklist design. The conclusions drawn from the interpretation data presented in the SPSS (Social Science

Statistics Package) tools and recommendations present a security assessment. Based on existing results identified through questionnaires and related work, it is recommended to establish an information system security assessment framework to mitigate cyber threats in recently discovered vulnerabilities.

Data Analysis

The frequency tables that reports the percentage of each of the categories and frequency that are easy to understand and interpret were used. Oher than the descriptive analysis, one way ANOVA test and correlation analysis were conducted.

Descriptive Analysis

Descriptive statistics were used to explain the demographic characteristics of the respondents along with security perception and security practice payment system of banks. Frequencies, mean and standard deviation were calculated to describe the variables.

Correlation Analysis

The correlation coefficient was used to depict the association of security perception and practice for payment system of banks.

One Way ANOVA

The used of ANOVA in this study to define if there were any statistically relatively differences' between the mean of two or more independent groups'.

Software used

The responses collected from the distribution of questionnaire were entered in Microsoft office Excel 2013 and IBM SPSS V23. After that data were analyzed, interpreted and was presented in the written format using Microsoft office.

IV. PRESENTATION AND ANALYSIS OF DATA

Results

This section contains' results obtained from data processing/presentation and analysis in the study. The first section of this chapter devoted to describe some descriptive information of the variables used in the study. Consequently, next section contains the inferential part of the study describing the fitted models and interpretation of the results.

28 commercial banking sector of Nepal along with different departments and position in banking sector were chosen for questionnaires to acquire the security perception and practice on banking payment system and was conducted from **16th June, 2019** to **16th july,2019**. As mentioned in the questionnaires are used for study was prepared based on Information Security Officer (ISO) and Internet Communication and Technology security checklist for to strengthen their security assessment. Questionnaires used as instrument to carry out the data collection based on the security domain for assessment in banking payment system of Nepal. The data analysis result showed in tabular and diagrammatically using the pie charts in number and percentage.

Descriptive Analysis

The descriptive information of the variables used in the study is analysed in this section. This analysis is made on the basis of departments and position of banks staff.

Dependent variable

Some information about the outcome variable of the study i.e. Department and positions of banks staff is given in the following below section and table.

Variable	Type	categories
Dependent Variable		
Department	Ordinal	1- Information Technology 2-Network and System 3-Security Officer 4-Audit /Risk/ Compliance 5-Security Consultant 6-Other
Position	Ordinal	1-Junior level 2-Supervisor 3-Senior level 4-Managerial level 5-Other

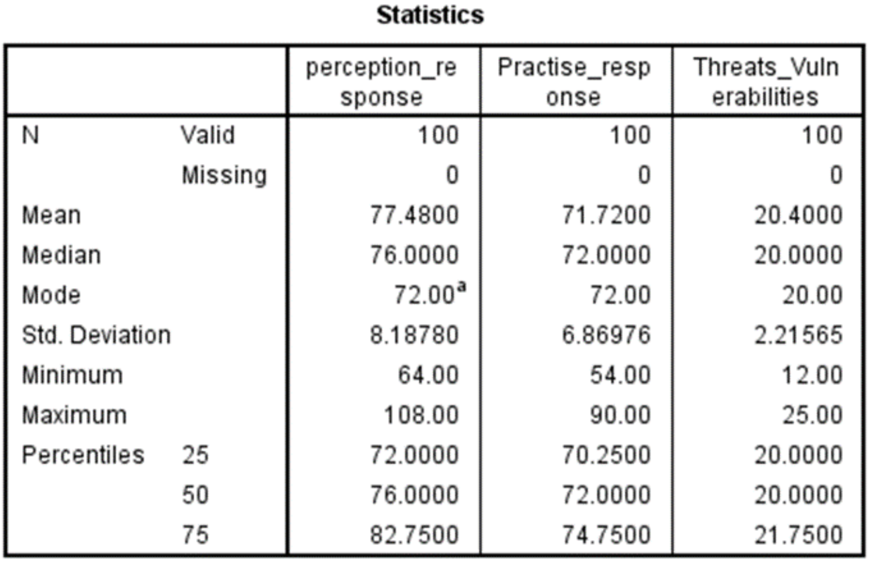
Independent Variable

Some information about the outcome variable of the study i.e. Security perception, security practice and threats and vulnerabilities assessment based on the banks departments and position of banks is given in the following below section and table.

Variable	Type	Categories
Independent Variable		
Security Perception	Ordinal	1-Strongly disagree. 2-Disagre. 3-Neutral. 4-Agree. 5-Strongly agree.
Security Practice	Ordinal	1-Strongly disagree. 2-Disagre.

		3-Neutral. 4-Agree. 5-Strongly agree.
Threats and Vulnerabilities Assessments	Ordinal	1-Strongly disagree. 2-Disagre. 3-Neutral. 4-Agree. 5-Strongly agree.

Descriptive information of Quantitative Variables



Statistics

		perception_response	Practise_response	Threats_Vulnerabilities
N	Valid	100	100	100
	Missing	0	0	0
Mean		77.4800	71.7200	20.4000
Median		76.0000	72.0000	20.0000
Mode		72.00[a]	72.00	20.00
Std. Deviation		8.18780	6.86976	2.21565
Minimum		64.00	54.00	12.00
Maximum		108.00	90.00	25.00
Percentiles	25	72.0000	70.2500	20.0000
	50	76.0000	72.0000	20.0000
	75	82.7500	74.7500	21.7500

Table 2: Descriptive information of Quantitative Variables

The above table shows that the mean security perception score of the respondent was 77.48 with the standard deviation 8.1878 ranging from 64 to 108. The median score was 76 indicating that the 50% of the respondents had perception score 76 or more. 25% of the respondents had score less than 72 whereas 75% of them had score 82.75 or more. Also, most of the respondents had perception on security score 72.

