INFORMATION TECHNOLOGY
COLLEGE OF MANAGEMENT &

Submitted by:

ISHWOR KHATIWADA

Submitted to:

Lincoln University College

Year/ Semester: 1st Semester/1st year

LCID: LC00017000772

Date: 03-07-2020

Q.n.1. Suppose you are appointed as an IT head of XYZ Bank of Nepal. Every day you are encountered with different cyber threats. Prepare a case report about different possible threats you encounter during your day to day official work and solutions to minimize their effects.

TABLE OF CONTENT

INTRODUCTION:

Banking sector is one of the major place where there involves major financial transactions.It is more likely that there possibly occur a lot of cyber-attacks and hacking activities. Direct handling of 100 to 1000's of customers daily on the one hand is issue on management whereas on the other hands security is also major issue concerned with all of it. Various types of banking, mailing software's from various vendors are deployed in bank with all these there exists various security concerns. Similarly various devices which runs from internet like computer, mobile, attendance, security devices and smart-devices etc. They are less secure and have to look up for their entire configuration and all the security concerns as well. Threats may come from various sources like email, spam ware, malicious links, and interconnection of various mobile devices to system, spyware, hacking and password sharing, and so on. Being IT head it is the major responsibility to lookup for all of these and everyday prepare for all such issues mostly be familiar with such issues and way to reduce vulnerabilities. Various tools and devices like firewall and VPN must be strictly implemented whereas specific permission to user group in ERP system must be ensured. Besides that wireless network also should be secured in different branches and should be secure and only useful sites must be given permissions to browse.

On the other hand, when it comes in getting secured with the customer's data and information there must be a secure permission to browse by bank staff whereas regular change in password and strong password policy must be implemented.

VALNURABILITIES AND CYBER THREATS

A cyber threat is a malicious act that generally seeks to harm data, steal data or disrupt digital life. Cyber threats include computer viruses, data-breaches, Denial of Service attacks (DoS) and other various forms of attacks. Various sector and industries are at high risk of various cyber threats and attacks. As the number of internet or smart devices user are increasing day to day the number of malicious software and application are increasing. In other hand Vulnerability is a defect that a malware offender may abuse to obtain unauthorized access to or conduct criminal activities on a computer network. Vulnerabilities may allow attackers to execute code, access memory of a system, install malware and steal, destroy or modify sensitive data and so on. Both of these are most challenging security concern in banking sector. Banking sector is the busiest industrial sector that directly involves financial transactions so security plays a vital role in this industry. Management of transaction in both digital form and hand cash involves high security. It head is responsible for all the security concern with all the devices used in banking institution like computer printers, attendance devices, cameras, and many network devices. Threats like computer viruses are most common in software that we use in daily uses for data entry to other purposes.so reduce the risk we use software from authorized platform and limit the installation from administrator only to any computer on the network.

POSSIBLE CYBER CRIME IN BANKING SECTOR

The emerging world of cyber-threats is under demand from banks and financial services firms. They generally operate on vast volumes of valuable customer and financial data. That's why knowing what there's to say about the latest security risks is crucial to keeping us secure from hackers. Various cyber threats that exist on banking sector are explained:

a.) Credential stuffing:

Credential stuffing is a kind of cyber-attack that typically attacks banking client's personal information. Hackers may obtain unauthorized access to user accounts using automatic large-scale authentication requests, utilizing stolen account passwords. The compromised information would also be used to target websites and networks so that connections to sensitive IT resources can be obtained.

b.) Phishing:

Phishing is a intensively growing method of cyber-attack used to steal data from consumers, including login credentials and credit card numbers. Lately, though, there has been an rise in phishing attacks against bank workers from the data of 2019. Phishing occurs when an intruder fools an unwitting user into opening a malicious connection, which leads to malware infection that then freezes the device as part of a ransomware attack.

c.) Ransomware

Ransomware in the context is a form of malware that encrypts data, rendering it difficult for the owners of the data to access it until they pay a ransom fee. Banks remain top targets for ransomware attacks, as cybercriminals chase the money for major payoffs. Cybersecurity figures reveal that attacks have been initiated in over 190 nations, with financial services becoming the second most attacked after health sector.

d.) Malware

End consumer machines that have been hacked by malware – such as laptops and mobile phones – present a danger to the information protection of your bank any time they link to your network. Sensitive data passes through this link and if, without proper protection, the end-user computer has malware installed on it, the malware may target the networks of your bank.

e.) spoofing

Spoofing is a newer type of cyber security threat-where hackers will find a way to impersonate the URL of a banking website with a website that looks exactly the same and works. When a user enters his or her login information, the hackers then stolen that information for later use. More specifically, modern spoofing methods do not use a slightly different but identical URL-they are capable of attacking users who have accessed the same URL,as a bank or financial company. It is important to consider strategies to minimize the risks to your cyber protection while also being able to provide easy, technically innovative solutions to customers.

