Framework for Minimizing Cyber Security Issues in Banking Sector of Nepal

Rupendra Maharjan[1] and Jyotir Moy Chatterjee[2]

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

ABSTRACT

Banks have become increasingly relying in recent centuries on the latest information-based IT schemes that maintain their wealth in the type of data opposed to traditional companies, where physical money and securities are placed in a safe and secure area. Banks have become the component of internet and daily lives. It is a real task to protect these bank procedures, systems from the attackers and minimize the security threats. With this Cyber-attacks increasing day by day, and this is the challenge facing by countries and organizations like banking where data is critical. Not only in frequency, but also in complexity, cyber threats are increasing. The number of cyber security attacks is increasing and becoming progressively destructive which is targeting and broadening the array of techniques and attack vectors. Most of these incidents could be prevented by implementing adaptable countermeasures promptly and minimizing risk. The goal of this research is to develop a framework to safeguard and minimize the cyber security issue that exists in banking sector of Nepal effectively and in a timely manner before cyber security incidents become a reality.

The core five elements of the National Institute of Standards and Technology (NIST) Identify, Protect, Detect, Respond and Recover is the baseline for the developing the framework for minimizing cyber security issues which will be fruitful in context to Nepalese environment.

This research presents the set of cyber security practices in minimizing the emerging risk and issue in Nepal. The developed framework will help control or avoid important corporate risk from delays in mitigation.

Keywords: Cyber Security, emerging threat, Minimizing security threat, Banking, Security tools

I. INTRODUCTION

An Overview

In Nepal there have been numerous cyber security violations in various sectors that are regularly on news portals. It was very risky, challenging and critical to cope the emerging cyber security issue in perspective of Nepalese environment. Despite of Nepal Rastra Bank (NRB) which is a regulatory bodies for directing and controlling the activities, due to lack of skill manpower and concrete cyber security law, policy and framework for reducing the cyber security threat, Nepal could not take the preventative and proactive measures against emerging cyber threat. For the country like Nepal, in order to understand the lack of a minimum risk of cyber safety in Nepal, it is essential to understand all the associated problems and concerns of the current cyber safety strategies. (Subedi, 2015).

Banking sector is the one of the target areas for c out malicious activities by the intruders. Several kinds are distinguished among common safety threats, based on the means and manner in which they occur, including malware, DDoS attacks, IP communications threats, phishing, vulnerabilities exploits, botnets, mobile phone threats, social networking threats and spam. All of these security threats violate one of the following characteristics; Confidentiality, Integrity and Availability.

Background

Attempting to defend banking against security threats continues to be an increasingly difficult issue, involving advanced technologies and approaches to unpleasant adversarial objectives. It is doubtful that organizations in existing business networks have the capacity or funds to identify and protect an opponent in order to obtain access to their networks and structures against every technique. Even if the company patching and software enforcement program of an organization are ideal, an opponent can leverage zero days or a social engineering attack to achieve a foothold on the network. (Strom, et al., 2017)

Threat Landscape against banking sector

ATM attacks

While investments continue to be made by ATM suppliers and banks for the security, ATM attacks are still growing. This is primarily due to the existing legacy safety checks for ATMs. Many ATMs are still running on Windows XP or Windows 7, which is vulnerable and has very few security controls, like using Endpoint Detection and Response (EDR). ATM attacks in the banking sector continue to grow every year, although they slowed down with the advent of Chip and PIN. Attacker are still trying to Gain access to the ATM network through a sophisticated cyber-attack on the financial institute.

POS attacks

In general, ATM and POS attacks are comparable, but actors take distinct approaches to threats. The reason for this is that end-customers visiting a retail store, bank, or insurance branch are intended to reach POS equipment. These POS systems typically have almost no security controls that are physically available. Threat actors therefore attempt to plug into these POS systems a malicious portal drive while no one is looking.

Distributed Denial of service

The distributed denial of service is one of the most common attacks of all kinds with easy but very strong attack systems and poses an enormous risk to the banking industries today where the services in number one priority. Besides banking, political organizations, stock exchanges and governments are seen as the major targets of DDoS.

Ransomware

The banking and finance sector is the frequent target of ransomware, which encrypts the data and demands for the random money for decrypting the data. Dyre, Dridex, Wannacry and Ramnit are botnets included especially for the banking sectors. Xbot used in Australia and Russia for stealing online banking details where as WannaCry ransomware was reported to have infected more than 200,000 computers in over 150 countries in May 2017 (Kumar & Khan, 2018).

Spear Phishing

Phishing messages provide a way to obtain access to organizations ' databases by promoting staff to press malicious connections or attachments. Generally spear phishing emails are tailored to specific person and organization which make the email looks more genuine and valid. Despite the use of awareness campaigns and phishing simulations, bank employees remain vulnerable to phishing emails. Banking sectors are increasingly under threat from attackers attempting to infiltrate their networks by exploiting the behaviour of human users. One means by which this can be achieved is via targeted, fraudulent emails, which aim to persuade employees to click on malicious links, download malicious attachments or transfer organisational funds or other sensitive information. (J.Williams, et al., 2018).

Aim of the Research

To analyses the cyber security issues related to banking sector of Nepal and to propose a novel framework for minimizing the cyber threat.

Research Objectives

Following are my objective of this research which is to:

- To analyze various emerging threats in cyber security in context to Nepal.
- To examine current practices, tool and techniques being used in order to prevent security threats.
- To propose a well-defined framework for prevention from security threats.

Research Question

- How do we proactively defend against security threats to minimize the impact?
- Why do we need to understand the emerging cyber threats to defend against them?

- How to mitigate cyber security issues in Nepalese banks proposing well standards framework?

Scope of the Research

While the scope of this research is quite large, the research focuses on the emerging cyber threats and the threats seen on financial and government bodies in Nepal, where the impact is very high. This research will identify the security threat faced and define the framework in context of Nepal relating with comprehensive global response to cyber threats. There will be no discussion on various anti-piracy, copyright violation and protection of intellectual property.