Comparison on Security Perception on the basis of Positon of the banks staff

Perception Response

	N	Mean	Std. Deviation	Minimum	Maximum
Junior Level	44	77.7273	7.04921	66.00	94.00
Supervisor	29	75.0690	6.16981	64.00	88.00
Senior Level	21	77.9524	9.54189	68.00	108.00
Managerial Level	6	85.6667	14.38981	65.00	105.00
Total	100	77.4800	8.18780	64.00	108.00

	Sum of Squares	Df	Mean Square	F	Sig.
Between Groups	578.085	3	192.695	3.053	.032
Within Groups	6058.875	96	63.113		
Total	6636.960	99			

Table 3: Comparison on Security Perception on the basis of Positon of the banks staff

The above table presents the comparison of average scores of response on IT security. It shows that the average score among the staff of managerial level had highest score (85.67) followed by senior level staff (77.95) and junior level staff (77.73) whereas supervisors had lowest score (75.07). The result of ANOVA table shows that the p-value of F statistics is 0.032, which is less than 0.05 indicating that there is significant difference in average score of perception on IT security due to level of staff.

Managerial level in banks oversight the IS (Information Security) policy and framework that provides an integrated set of protection control measures that apply across the organization to ensure a secured business operation.

Comparison on security practice based on different position of banks

Practice Response

	N	Mean	Std. Deviation	Minimum	Maximum
Junior Level	44	69.6591	6.92801	54.00	87.00
Supervisor	29	71.5172	6.32806	59.00	90.00
Senior Level	21	76.0952	5.15660	67.00	87.00
Managerail Level	6	72.5000	8.50294	62.00	84.00
Total	100	71.7200	6.86976	54.00	90.00

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	593.723	3	197.908	4.658	.004
Within Groups	4078.437	96	42.484		
Total	4672.160	99			

Table 4: Comparison on security practice based on different position of banks

The above table presents the comparison of average scores of response on IT security practice on payment systems. It shows that the average score among the staff of senior level had highest score (76.09) followed by managerial level staff (72.5) and supervisor staff (71.51) whereas junior level had lowest score (69.6). The result of ANOVA table shows that the p-value of F statistics is 0.004, which is less than 0.05 indicating that there is significant difference in average score of perception on IT security practice on payment system due to level of staff. It conclude that the senior level staff are more concerned about security practice based on IT security perception

Comparison on Security Perception on the basis of bank departments

Security Perception

	N	Mean	Std. Deviation	Minimum	Maximum
Information Technology	28	78.0000	8.98971	64.00	105.00
Network and system	7	79.8571	13.14570	71.00	108.00
security	13	73.9231	3.98877	69.00	82.00
Audit/Risk/Compliance	15	77.3333	6.66190	70.00	94.00
security consultant	2	75.5000	2.12132	74.00	77.00
Others	35	78.0857	8.34679	65.00	95.00
Total	100	77.4800	8.18780	64.00	108.00

	Sum of Squares	Df	Mean Square	F	Sig.
Between Groups	232.604	5	46.521	.683	.638
Within Groups	6404.356	94	68.131		
Total	6636.960	99			

Table5: Comparison on Security Perception on the basis of bank departments

The above table presents the comparison of average scores of response on IT security perception based on department. It shows that the average score among the department of Network and System had highest score (79.8) followed by others (78.08) and IT (78.0) and Audit/Risk/Compliance (77.33) whereas security department had lowest score (73.9). The result of ANOVA table shows that the p-value of F statistics is 0.63f, which is greater than 0.05 indicating that there is no significant/relation difference in average score of perception on IT security practice on payment system due to different departments in bank.

Network and system department manage all the information systems functionalities including day to day IT operation and troubleshooting more than security perception and security. Security officer of banks ensures all the system are compliance as per the standards IT security policy, procedures, and banks requirement.

Common Security Flaws in Banking Payment Systems.