EFFECTS OF CYBER CRIME IN BANKING SECTOR

The banking industry across the globe is facing a challenging situation which is thought provoking due to the geopolitical and global macro-economic conditions.The banking industry is required to evaluate the existing activities in order to better identify and handle their threats. Technology-driven solutions to risk control have been embraced. The financial services have spread to millions because of the development of IT, the proliferation of cell networks in daily life. Technology has ensured that banking services touch masses because it has made such services available and affordable. However, this also raised the possibility of cyber-attacks being targeted.

Cybercriminals also developed sophisticated strategies not only to trigger knowledge regarding stealing in money and assets, but also to spy on firms and obtain sensitive financial information that indirectly influences the financing of the corporation. Globally, almost every year, USD 114 trillion is destroyed owing to cybercrimes, and the expense of combating cybercrimes is twice that number. On average, banking facilities take 10 days to recover completely from a cyber attack which adds further to operational costs. Comparing the financial risks the neplease banking industry suffers, it constitutes approximately 1.5 percent of cash loss relative to global risks. Recovering from the incident, USD 2 billion is wasted and USD 1.5 billion is expended on preventing these crimes in the future. The average period taken in the neplease banking sector to address the crime is also higher as comparison to the global scenario.

SOLLUTIONS

With the growing cyber-crime threat and increasing institutional liability, there is no other option for banks but to be proactive logic made all the more certain given that more than 30 percent of successful hacks are committed by employees or related persons. However, contrary to conventional thinking, any bank taking the lead in enacting a first-line of defense needs to start with Senior Management, not the Information Technology (IT) Department. The concern, commitment, and control of management are critical to adopting, funding, and enforcing an effective protection scheme that may be fully implemented in the workplace. That is not to say that internal IT or contract technology personnel have no role to play, but simply directing IT personnel to install a firewall or regularly change passwords would not be a cure-all. Like any other form of corporate security from sign-in sheets to identification badges to biometrics. it only takes one motivated person dedicated to breaching a system's weakest point to overcome a seemingly impenetrable chain of protection. A bank simply cannot afford to make the mistake of deploying anything less than a comprehensive top-down strategy to enable a reliable system of computer network security.

Generally, a bank's goal is to adopt a customized set of procedures and practices that enable control to be exercised over critical information and technology assets in a cost-effective manner. A Software Institute categorized a comprehensive approach to physical, technical, and administrative security controls as follows: preventive (i.e., secure card readers, encryption, spyware, and company policies and procedures); detective (i.e., archival seals, log messaging controls, and regular e-audits); deterrent (i.e., closed circuit cameras, rejection after incorrect password use, and multi-departmental approvals); corrective (i.e., isolation of servers, updated firewalls and procedures, segmentation of space by function); and recovery .With the growing cyber-crime threat and increasing institutional liability, there is no other option for banks but to be proactive.

CONCLUSION:

A bank, therefore, needs a broad strategy of prevention. None method can protect a bank against all types of cyber-crimes and cyber-enabled perpetrators. Because of the high-level of risk in banking related to cyber-criminal activities, banks must maintain constant vigilance and diligence to be aware of the risks, assess and priorities the risks, and take appropriate actions to mitigate the risks. One of the general issues in the development of cyber-laws is the nature of cyber-space itself, which is new and young. Traditional laws, thus, will not be effective in tackling the various types of activities conducted on the cyber-space. For example, deception of computer, or theft of electronic data cannot be dealt with under the traditional penal laws in many countries. That is why certain countries like India, Malaysia and others began to enact the new "Information Technology Act" and "Digital Signatures Act," respectively. The other issue is jurisdiction of the courts and applications of the laws due to the nature of the cyber-space beyond national jurisdiction. In order to survive and grow in a global competitive scenario, time has already come when the security aspects of the banks must be dealt with on a priority basis.