Significance of the Research

The output and finding from this research with result in providing a common organized approach in managing and reducing the security issues. Organizations can realize and identify existing vulnerable areas and loop holes which can be secured.

This study has the following significance for different parties. These are:

- The study shall serve as a guideline for minimizing the cyber security issues (attacks) in banking industry in Nepal.
- It enables all banks to follow a common framework
- It adds a new way of thinking in the existing body of knowledge.
- It also helps for practitioners and researchers to conduct more comprehensive research in minimizing and mitigating cyber security incidents in Nepal.

Limitation of the Study

The result of the research would be more comprehensive if it covers the entire Banks and their branches in Nepal. However, due to time constraints study was only focused on headquarters of selected commercials banks in Nepal. As the size of the Nepalese banking sector is relatively small only 28 commercial bank banks were taken into this research study.

II. REVIEW OF LITERATURE

This chapter reviews previous research in field of minimizing the cyber security issues and attack vectors particular. It begins by providing background knowledge for the reader on the topic, starting from the terms Social engineering, Vulnerabilities, Cyber security attacks in banking sector and moving on to phishing and other types of attacks. Furthermore, it illustrates current practices and mechanisms cyber security frameworks along with the emerging security challenges. Also, Reviews mitigations and security monitoring strategies for business protection and support for a banking security defense strategy, since the research focuses on minimizing the security issue.

Cyber Security and Threats

The more thorough look at one of the common attack steps and its dependence on certain system access pieces, system knowledge and/or attack skills'. In accordance with the attack step definition, the exact nature of the preconditioned dependence and the attack result is specified. The Figure below show the attack execution steps where it reveals' the overall structure of possible attack surfaces or paths', but the creation of an executable model to simulate adversaries' a system attack requires more in-depth information on every attack step. (Cherdantsevaa, et al., 2016)

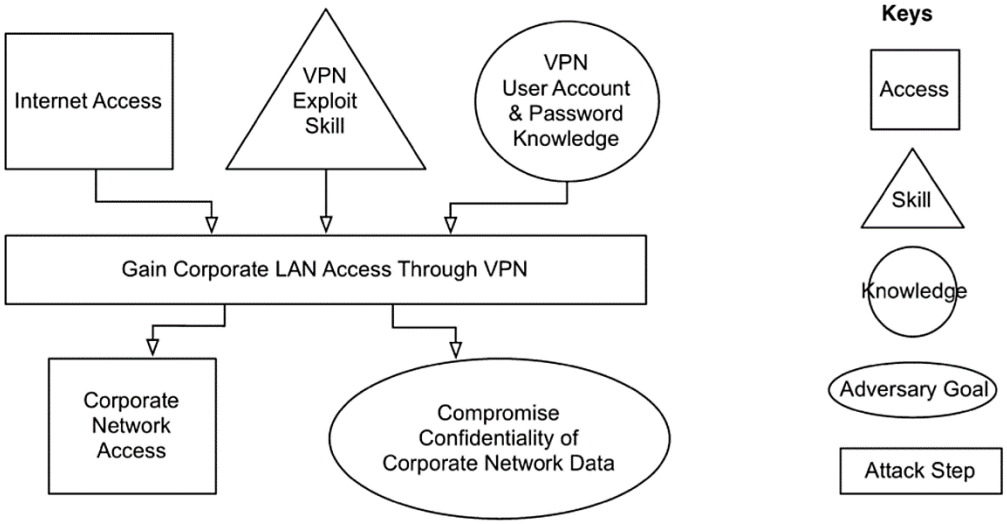

Figure 1 An attack step (Cherdantsevaa, et al., 2016)

There are three areas in which assets are protected by cyber security.

- Confidentiality – Protecting sensitive information from being accessed.
- Integrity – Preventing assets from being modified or destroyed.
- Availability – Ensuring that assets can be accessed by authorized parties.

Threats can be activities that can cause adverse harm to an asset of an organization. Cyber threats in particular cause harm to software, hardware or data. A common method for categorizing threats was created by Microsoft called STRIDE (Muckin & Fitch, 2019)

- Spoofing – Impersonating someone
- Tampering – Modifying the system or its data
- Repudiation – Disputing who performed a specific action
- Information Disclosure – Accessing sensitive information without proper authorization.
- Denial of Service – Preventing authorized users from fully accessing a resource
- Elevation of Privileges – Gaining privileges without proper authorization

Policies and frameworks for compliance drive actions where the list of checks is considered compulsory. These control lists comprise instances of prospective checks and are the consequence of long-term threats and vulnerability analyzes and assessments by the industry itself. If these lists are considered to be the main cause of cyber security design or evaluation operations, they blind or prevent an organization from applying measures that effectively protect and defend the property in the specific environment of the organization.

Cyber Security Frameworks

Although there are several risk models and framework that directly attempt to address the cyber security issue and challenges, NIST released a comprehensive guidance on a wide range of security issues, and technical, operational and management security controls. The NIST Cyber Security Framework defined by international cyber security framework standard define core five components of cyber-security for a defense strategy (National Institute of Standards and Technology, 2014).

1. **Identify**: Continuous cyber threat identification, evaluation, and governance using techniques of management and risk assessment best practice.
2. **Protect**: Structured, solid integrated safety architecture, perimeter network protection, host protection, network protection, device protection and remote connectivity safety.

3. **Detect**: The ability to identify viruses and other cyber annoyances, as well as advanced cyber-attacks like APTs both within the network and within the scheme, and on each recipient.
4. **Respond**: Well established and effective cyber-attack management procedures.
5. **Recover**: Ability to return to normal or degraded operations quickly following an attack–the defense part after the fact, in depth. It is not feasible to avoid or react to certain cyber-attacks. Mostly, APTs and other disastrous assaults are cyber-attacks with an extremely small chance of occurrence and have a strong effect.