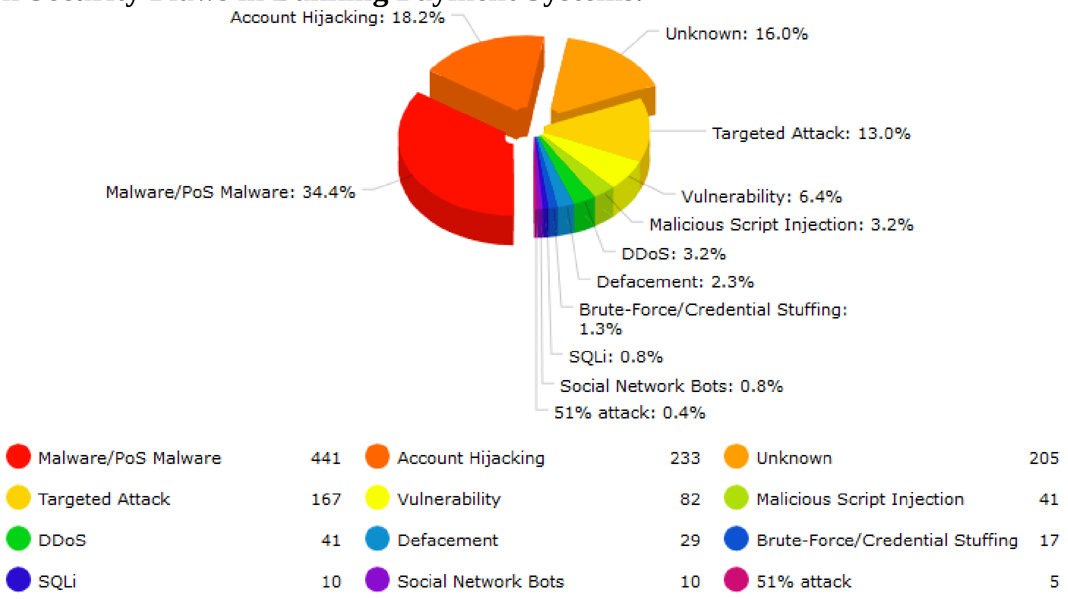


Figure 1: Attack Distribution Top 10 2018
(Source: https://www.hackmageddon.com/2019/01/15/2018-a-year-of-cyber-attacks/)

Most banks in the payment system are facing cybersecurity issues in Nepal and have changed the visual appearance, complete server compromises - system hacking, ransomware, ATM fraud, e-bank fraud, critical data breaches and more. Banking institutions and payment systems play a vital role in the country's overall economy. A quick analysis of the web analytics of these organizations' web applications revealed that most banks still lack basic security practices such as vulnerability assessment and risk assessment.

Most sites in Nepal face frequent attacks and destruction by various hacker organizations belonging to financial institutions, government agencies and other software companies. Common pitfalls or weaknesses faced by Nepal, such as cross-site scripting (XSS) in Nepalese web applications, cross-site request forgery (CSRF), server-side request forgery (SSRF), structured query language injection (SQLi), etc. Application form data. In a network system, an error occurred due to unmanaged OS patches and firmware. However, other security vulnerabilities may occur due to improperly configured resident devices and default credentials in critical systems. This indicates a lack of vulnerability management in all payment applications that execute transactions.

The IT security situation is declining due to the lack of clear separation between key sectors and Nepal's existing network laws and regulations. The government should implement strict policies for regulators that monitor network scenarios and help companies and organizations become more secure over time.

Statistic of A Grade Bank and Payment system in Nepal

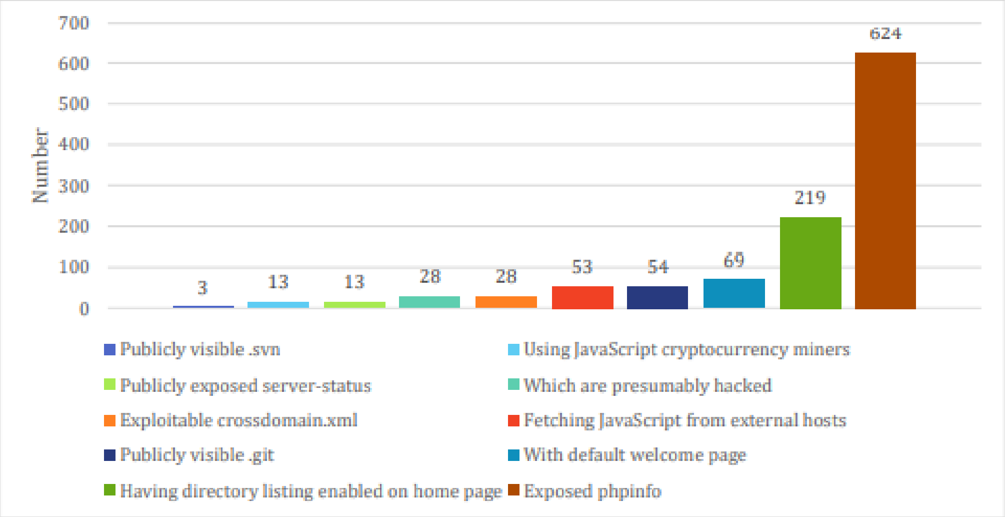


Figure 2: Static of Nepalese Website
(Source: https://techlekh.com/threat-report-2017-cyber-security-nepal/)

With the technological advancement of each component in the IT architecture, the IT world is evolving. We are facing an increase in cyberattacks, and few people know how to deal with these threats after the highly connected Internet of Things (IoT) and cloud usage have increased dramatically.

According to the Threat Nix report, Nepal's famous network security solution, after analyzing the e-banking websites of 27 A-level banks and 4 payment service providers, most applications are vulnerable to Clickjacking attacks. Clickjacking tricks web users into clicking on certain content by spreading malicious techniques that are different from user-identified clicks. However, most operations in an e-banking application are protected by a secondary password with a strong password combination and OTP (one-time password). In some cases, an attacker could allow a malicious user to steal funds from a victim's account.

According to statistics from the Knicks Nepal, four of the 27 e-banking websites are vulnerable to POODLE attacks. POODLE allows users to decrypt encrypted data and control the connection between the client's browser and the server, and can run some code in the client browser. In 27 e-banking websites and 4 online payment systems, one application has serious security vulnerabilities, allowing attackers to steal funds from the logged-in victims. (Shrestha, 2018).

V. FINDINGS, CONCLUSION AND RECOMMENDATION

RESEARCH FINDINGS

RESEARCH OBJECTIVE 1

To determine the landscape of threats and vulnerabilities facing commercial bank in Nepal.