Q.N.2

"Internet has revolutionized Banking Services and has made payments and fund transfer easy via online payment gateways". Critically analyzed the statement and give examples to support to your answer.

SOLLUTION:

The creation and access of internet has opened new horizons and scenarios for the retail banking industry. The retail banks are now providing their products and services through the electronic medium like Internet-banking. E-banking is considered to have a substantial impact on banks performance. The evolution of electronic banking (e-Banking) started with the use of automatic teller machines (ATMs) and has included telephone banking, direct bill payment, electronic fund transfer and online banking. According to some, the future direction of e-banking is the acceptance of mobile telephone (WAP-enabled) banking and interactive-TV banking. However, it has been forecasted by many that online banking will continue to be the most popular method for future electronic financial transactions.

As technology is now considered as the main contribution for the organizations success and as their core competencies. So the banks, either domestic or foreign are investing more on providing on the customers with the new technologies through e banking. PC banking, mobile banking, ATM, electronic funds transfer, account to account transfer, paying bills online, online statements and credit cards etc.

By the help of online payment system we can make payment go cashless and travel anywhere and buy anything with digital wallets. In Nepal from past 5 years digital payment wallets have been tremendously increasing and the people are becoming proactive with them. Some of the reknown payment partners are:

Khalti Digital Wallet: It is one of the online wallet which is directly associated with bank, theater, shopping mall, internet service provider and other many organizations.. E.g. we can pay electricity, television, internet payments on time . khalti digital wallet helps for mobile top up and fund transfer easily in effective way by synchronizing with bank.

E-sewa: E-sewa is almost like Khalti Digital Wallet. Features of e-sewa and khalti are same. Whereas e sewa is almost more easy to use and has connected with government bodies like electricity authorities and many other institutions. It is considered as pioneer of digital payment system in Nepal.

I-PAY: same as e sewa and khalti I pay also is a digital wallet offering same services and is mostly familier among fuel suppliers like petrol diesel as it has connected with government bodies of fuel association to provide easy payment in fuel and has good offers.

IMPACT OF E BANKING ON TRADITIONAL SERVICES:

The current issue is the view that the Internet is a revolution that will sweep away the old process of satisfying the customer and need of instant solution. In traditional system customer have to wait a long day in a queue to get paid and deposit.

•E-banking transactions are much cheaper than branch or even phone transactions. This could turn competitive advantage to customers and banking institutions and also reduces effort to reinsure to the payment.

•E-banks are easy to set up so lots of new entrants will arrive. Old-world systems, cultures and structures will not encumber these new entrants. Instead, E banking gives consumers much more choice much more freedom and facilities.

•E-banking will lead to an erosion of the bank deposit. Deposits will go elsewhere with the consequence that these banks will have to fight to regain and retain their customer base. This will increase their cost of funds, possibly making their business less viable. Lost revenue may even result in these banks taking more risks to breach the gap.

RISKS IN E- BANKING:

- STRATIGIC RISK: with e-banking services and evaluate the resulting risk management costs against the potential return on investment Prior to offering e-banking services. Poor e-banking planning and investment decisions can increase a financial institution's strategic risk.
- Business risks : Business risks are also significant. The banks will not be able to measure the business risk as it will be new to the bank. Banks may face certain difficulties in providing their basic services such as credit, deposit, transfer and other services.
- Security Risk:

  Running a e-banking service is not that easy. It has to lookup for all the security concerns applications vendors and device compatibility and server and many more other things.

CONCLUSION: The electronic banking is gaining more importance by the passing time. The electronic banking services provided by the banks include ATM, credit cards, funds transfer, cheque payment, funds deposit, balance enquiry, utility bills payment, statement of account, remittance, draft, pay order, phone banking, mobile banking, PC banking etc. The introduction of e banking has changed the banking environment. Digital wallets have been gaining more and more importance. The manual banking was a lengthy and time consuming procedure, there was manual maintaining of the accounts and transactions for which the accuracy was damaged due to human errors, labour cost was considerable as a result digital wallet are gaining much more popularity with minimal functions. digital wallet are gaining much more popularity that some banking institution, group institution are also lunching their own payment app which is a replication of international payment gateways.