According to Juniper network whitepaper (Latha, 2016), attackers knowledge and understanding of technology have increased which is any enterprise network can be attacked easily. The above figure illustrates the frequency and sophistication of cyber-attacks. The knowledge an attacker needs to know about enterprise network in order to launch a sophisticated attack is decreasing. This means sophisticated attacks are growing more severe each day (Delmee, 2016).

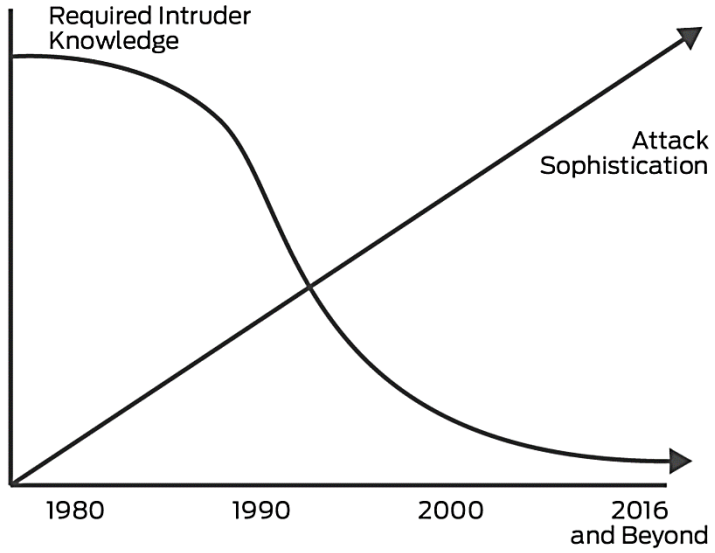

Figure 2 Attack Sophistication vs. Intruder Technical Knowledge

The breaking Down Threat and Behaviors is provided by MITRE ATT&CK. This is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. CHAPTER

III. RESEARCH METHODOLOGY

The guide to any research is the research methodology. Information and data are research lifeblood. Methodology for studies is the strategy for obtaining a study response by analyzing primary data.

This chapter contains research methodology used for achieving the objectives set for this study. In this section, it is discussed about the Research design, sample size, data analysis procedure, tools and techniques, validity and reliability of data.

Research Design

The study layout is, in reality, the conceptual framework underlying study; it represents the blueprint for information compilation, evaluation and evaluation. This research adopts a mixed-methods research methodology. A mixed-methods research caters both qualitative and quantitative approaches (Denscombe, 2012). Since cyber security issues are the complex and interdependent topic of threats, attacks and vulnerabilities, mixed research methods will achieve this goal. Qualitative and quantitative research supports the understanding of the problem or develops ideas. Some methods that are prevalent include focus groups

or organizations, personal surveys, and participation / comments. Typically the sample size is tiny and participants are chosen to finish a certain quota.

In order to get the desired output the selected methodology must well-matched with the research problem and objective. As for the research topic in minimizing the cyber security issue in Nepal the quantitative approach will greatly help as this approach will draw the larger participants and responses.

Sample size and Data Analysis Procedure

Data of this study were collected from two sources. The Sample size for this research was comprise of the entire person belonging to or associated with Banking professionals and IT Sector of Nepal. They were IT professionals, Audit Risk, Compliance, Network and system administrators and Security Officers. Questionnaires. First of all these sets of questionnaires were developed and distributed to respondents. Distribution was done personally through the online survey medium and field visit for the hardcopy offline questionnaire. Secondary data were collected from published reports of different organizations. Questionnaire for 300 users were distributed through the online survey and field visit to different types of respondent i.e were IT professionals, Audit Risk, Compliance, Network and system administrators and Security Officers of the commercial banks of Nepal between the fixed period and only 112 responses were received including online and hard copy. In order to fulfill the objectives of the study, 100 valid samples from the data collected from online survey and offline questionnaire were selected.

Presentation and Analysis of data/ techniques and Tools

After data and information are collected, they are tabulated and presented in the tabular from. After this, different statistical tools are used to analyze those collected data & information to draw the result/conclusion of the research work. The data are collected according to the subject matters. In this research the bibliography have been first on the basis of available literature, journals, reports

and data. Then the accumulated literature, reports and data were reviewed and tabulated accordingly with the objectives. The techniques included are statistical tools, tables, bar diagrams, pie charts, simple average, percentage and others tools as needed to obtain the result.

Tools used:

- Microsoft Excel 2013
- IBM SPSS Statistics Version 25

Validity and reliability of the data

Because quantitative and qualitative instruments are used in this study, accurate information are highly possible. Besides the additional data collected through questionnaire also help to make data more reliable and valid. Limitations may arise, as it could not represent all the respondent and participants as the limited samples are taken. Since major of the bank and IT operations are centered.

Analysis of literature and sources of information

To identify academic papers on the developing the framework for minimizing the cyber security issues, following search will be carried out for papers in the archives like IEEE Computer Society Digital Library, ACM Digital Library, Springer Link, Access Engineering Emerald Insight, Google Scholar, , Science Direct and other journal publishing websites.

A qualitative sampling technique will be used to obtain the sample for the articles selected to conduct the qualitative phase of this study.

The search for Journals, articles and reports will be carried out later than 2014 using the search terms but not limited to “cyber security issues”, “minimizing the the security issue with framework”, “cyber security

framework", "framework for minimizing security issue is developing country" and "how to reduce security threats".

Source of data collection will both primary and secondary as follows:

Table 1 Data collection sources

Primary	**Secondary**
Interviews	Journals
Field observation	Reports
Online Survey and Questionnaire	Books
	Data availed from Internet sources

Interview, Online survey and questionnaire will be one of the data collection instrument for this study. Different government and non-government organization will be interviewed. Similarly Online questionnaire and survey will be divided into different section such as personal data, need/ objective, problem, solutions and opinions etc. through available survey portals like google forms or survey monkey.