Findings

From the questionnaires/survey, it found that banks of Nepal in payment system lack national IT security practice and standards to follow and find the threats and vulnerabilities in the system, process and people. The managerial level of banks are more concern on security perception rather than the practice and implementation. There is lack of practice in security monitoring and vulnerability management; Security Assessment Service like vulnerability assessment and penetration testing (VAPT); Incident Response and Security Consulting like information system audit and security system architecture; and IT/IS Policy.

When bank staff ask about banks' IS policies and standards, there are no standard IS policies and standards' in practice. In terms of bank security, the top management team is unable to ensure top management support for IS security and lack of information security training for bank employees. Top management support is essential for long-term and short-term IT strategies, and they must understand the information security program.

However, in all banks, there is a new authorization process for the payment system processing facility (hardware/software) prior to implementation, but there appears to be a lack of IT risk assessment for system-related threats and vulnerabilities and SLAs with service providers (service levels) protocol). Only some bank management are concerned about risk assessment. It is weak to conduct an IT risk assessment of all assets associated with the bank and execute transactions through the payment system to determine the threat of newly discovered vulnerabilities. Identifying and classifying data on the network based on sensitivity is the initial step in developing an attack plan to ensure its security. This helps identify vulnerabilities and threats associated with your organization and enforces security controls accordingly.

RECOMMENDATION

The report recommends that an effective safety management framework must consider the various assets that contribute to the operation of the system, based on an assessment of risks, threats and vulnerabilities. They are technology, people and processes. More specifically, it is recommended that secure device technology solutions alone cannot guarantee safe and reliable operation on payment system of banks. There is a need for a strategic approach that combines technology with other factors like IS policy, security framework and procedure. It is recommended that the below proposed security assessment framework for payment be further reviewed and validated for further study.

Conceptual Framework

After reviewing the related literatures, the developed concept about the study described in this section.

Schematic diagram of conceptual framework

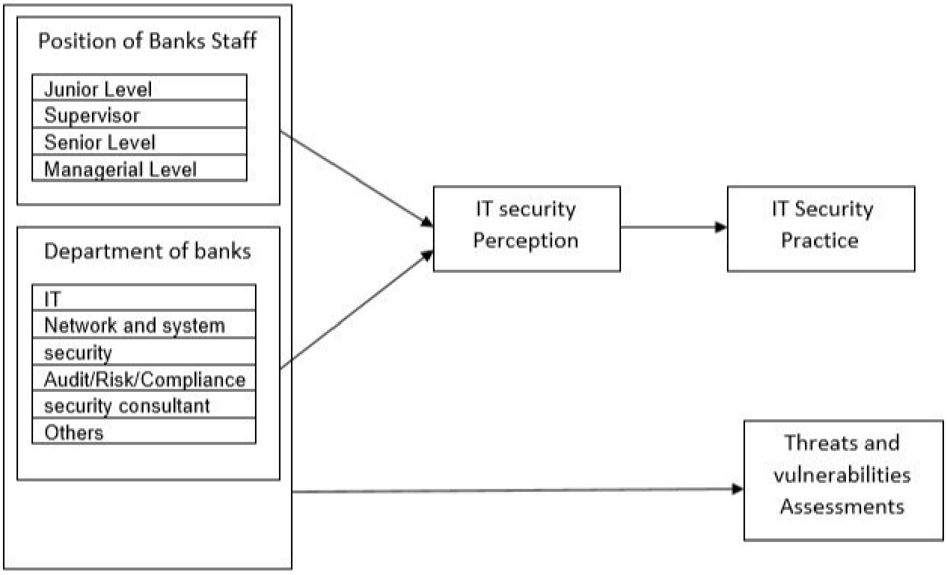


Figure 3: Schematic diagram of conceptual framework

In above figure, it shows the conceptual framework regarding IT security perception based on the banks staff and position for threats and vulnerabilities assessment with security practice and implementation of payment systems. It also shows the relation between security perception and practice based on different position and departments of banks

Introduction

When a network event occurs in a bank payment system, the bank should protect the system and the bank by implementing an appropriate security framework to identify and respond to cybersecurity threats. It provides the important information needed to understand and integrate network security best practices into your system to manage external threat risks. The above conceptual framework defined as an IT risk management framework that prepares for network events and uses cybersecurity metrics to protect its bottom line and take decisive action to mitigate and recover the consequences of cyber threats and vulnerabilities.

Information technology (IT) plays an important role and is an integral part of every business. The full advantage took by IT can bring important benefits to the business & but involves the security risks of different threats within the organization. It contains information assets related incidents that may affect the financial business. It can occur at an indeterminate frequency and extent and poses challenges to achieving strategic goals and objectives. Risk in the risk category. Different IT risk management frameworks consider the details of the IT domain in different ways. COSO ERM, AS / NZS 4360, ISO 31000 and BASEL II are typical examples of financial institutions that do not pay special attention to IT risk management (Vlasta Svatá, 2011).

The purpose of the framework is to provide guidance to effectively manage and mitigate IT-related risks from cyber threats from different sources of payment systems that have an impact on banking. It defines a systematic process for IT risk management so that bank employees fully understand the extent of the threat and ultimately allow the bank to make appropriate decisions for risk ware. Develop a risk management process to achieve the goals of this report

- Obtain adequate security for bank information and payment systems by implementing appropriate IT security response strategies.
- Evaluate security controls to meet current information protection needs and future protection needs based on changing cyber threat requirements and technologies.
- Promote a more cost-effective assessment of safety controls to help determine overall control effectiveness and create more complete, reliable and trustworthy information for bank officials to support management staff's risk management decisions.
- Promote a better understanding of the IT-related risks of bank employees, departments (including all people involved with employees, third parties and bank stakeholders).

Target Audience

This report aimed for following audiences:

- Top executives' & Board members' of banks' who need to set direction and make risk aware business decision for cyber threats.
- Control function of organization performing the IT security risk assessment
- IT and security/compliance/Audit/Risk departments implementing the controls because of IT risk assessment process.

IT Risk Governance Structure

Bank IT risk management and management includes a variety of structures and relationships. It stands out from the Board of directors' through the Risk Management Committee, the CEO and the head of the risk department, through a dedicated IT risk management function. This backbone is supplemented by related control functions and is performed by the Compliance, Internal Audit and Information Security departments. Finally, support risk procedures and responsibilities should be distributed throughout the organization and distributed to all departments and employees.

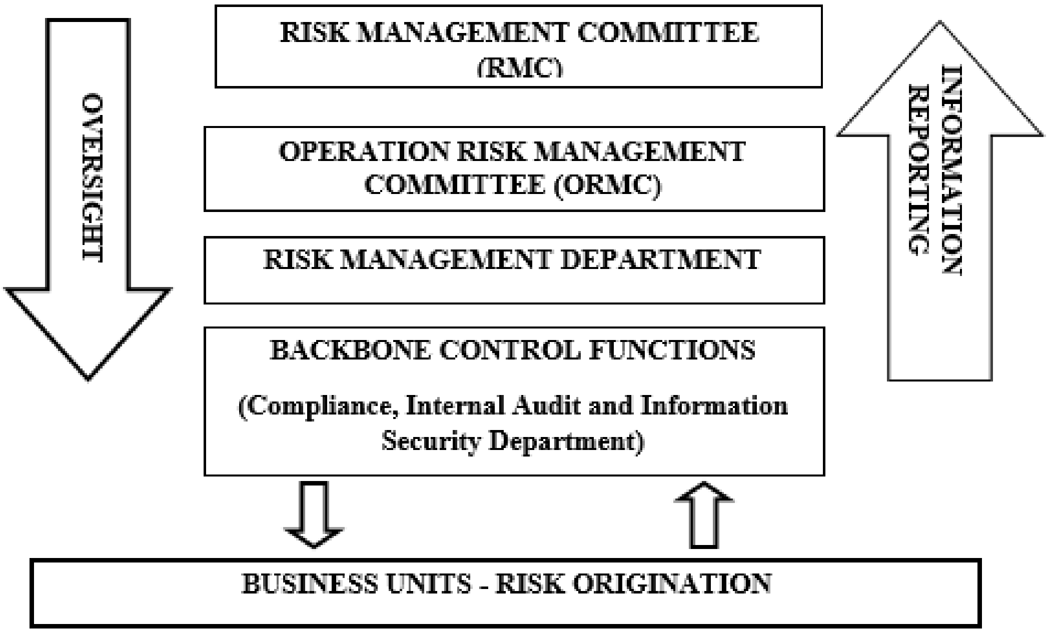

OVERSIGHT
RISK MANAGEMENT COMMITTEE (RMC)
OPERATION RISK MANAGEMENT COMMITTEE (ORMC)
RISK MANAGEMENT DEPARTMENT
BACKBONE CONTROL FUNCTIONS
(Compliance, Internal Audit and Information Security Department)
INFORMATION REPORTING
BUSINESS UNITS - RISK ORIGINATION

Figure 4: Governance Structure for Risk information reporting and oversight

Board Oversight

The Board Risk Management Committee (RMC) is the apex body of overall risk management in Bansks. Board of directors has delegated oversight of risk management to the Risk Management Committee, a sub-committee comprising of board members, CEO, Head of Risk Department. RMC ensures that IT risk management practices embedded in the enterprise, enabling the enterprise to secure optimal risk-adjustment returns.

The main objectives' of RMC is to:

- Examine of risk management plan, system, processes, and procedures' effectiveness
- Review risk policies, guidelines, and limits as well as risk exposure and risk mitigation plans.
- Define and review IT risk exposure based on change management and evolving threat.
- Cost benefit analysis and make risk-aware business.

Operation Risk Management Committee (ORMC)

Operation Risk Management Committee is accountable for reviewing, managing and controlling the risk reported within the organization. The committee ensures that the risks under their control effectively managed, promote, and implement strong risk culture within an organization.

Risk Management Department

Risk Management Department is key part of Risk Management Framework and is responsible for design and maintenance of Risk Management Framework. It provides' the standards' framework, tools', advices' and mitigation strategies' that enables operational business units' & management to effectively identify & manage risk; & through monitoring, provides' key boards, committees and management with a view of the effective & efficiency of risk management through regular risk reporting.

Backbone Control Function

The responsibility of backbone control functions such as Compliance, Internal Audit and Information Security Department is to identify and analyze the risk identified within the organization and evaluate and monitor the level of effectiveness of the control measures applied to mitigate the risk identified.

Business Units

Business units are the users and the owner of the business or systems of the organization that have direct interaction with the business process and system. They are responsible for identifying the risk that exists in their day-to-day operation or activities or system and report it to the Backbone control function or Risk Management Department.

The Risk Management Framework process workflow has developed for accountability and responsibility of banks staff (**refer to Annexure IV**).