Then instrument will be structured in the modified on a 5 – point scale, ranging from

"Strongly disagree" (SD), "Disagree" (D), "Neutral" (N), "Agree" (A), "Strongly agree" (SA)

The data collected from the field observation which are then statistically weighted average of the online questionnaire was used to answer the questions of studies. Response options are weighted in the instrumental tool as shown below.

Table 2 Likert scaling

Likert Option	Likert Option	Points
Strongly disagree (SD)	**Don't know**	1 Points
Disagree (D)	Never	2 Points
Neutral (N)	Very rarely	3 Points
Agree (A)	Sometimes	4 Points
Strongly Agree (SA)	Frequently	**5 Points**

IV. PRESENTATION AND ANALYSIS OF DATA

Presentation and analysis of primary and secondary data is very important stage of any research study. Its main purpose is to change the unprocessed data into understandable form. It is the process of organizing the data by tabulating and then placing that data in presentable form by using various tables, figures and source. Data and information were collected from different sources. To achieve the stipulated objective, collected dates are analyzed and interpreted. Collected primary and secondary data are analyzed using the statistical tools and techniques.

In this chapter all the statistical background required to perform an effective data analysis is described. This chapter focuses on analysis of our data variable, with method developed by R.A. Fischer. Analysis of variance is used to measure the differences among means. The "analysis of variance" is abbreviated as ANOVA

(Fischer, 1954). The formulation of a hypothesis and its effective validation is also explained in this chapter. In fact, this chapter determines findings of the research and helps to fulfill research objectives.

Analysis of Primary Data

A Primary Data Analysis has been conducted in order to find out various aspects of security practices and threats in the banking organization. The major tool used for this purpose is an opinion survey through a set of structured questionnaire. Questionnaire for 300 respondent are distributed through the online survey and field visit to different types of respondent i.e were IT professionals, Audit Risk, Compliance, Network and system administrators and Security Officers of the commercial banks of Nepal between the fixed period and out of 112 responses were received including online and hard copy. Out of which only 100 valid samples were taken for further data analysis. The responses received from these respondents have been arranged and inputted on the SPSS tool where all the frequencies and correlation are generated, tabulated and analyzed in order to facilitate the descriptive analysis of this study.

The survey was carried out in commercial banks which is of different size, age, position and experiences which is shown in the table below along with the bar diagram. The survey questionnaire were later categorized into Threat identified, Perception of individuals, Tool and Practices. These categories were used for generating the correlation with each other.

SPSS Statistics Output of the one-way ANOVA

With the respondents results SPSS Statistics generates quite a few tables in its one-way ANOVA analysis which compares three or more unmatched groups, based on the assumptions. ANOVA is based on the assumption that the data are sampled from populations that all have the same standard deviations. (GraphPad Software, 2014)

Later, we have generated the descriptive table, as well as the results for the one-way ANOVA and will go through each table in turn.

P value

P value is the statistical value generated which is used for testing the hypothesis with identical means that is generated from all groups are drawn from respondent. The information do not show any reason to assume that the mean is different if the total valuation of P is high. Even though the respondent had the same means. If the total P is low, the difference found is unlikely to be due to random sampling. The P value is derived from the from the F ratio which is calculated through the ANOVA table.

ANOVA table

ANOVA divides the variability between all the values into one element. Variability within groups is quantified as the sum of squares of the distinctions between each value and its mean group.

The 'F ratio' is the ratio of two mean square values. If the hypothesis is true, we expect value of F close to 1 where as a large F ratio means there is a variation among group means. (Drummond & Vowler, 2012)

Analysis of Security Perception on the basis of Age

The following table describes the mean and standard deviation for the variable Security Perception for each separate age group (20-30, 31-40, 41-45 and above 45), as well as when all groups are combined (Total). This tells us that, on average, respondent aged between 31-40 and 41-45 has the good perception on the banking security. For both all age group, the mean are all similar, which is a good indication that the data are equally distributed. The spread of scores as shown by the Std. Deviation is a higher for age group 31-40, suggesting that age group 31-40 have good perception on security than any other age group. The Std. Error. Is fairly low which suggests that if the study is repeated, we are likely to get the almost same results..

Table 3 Descriptive analysis of security perception on the basis of age

Security Practice

	N	Mean	Std. Deviation	Std. Error	Minimum	Maximum
20-30	43	22.0233	1.98192	.30224	18.00	26.00
31-40	44	20.6364	2.22136	.33488	11.00	25.00
41-45	8	20.8750	1.24642	.44068	19.00	23.00
above 45	5	20.4000	.89443	.40000	19.00	21.00
Total	100	21.2400	2.10396	.21040	11.00	26.00

Table 4 One way ANOVA by the factor age

ANOVA

Security Perception

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	47.006	3	15.669	3.845	.012
Within Groups	391.234	96	4.075		
Total	438.240	99			

One way ANOVA analysis is shown on the table above, which indicates the significant difference between our group means on the basis on organization size. We can see the significance value is 0.012 (i.e., p = .012), which is below 0.05. Therefore, there we can state the statistically significant difference in the perception on security on banking sector with respect to the age of the respondents.

Here the responded aged between 31-40 and 41-45 has the good perception on the banking security.

Security threats by size of organization

The following table describes the mean and standard deviation for the dependent variable Security threats for different size of banking organization, as well as when all groups are combined (Total). This tells us that, on average, organization sized between 1-50 has the greater number of threats and other mean for different size of organization are similar, which is a good indication that the data are equally distributed and the spread of scores as shown by the Std. Deviation is a 15.09 for organization size 1-50 followed by 12.24 for organization size 51-200, suggesting that organization with lower employee size have greater security than large organization. The Std. Error. Is fairly low which suggests that if the study is repeated, we are likely to get the almost same result.