IT Risks Assessment

IT risk assessment is the only process for assessing and analyzing IT risks and threats that affect your business. Banks can conduct an IT security assessment process based on assets and data categories to control the likelihood and potential damage of identified threats and vulnerabilities on payment systems. It measures the individual risk level of each critical information/asset associated with CIA. The assessment results' help to identify appropriate controls and strategies to reduce/tolerate or eliminate risks in risk mitigation and related threats and vulnerability responses.

IT systems made possible by a combination of potential vulnerabilities and threats analyzed by control measures. The extent of damage that can caused by a different source of threats to vulnerable systems called impacts. The degree of impact depends on the potential mission impact, which produces the qualified value of the process and the impacted resources. The risk assessment process includes the following steps.

Asset Identification

Everything that is valuable to an organization is called asset/information. Assets/information includes personnel, processes and technologies related to the processing, storage, transmission and protection of further classified data. ISO 27005 suggests that information assets are the primary asset, while hardware, software, personnel, etc. are supporting assets. Banks can establish responsibility for each asset by tagging the owner/custodian of each asset.

Banks can assign assets to individual owners (users/departments/branch offices) who are fully responsible for adequately protecting the assigned assets based on their importance and severity. Some of the identified assets in the bank are database systems, application servers, firewalls, switches/routers, laptops/desktops, software/IP, personnel and back-office and support payment systems.

Threats identification

A threat is specific threat source of events that effectively runs particular vulnerabilities. Vulnerabilities are a weakness on the system that can be triggered accidentally or deliberately.

In a bank, threats may include people, the systems and processes they use, and the conditions threat can cause harm and negative impact on their business operations. Some potential threats may be hacking, poor quality data, hardware failures, data or system corruption, viruses, worms or other harmful malware, data leakage or disclosure, theft, accidental damage or criminal fraud. Banks ensure that threats should identify and assess their access channels, motivations, outcomes and likelihood of occurrence in a timely manner.

The following table lists the list of threat sources and the events, causes, and consequences of the threat identification process.

Vulnerability Identification

Vulnerabilities are weaknesses in assets that can be exploited, and threats can come from technology, organization, internal processes, and the external environment. Some known, suspected or identified vulnerabilities are inadequate firewall protection, limited adherence to procedures and guidelines, lack of awareness of threats, poor quality of information provided, incomplete inspections and updates, unauthorized access, etc. Banks can develop a set of rules and policies and procedures for most of their internal activities and processes, and ensure that all employees adhere to these policies and procedures.

Risk Category

Risk identification is performed in an orderly manner to ensure that all important activities and events within the organization identified and all risks present in those activities are identified and categorized. It provides systematic and structured approach to identifying the risk. Another benefit is that it better manages risk, identifies' risk, & helps risk management processes work with specific risk categories.

Risk Category	**Description**	**Implications of Risk**
Strategic Risk	Loss arise from unsuccessful business plan and poor business decision.	Unable to meet business related strategic goals.
Operation Risk	Loss caused by an incomplete or failed program, system, policy, employee error, fraud, other criminal activity, or any event that disrupts a business process.	Fraud Breaches of employment law Unauthorized activity Loss or lack of key personnel
Technical Risk	Failure or delay in delivering IT Required process or information Failures of hardware's', network leakage, improper change management plans', & data center failures', business transactions & operations.	Transactions failure and lost sales. Productivity of employees' reduced.
Security Risk	Compromise information, confidence and technology. And the process of managing external attacks, malicious payload, physical damage, unauthorized access, and dissatisfied employees.	Information corruption Internal Fraud Theft and crime Theft of financial assets Reputation & brand Information assets damage
Compliance and Legal Risk	Organizational damage may be compromised by its failure to comply with the law, its own regulations, and codes of conduct and best/good practice standards.	Fines, penalties, damages, contractual problems, diminished reputation
Reputation Risk	Risk of loss to organization resulting from damages to brand value or reputation.	Deter new relationships and ability to service existing customers, accelerate customer runoff.

Table6: Risk Category

Risk Analysis

Risk analysis is the process of identifying the likelihood of an event that may occur and affecting business goals and objectives. Determining the consequences of the risk analyze the risk and its likelihood, as well as other attributes and events of the risk. An event or a set of conditions can have multiple consequences and can affect multiple targets. The process also involves determining existing risk controls and their effectiveness. Risk analysis provides the basis for risk assessment and the need to address risks and the most appropriate risk management strategy for making decisions.

Existing control

Existing control measures been taken to mitigate the effects of risk. Controls' may be strong or weak with measured & repeated. Control measures may include' regulator body, policies or procedures, employee awareness and training, separation of duties', protective control measures & equipment, and structural. The following table describes the control scores and corresponding definitions.

Likelihood/Probability of occurrence Determination

Achieving an overall likelihood rating indicates the potential for potential vulnerabilities within the structure of the related threats' environment; the below control factors should considered:

- Threat capability
- Vulnerabilities' associated with threats
- Efficiency of existing controls.

Potential vulnerabilities may describe as high, medium or low by a particular behavior. The three possible levels described in the table below.

Level	**Likelihoods' Definition**
High (3)	The source of the threat is highly motivated and sufficient to protect the threats and vulnerabilities' from being invalid.
Medium (2)	The source of threats triggered but may delay the control of successful vulnerability implementation.
Low (1)	The source of threats' lack motivation or capacity, or control measures been taken to protect or at least significantly hamper the exercise of loopholes.

Table 7: Threats Likelihood

Impact Analysis/Impact score

Impact analysis ranks the level of impact associated with an organizations' critical information asset tradeoff based on a qualitative or quantitative assessment'. Information asset critical assessment identifies and prioritizes sensitive and critical organizational information assets that support the organization's mission-critical tasks. The following table describes the definition of the degree of impact:

The adverse effects of a security incident or events will described in terms of loss of any one or following three security objectives: "Confidentiality, Integrity, and Availability (CIA)". The following list outlines each security objective and its unmet consequences (or impact).

Loss of Confidentiality - Data confidentiality means protecting information from unauthorized disclosure. Unauthorized disclosure of confidential information may include exposing customer contractual requirements, national security. It may results in loss of confidence & action against the organisations'.

Losses of Integrity -Integrity refers to the requirement of data to protect assets' from improper configuration changes. If IT systems unauthorized to changes through intentional or unintentional actions, integrity will be lost. Continued use of contaminated systems or corrupted data may result in inaccurate, fraudulent or erroneous decisions if system or loss of data integrity is not corrected. In addition, breach of integrity may be the first step to successfully attacking for the critical information.

Loss of Availability - If end user is not able to use critical information systems, the daily operation tasks may be harm. For example, loss of system functionality & operational effectiveness can result in losses' of production time, thereby preventing users' from performing their functions to support the business.

The impact of potential vulnerabilities that can occur for a given threat source can be described as high, medium, or low. The three impacts' level described in the following table.

Level	**Impact Definition**
High (3)	Vulnerability exercise (1)High cost or high cost loss that may result in significant tangible assets or resources; (2) Serious violations that may damage or impede the organization's mission, reputation. (3) It may result in death or serious injury.
Medium (2)	Exercise vulnerability (1)The cost of tangible assets or resources may be high; (2) may violate, damage or obstruct the organization's mission, reputation or interests; (3) May cause personal injury.
Low (1)	Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources or (2) May noticeably affect an organization's mission, reputation, or interest.

Table 8: Threats Impact

Risk Rating

For the risk analysis process, risk parameters are considered based on intensity levels or impact on assets. In addition, to assess it, a scale measures the risk. To measure risk, a risk level and risk level matrix was developed. The following sections represent the standard risk-rating matrix:

Risk Level Matrix

The task risk is ultimately determined by multiplying the ratings assigned to threat likelihoods (probabilities) and threat impacts. The table below shows how to determine the overall risk rating based on the threat likelihood and the input of the threat impact category. The matrix below is the 3 x 3 matrix of threat possibilities (high, medium, low) and threat effects (high, medium, low).

Risk level scale = Threat likelihood * Threat Impact

The sample matrix in Table below shows (**refer to Annexure II**) how the overall risk levels of High, Medium, and Low are derived. The rationale for this justification can explained in terms of the probability assigned to each threat likelihood level and a value assigned to each impact level. For example,

- The probability assigned to each threat likelihood level is 3 for High, 2 for Medium,1 for Low
- The value assigned for each impact level is 3 for High, 2 for Medium, and 1 for Low.

Threat Likelihood	**Impact**		
	Low (1)	**Medium (2)**	**High (3)**
High (3)	Low (1 X 3 = **3**)	Medium (2 X 3 = **6**)	High (3 X 3 = **9**)
Medium (2)	Low (1 X 2 = **2**)	Medium (2 X 2 = **4**)	Medium (3 X 2 = **6**)
Low(1)	Low (1 X 1 = **1**)	Low (2 X 1 = **2**)	Low (3 X 1 = **3**)

Table 9: Risk Scale Matric

Risk Scale: High (>6 to 9); Medium (>3 to 6); Low (1 to 3)

The risk scale is calculated with its ratings of High, Medium, and Low, represents the degree or level of risk to which an IT system, facility, or procedure might be exposed if a given vulnerability were exercised. The risk scale also presents actions that senior RMC (Risk Management Committee), the mission owners, must take for each risk level. Below table describes the Risk definition and necessary action:

Risk Level	**Risk Description and Necessary Action**
High	If observations or findings assessed as high risk, corrective actions and controls are required. Existing systems may continue to operate, but corrective action plans must be taken immediately.
Medium	If the observation is rated as moderate risk, corrective action is required and a plan is in place to incorporate these actions in a reasonable amount of time.
Low	If the observation is described as low risk, the system owner must determine if corrective action is still required or to accept the risk.

Table 10: Risk Level

Risk Evaluation and Prioritization

The purpose of the risk assessment is to help determine which risks require treatment and treatment priorities based on the results of the risk analysis. Risk prioritization has been completed so that the identified risks are short-listed and require immediate attention from management.

IT Risk assessment involves relating the level of risk found during the analysis to previously discovered risk criteria and defining if the risk is acceptable. If the risk is in a lower or acceptable category, then further treatment can be minimized. These risks should be monitored and reviewed regularly to ensure they are still acceptable. If the risk is not a low or acceptable category, one or more treatment regimens should be used for treatment.

Once the risk is identified and assessed, the appropriate risk response options are identified and applied.

Risk Response

Risk response is the systematic process to bring the risk in line with the defined risk tolerance level of the enterprise. When the analysis shows risks deviating from the tolerance levels defined by the committee, a response needs to be defined. This response can be any of the four possible responses.