Table 5 Analysis security threats by size of organization

	N	Mean	Std. Deviation	Std. Error	Minimum	Maximum
1-50	7	60.8571	15.09336	5.70475	34.00	74.00
51-200	29	47.2759	12.24715	2.27424	37.00	76.00
201- 500	13	54.3077	8.91052	2.47133	44.00	72.00
501-1000	20	46.1000	9.69482	2.16783	37.00	69.00
1001 and above	31	51.5806	7.89841	1.41860	34.00	66.00
Total	100	50.2400	10.93333	1.09333	34.00	76.00

Table 6 One way ANOVA by the factor organization size

ANOVA

Security_threats

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	1657.472	4	414.368	3.868	.006
Within Groups	10176.768	95	107.124		
Total	11834.240	99			

One way ANOVA analysis is shown on the table above, which indicates the significant difference between our group means on the basis on organization size. We can see the significance value is 0.006 (i.e., p = .006), which is below 0.05. Therefore, there we can state the statistically significant difference in the Security threats faced by organization according to their size. The above tables shows that the average score of threats in an organization size 1-50 has the had highest score

Analysis of Security Practice by level of employee

The following table gives descriptive statistics including the mean and standard deviation for the dependent variable (Security practice) for different level of employee, as well as when all level of employee are combined (Total). This tells us that, on average, manager level of employee has the good security practices with the mean of 88.16 followed by Officer Level of employee with the mean of 79.88 and other mean for different level of employee are similar, which is a good indication that the data are equally distributed. The spread of scores as shown by the Std. Deviation is a 14.60 for officer level followed by 10.92 for manager lever, suggesting that higher level in banking sector has the good security practices than the junior level

The Std. Error. Is fairly low which suggests that if the study is repeated, we are likely to get the almost same result.

Table 7 Analysis of security practice by level of employee

	N	Mean	Std. Deviation	Std. Error	Minimum	Maximum
Assistant	22	79.5909	5.60322	1.19461	65.00	85.00
Supervisor	17	76.4706	10.22324	2.47950	67.00	100.00
Officer	30	79.8667	14.60216	2.66598	62.00	117.00
Manager	31	88.1613	10.92428	1.96206	57.00	108.00
Total	100	81.8000	11.91383	1.19138	57.00	117.00

Table 8 One way ANOVA by the factor level of employee

ANOVA

Security_Practice

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	1956.786	3	652.262	5.177	.002
Within Groups	12095.214	96	125.992		
Total	14052.000	99			

One way ANOVA analysis is shown on the table above, which indicates the significant difference between our group means on the Security Practice by level of employee. We can see that the significance value is p = .002, which is below 0.05. and, therefore, shows statistically significant difference in the Security Practice by level of employee. The above tables shows that the average score of Security Practice by officer level has the had highest score .

Analysis of Security Perception and Security practice

The Pearson Correlation generates a coefficient of variable correlation, r, which measures the power and direction towards of linear interactions between variables. By expansion, the Correlation evaluates whether there is statistical proof of a significant connection among the same pairs of factors in the different variable.

Table 9 Correlation of security perception and security practice

Correlations

		Security_Perception	Security_Practice
Security_Perception	Pearson's correlation	1	.275**
	Significance (2 tailed)		.006
	N	100	100
Security_Practice	Pearson's correlation	.275**	1
	Significance (2 tailed)	.006	
	N	100	100

1. Correlation of Security Perception with Security Perception (r=1), where the number of valid respondent for Security Perception (n=100).
2. Correlation of Security Perception and Security Practice (r=0.275), among n=100 respondent and non missing values.
3. Similarly, Correlation of Security Practice and Security Perception (r=0.0.275), among n=100 respondent.
4. Correlation of Security Practice with Security Practice (r=1), where the number of valid respondent for Security Perception (n=100).

The correlations in the *Right diagonal* (1 and 4) are always equal to 1 as a variable is always correlated perfectly with itself. Also the sample sizes in cell are same A (*n*=100) versus cell D (*n*=100). *Right diagonal* (2 and 3) shows correlation between Security Practice and Security Perception and its p-value.

Sig (2-tailed) value indicates that the correlation between two variables is statistically significant, here Significance (2 tailed) value is 0.006 which is less than less than or equal to .05

We can state the following on the basis of the outcomes:

- As p (.006 < .001) Security Perception and Security Practice statistically significant and positively correlated. That means, increases or decreases in Security Perception do significantly relate to increases or decreases Security Practice and vice-versa.
- The relationship is positive (i.e., Security Perception and Security Practice are seen positively correlated), which means that these variables tend to increase together.
- The magnitude, or strength, of the association between Security Perception and Security practice is weakly positive .275 (r | < .5) means according to security perception, security practice is not performed in the banking sector.

Analysis of Security Practice and Security threat

Table10 statistics of security practice and security threat

Descriptive Statistics

	Mean	Std. Deviation	N
Security_Practice	81.8000	11.91383	100
Security_threats	50.24000	10.933333	100

Table 11 Correlation of security practice and security threat

Correlations

		Security_Practice	Security_threats
Security_Practice	Pearson's correlation	1	.418**
	Significance (2 tailed)		.000
	N	100	100
Security_threats	Pearson's correlation	.418**	1
	Significance (2 tailed)	.000	
	N	100	100

1. Correlation of Security Practise with Security Practice (r=1), where the number of valid respondent for Security Practice (n=100).
2. Correlation of Security Practice and Security threat (r=0.418), among n=100 respondent and non-missing values.
3. Similarly, Correlation of Security threat and Security Practice (r=0.0.418), among n=100 respondent.
4. Correlation of Security threat with Security threat (r=1), where the number of valid respondent for Security threat (n=100).

The correlations in the *Right diagonal* (1 and 4) are always equal to 1 as a variable is always correlated perfectly with itself. Also the sample sizes in cell are same A (*n*=100) versus cell D (*n*=100). *Right diagonal* (2 and 3) shows correlation between Security Practice and Security threat and its p-value.
Sig (2-tailed) value indicates that the correlation between two variables is statistically significant, here Significance (2 tailed) value is 0.000 which is less than less than or equal to .05
We can state the following on the basis of the outcomes:

- As p (.000 < .001) Security Practice and Security threats are statistically significant and positively correlated. That means, increases in Security practice do significantly relate to Security threat. Despite of security practices there is increase in the security threat. Hence more security practices need to be implemented in current scenario.
- The magnitude, or strength, of the association between Security Practice and Security threats is weakly positive .418(r | < .5) means security practice is not according to the security threats in the banking sector.

Analysis of Security perception and Security Threat

Table 12 Correlation of security perception and security threat

Correlations

		Security_threats	Security_Perception
Security_threats	Pearson's correlation	1	-.283**
	Significance (2 tailed)		.004
	N	100	100
Security_Perception	Pearson's correlation	-.283**	1
	Significance (2 tailed)	.004	
	N	100	100

1. Correlation of Security threat with Security threat (r=1), where the number of valid respondent for Security threat (n=100).
2. Correlation of Security threat and Security perception (r=-.283), among n=100 respondent and non-missing values.

3. Similarly, Correlation of Security perception and Security threat (r=-.283), among n=100 respondent.
4. Correlation of Security perception with Security perception (r=1), where the number of valid respondent for Security perception (n=100).

The correlations in the *Right diagonal* (1 and 4) are always equal to 1 as a variable is always correlated perfectly with itself. Also the sample sizes in cell are same A (*n*=100) versus cell D (*n*=100). *Right diagonal* (2 and 3) shows correlation between Security Perception and Security threat and its p-value.
Sig (2-tailed) value indicates that the correlation between two variables is statistically significant, here Significance (2 tailed) value is 0.004 which is less than less than or equal to .05
We can state the following on the basis of the outcomes:

- As p (.004 < .001) Security Perception and Security threat statistically significant and positively correlated.
- The magnitude, or strength, of the association between Security Perception and Security threat is weakly negative= - .283 (r | < .5) means security practice tends to decrease the security threats.

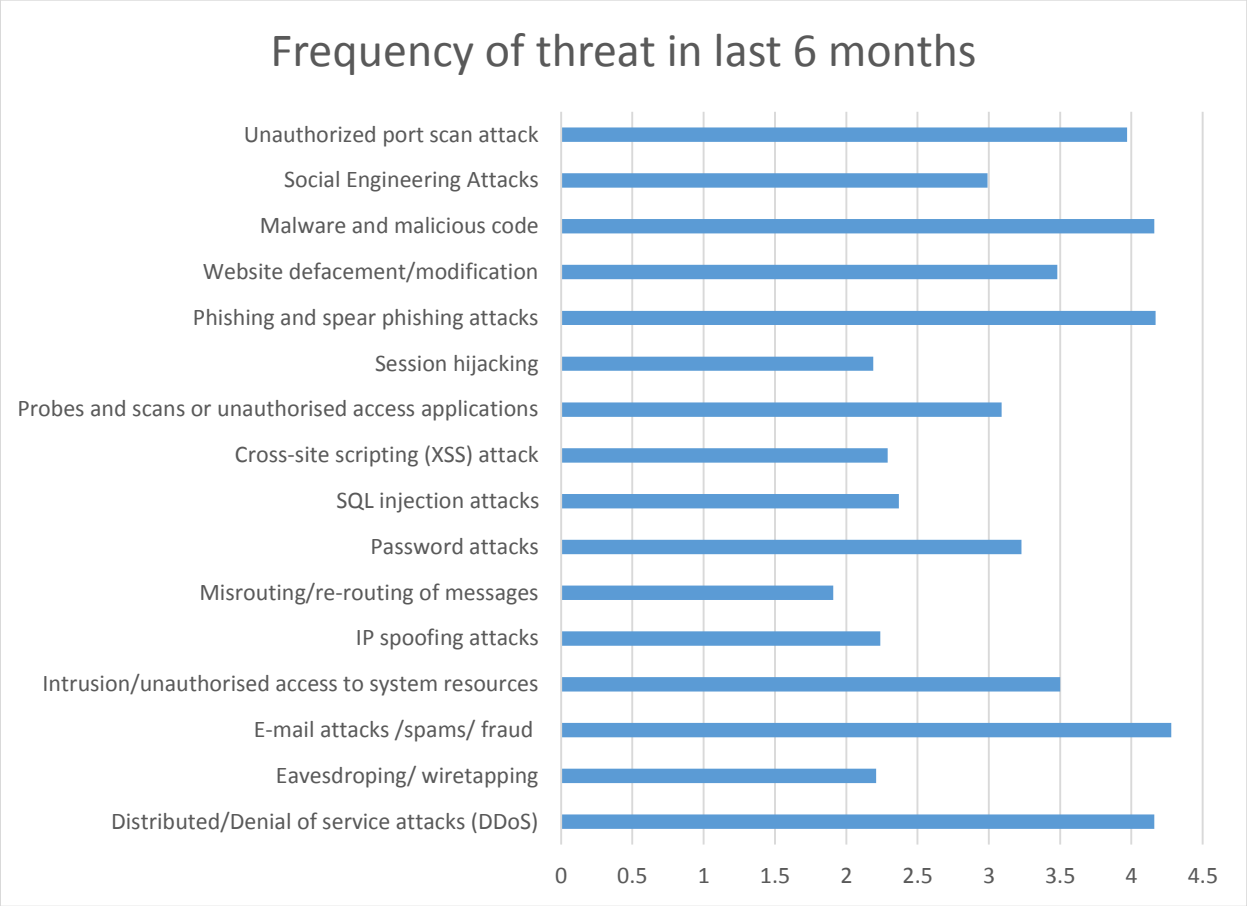

Figure 3 Graphical representation of different attacks in banking sector

The respondent were asked the likert question Don't' know, Never, Rarely, Sometimes, and Frequently for the threats that is seen banking sector in past 6 months. As the chart above Figure 24 shows, Phishing, Email attack is the most frequent threat for the banking organizations, followed by malware/malicious code and Distributed denial of services. Also it is seen that unauthorized port scan and access to system resource is occurred frequently. Among the incidents most of them were seen as the outsider threat with the network medium as bank's services are accessed by customers over the internet.