- Risk Avoidance
- Risk Mitigation
- Risk Sharing/Transfer
- Risk Acceptance

Risk Avoidance

Risk prevention is a risk response option that avoids activities or conditions that trigger a particular risk. Risk prevention shall apply if no other risk response is adequate.

This is the case when:

- There is no other cost-effective response that can succeed in reducing the frequency and magnitude below the defined threshold for risk appetite.
- Risk cannot be shared or transfer.
- The risk deemed unacceptable by management.

Risk Mitigation

Risk Mitigation is a method of controlling risk by implementing control activities that reduce or minimize the likelihood of a risk occurring prior to its occurrence

Implementing Controls

Prioritize Actions *– on the basis of risk levels presented in the IT risk assessment matrix, the implementation actions selected. In allocating resources, the top priority given to risk items with unacceptably high-risk rankings / high-risk level). This vulnerability/threat require immediate corrective action and mitigation strategies to protect bank payment system.*

Conduct cost-benefit Analysis - To aid management in decision-making and to identify cost-effective controls, a cost-benefit analysis is conducted.

Select Control – Based on the results of the cost-benefit analysis, top level management determines the most cost-effective control(s) for reducing risk. The controls selected combine technical, operational, and management control elements to ensure adequate security for the Information System associated with organisations.

Assign Responsibility - Appropriate persons (in-house personnel or external contracting staff) who have the appropriate expertise and skill-sets to implement the selected control identified, and responsibility assigned.

Implement Selected Control – Organize resources and implement selected controls

Risk Sharing/Transfer

Risk Transfer is a risk response option to reduce risk frequency or impact by transferring or sharing the risk such as insurance or outsourcing.

Risk Acceptance

Risk Acceptance means that no action is taken in relation to a particular risk and the loss is accepted when / if it occurs. Accepting the risk assumes that the risk is known, i.e. that the management has taken an informed decision to accept it as such.

Risk Communication

The results of the risk analysis and evaluation shall be reported to management in order to support the business function and to make risk-aware business decisions so that appropriate risk response options can be used. Decision-makers are made aware of the worst-case scenarios and most likely scenarios, significant reputation, compliance status, legal or regulatory considerations.

Risk Action Plan

Risk Action Plan is the course of action to mitigate identified analyzed, evaluated and prioritized risks. Based on prioritized risk reaction, duties, timeline, expected outcome, cost impact, the risk action plan is created. Implementation of the action plan is frequently tracked and timely reporting of progress reports and deviations to leadership. **Annexure III** shows the Risk/Threats Action Plan Template.

Risk Monitoring and Incident Response

Monitor the general IT environment for any security breaches that are in place and follow the incident response plan to restrict the timely impact of the violation and incident. Communicate the results of the incident to the business impact decision-maker.

REFERENCES

1. Anna Sapienza, P. S. ,. K. L. S. D. ,. E. F. ,. B., 2017. Early Warnings of Cyber Threats in Online Discussions. *IEEE International Conference on Data Mining Workshops,* pp. 667-674.

2. Bouveret, A., 2018. Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment. *IMF Working Paper ,* pp. 1-28.

3. Cavelty, M. D., 2014. Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities. *Sci Eng Ethics,* pp. 1-15.

4. David Airehrour, N. V. N. ,. S. M., 2018. Social Engineering Attacks and Countermeasures in the New Zealand Banking System: Advancing a User-Reflective Mitigation Model. *Information,* pp. 1-18.

5. Kautish, S. (2008), “Online Banking: A Paradigm Shift”, E-Business, Vol. 8, No.10, pp. 5459.

6. Kautish S. 2013. Knowledge sharing: A contemporary review of literature in context to information systems designing.,Academia 3(1). The South Asian Academic Research Journal: 101-113.

7. Kautish, S., & Thapliyal, M. P. (2013). Design of new architecture for model management systems using knowledge sharing concept. *International Journal of Computer Applications, 62*(11), 27–30.

8. Elena Sitnikova, M. A., 2014. A Strategic Framework for Managing Internet Security. *International Conference on Fuzzy Systems and Knowledge Discovery,* pp. 947-955.

9. G.NIKHITA REDDY, G. R., 2014. A STUDY OF CYBER SECURITY CHALLENGES AND ITS EMERGNING TRENDS ON LATEST TECHNOLOGIES. pp. 1-5.

10. jang, j., 2014. A survey of emerging threats in cybersecurity. *Journal of computer and system sciences,* pp. 973-993.

11. Mohamed Al Kilani, V. K., 2016. An Overview of Research Methodology in Information System (IS). *Open Access Library Journal ,* 3(2333-9721).

12. Solms, J. F. v. N. a. R. v., n.d. Research Methodologies in Information Security Research: The Road Ahead. *Research Methodologies in Information Security Research: The Road Ahead.*

13. Stephen A. Ojeka, E. B.-C. E.-O. I. E., 2017. Cyber Security in the Nigerian Banking Sector: An Appraisal of Audit Committee Effectiveness. *International Review of Management and Marketing ,* 7(2), pp. 340-346.

14. Vlasta Svatá, M. F., 2011. IS/IT RISK MANAGEMENT IN BANKING INDUSTRY. *IS/IT RISK MANAGEMENT IN BANKING INDUSTRY,* Issue 0572-3043, pp. 42-60.

15. Wu He, X. T. ,. J. S. ,. Y. L., 2015. Understanding Mobile Banking Applications’ Security risks through Blog Mining and the Workflow Technology. *Security Risks Associated With Mobile Banking Applications ,* pp. 1-10.