As we can see in Figure 25 more than 60% of respondent answered for unauthorized port scan attacks in the banking network which is the first stage of any major attacks through scanning the vulnerabilities and reconnaissance whereas more than 80% of respondent answered for DdoS attacks in last 6 months. These data shows the bank's networks is being regularly scanned and targeted by the intruders through the public faced network which need to be more secured.

V. FINDINGS, CONCLUSIONS AND RECOMMENDATIONS

Major Findings

This section provides finding for the banking industry in particular and especially for the banking industry in Nepal. Based on the study findings described in the thesis, the study goals outlined in chapter one are evaluated and their accomplishment discussed. Finally, suggestions are being suggested for future job. Finally, the researchers' ultimate and most significant objective is to list the results of the research and to provide recommendation which is provided in this chapter.

Recommendation

Conceptual framework

Communication and network protocols include large components of the cyber-attack landscape. Therefore, many threats are directed at the networks or communication channels of people, systems and devices. As we have already seen, therefore, there are many techniques of attack and instruments intended to exploit prevailing vulnerabilities in networks and channels of communication. A striking reality about these targeted attacks is that in order to be effective, cyber attacker also depend on human vulnerabilities within the directed organization. Since the ability and technology of cyber attackers is rising and the effects of impaired banking structures can be great, it is vital to evaluate the danger.

Although the focus of this study is on banking sector, other kinds of financial organizations also affect the danger of targeted attacks due to vulnerability of human behavior as well as vulnerabilities in networks and channels of communication. In this chapter we discuss and present framework that covers the techniques behind targeted attacks, vulnerabilities, and mitigating measures and to develop a generic technique for assessing susceptibility in order to minimize the security threats for the banking sectors of Nepal. Conceptual framework has been defined below along with the further actions:

Discover and Identify threat

Conduct Assessment on the Asset inventory

It is essential to store your data assets and guarantee that you are protected when preparing for the threat. Bank need to define its data resources, including hardware, software, computer systems, services and any other technological resources associated List the assets in a table, then use the words critical, vital and normal to weigh need to be given accordingly.

Identify threat Source and events

The threat source need to be identified which may be Individual like Insider, Outsider, Trusted Insider, Privileged Insider , Group or Organization like Competitor, Supplier, Partner, Customer and - Nation-State. Any trigger that seek to exploit the organization's dependence on resources'

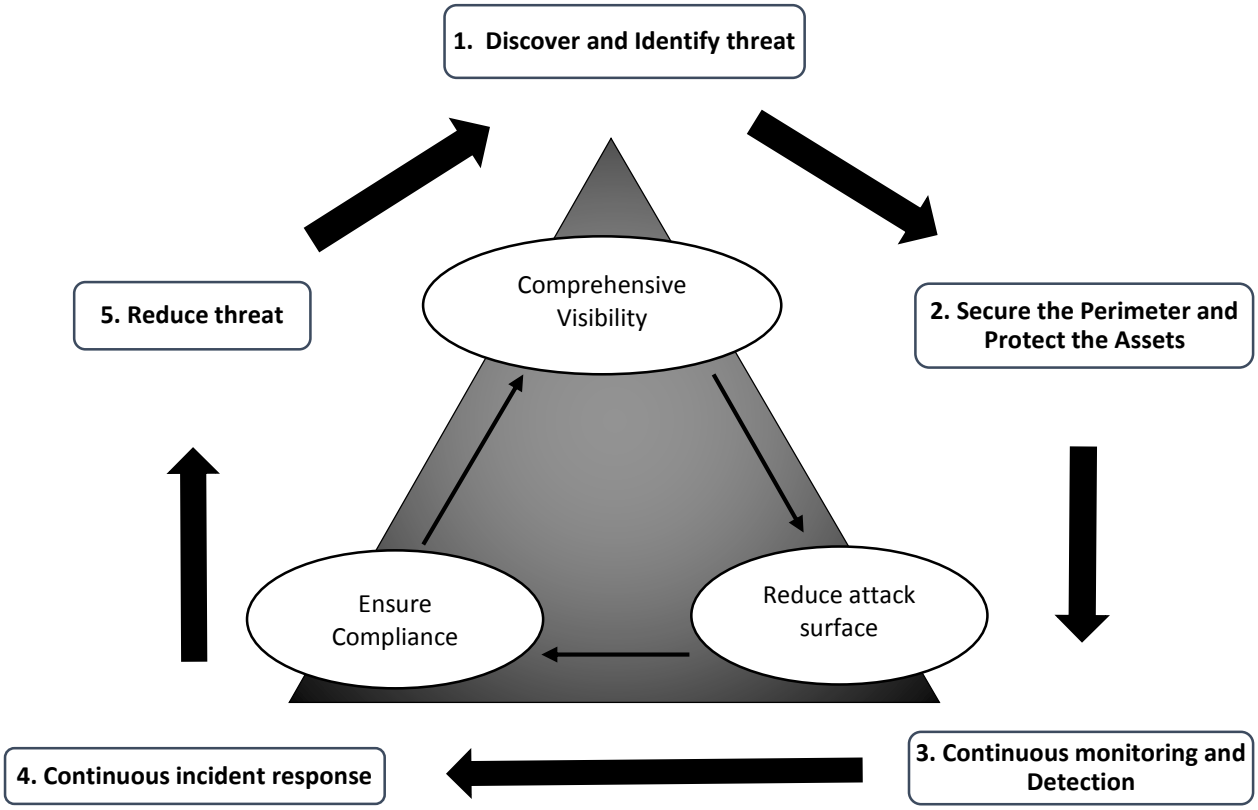

Figure 4 Framework for minimizing the threat

Identify Vulnerabilities

Vulnerability is a weak spot in your network or system that might be exploited by a security threat. Some of the risks related with that vulnerability could be loss of data, site downtime, data breach or even crash. Banks need to identify all the vulnerabilities that exists on the system and network.

Vulnerability assessments are used to gain insight into banks security deficiencies. “Similar to the way an attacker may use reconnaissance techniques to assess the vulnerabilities of a target’s network, the bank can greatly benefit from the same actions”. This can be achieved through regular (Vulnerability assessment and penetration testing) VAPT tools and practices.

Determine threat likelihood, Impact and Risk

Determining threat identification in a risk analysis identifies the exposure of an bank towards threats. Bank can perform a threat-oriented approach which will focus on the threat sources and possible threat events. These events will be interpreted into threat scenarios that provide the vulnerabilities as well as the impact of these events. The threat-based approach recognizes the threats by looking at all the possible risks.

Four categories of information about this agent should be gathered: its skill level, its motive, the opportunity, and the Capacity (OWASP, 2019) provides an approach to rate the threat on one of three categories.

1. Attackers must have the motivation to attack
2. They must identify a target
3. Ability to launch an attack

For the bank to predict a potential threat, All parameters gathered by the attacker have to be related to each other . The motivation, opportunity and capacity all the three variables must relate all parameters collected by the attacker to each other profiles and technical sources where each factor gets an evaluation value as follows.
Low (1-2), Moderate (3-4) , and High (5-6) .

Table 13 Risk Scoring

Motive	Opportunity	Capability		
		Low	Moderate	High
Low	Low	2	3	4
	Moderate	3	4	5
	High	4	5	6
Moderate	Low	3	4	6
	Moderate	4	4	7
	High	5	6	8
High	Low	4	5	7
	Moderate	5	6	8
	High	6	7	9

Securing the Perimeter and Protecting the Assets

Securing the perimeter in order to protect assets can be a very broad, still a robust IT perimeter security plan will demonstrate bank's security architecture, technologies in use and established processes, which can prevent cyber-attacks and quickly detect and react when they occur.

Network segregation and Firewalls

In the inner network, systems or user credentials can be damaged, particularly when using internet access, e-mail service apps, and customers who can communicate with them. If critical banking assets are not in the same network, there will be no compromises to the component. Furthermore, it can only assist safeguard rogue devices from being accessed by registered devices in the network and banning access in the internal network for the unregistered network equipment. Internal and External firewall need to be in place for blocking unauthorized access to networks and control incoming and outgoing network traffic.

Limiting open interfaces

Limiting the workstation's open interfaces can be viewed as a securing the perimeter and protecting the assets and also a basis for hardening. Bank's system should have a minimum open interfaces. The mobile workstations, which can also be used in unprotected fields, must be shielded in such a manner as to prevent any disastrous failures, even if they end up in the incorrect hands. It is possible to protect data in workstations. First, it is necessary to keep the information minimal. Second, it should be ensured that it takes sufficient time to open the workstations without credentials, so that the operation's safety is not compromised.

Least privilege principle and hardening

Least privilege is a basic method behind the ideology of the hardening and protecting. Everything that is not necessary for completing the job should be blocked out and closed in the banks. Limiting system access on a necessary basis including the separation of responsibilities could reduce even a zero-day exploit to a minimum when the banking system has been adversely affected.

REFERENCES

1. Cherdantsevaa, Y. et al., 2016. A review of cyber security risk assessment methods for SCADA systems. *elsevier,* Volume 56, pp. 1-27.
2. Delmee, F., 2016. *THE STRUCTURE OF A CYBER RISK A SCENARIO BASED APPROACH IN CYBER RISK ASSESSMENT,* Netherlands: Deloitte.
3. Denscombe, M., 2012. *Research Proposals: A Practical Guide.* 1st ed. Berkshire: McGraw-Hill Education (UK).
4. Drummond, G. B. & Vowler, S. L., 2012. Analysis of variance: variably complex. *he Journal of Physiology,* pp. 1303-1306.
5. Fischer, R., 1954. *Statistical Methods for Research Workers.* 12th ed. Edinburgh: Oliver & Boyd.
6. GraphPad Software, 2014. *GraphPad Statistics Guide,* s.l.: GraphPad Software Inc.
7. J.Williams, E., JoanneHinds & N.Joinson, A., 2018. Exploring susceptibility to phishing in the workplace. *Elsevier,* Volume 120, pp. 1-13.
8. Kautish,S. 2008, "Online Banking : A Paradigm Shift", E-Business, Vol. 8, No.10, pp. 5459.
9. 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.
10. Kumar, N. & Khan, P. R. A., 2018. Ransomware Evolution, Target and Safety Measures. *International Journal of Computer Sciences and Engineering,* VI(1), pp. 80-85.
11. Latha, M. K., 2016. *Learn About Intrusion Detection and Prevention,* s.l.: Juniper Networks.
12. Muckin, M. & Fitch, S. C., 2019. *A Threat-Driven Approach to Cyber Security,* s.l.: Lockheed Martin Corporation .
13. National Institute of Standards and Technology, 2014. *Framework for Improving Critical Infrastructure Cybersecurity,* s.l.: NIST.
14. OWASP, 2019. *OWASP Risk Rating Methodology.* [Online] Available at: https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology [Accessed 20 July 2019].
15. Strom, B. E. et al., 2017. *Finding Cyber Threats with ATT&CK-Based Analytics,* s.l.: The MITRE Corporation.
16. Subedi, D. R., 2015. *Cyber Security Situation in Nepal.* [Online] Available at: https://www.enepalese.com/2015/07/32099.html [Accessed 02 01 2019].