Improve Data, Security & Training at JP Morgan Chase

Submitted to
Dr. Asila Sayedi

Submitted By
Manideep Batchu
California University of Management and Sciences

Abstract

Information systems security is one of the major issues for companies that handle sensitive information such as financial institutions and JP Morgan Chase is no exception. Despite the company making efforts to reinforce its information systems with new technology, it still faces problems such as poor system maintenance, lack of skilled personnel and outdated software and hardware. In order to solve these problems, the company will need to implement certain recommendations to ensure there systems are as safe as possible from cyber criminals. This research focuses on creating solutions or possible solutions that the company may implement using various avenues to ensure maximum results. Through review of various secondary sources, the study creates detailed explanation for each recommendation along with its implementations. In order to achieve the goals of the study, a SWOT and porter's analysis has been applied in the study. The SWOT analysis helps create a picture of the current status of JP Morgan Chase. On the other hand, the porter's analysis creates an assessment of the competitive environment of the company and helps plan for future growth as well as challenges. Through the study, JP Morgan will find recommendations to help solve their current issues of data security and also make it easier to project any future growth or issues that may arise as a result of the company's current issues.

I. INTRODUCTION

The issue of security breaches of information systems of companies is quickly growing at an alarming rate. Threats to systems security are progressing from the commonly known threats to more complex methods used by cyber criminals and it is becoming more and more difficult for companies to protect their information systems from such threats. As much as companies can put all their efforts and resources into anticipating security threats and preventing them, it is just not possible. Expecting to anticipate every systems security breach is impossible because threat agents only become actual threats when they are provided with vulnerability that they have the potential to exploit and the existence of vulnerability still does not guarantee that it will be exploited. It is therefore necessary for an organization to identify vulnerabilities that apply to their organization specifically and work towards those instead of working through a range of possibilities that may never affect them.

A. Problem statement

The main purpose of this research is to provide insight into ways through which JP Morgan can ensure the security of its information systems. Some of the problems identified at JP Morgan include:

- Lack of regular systems maintenance
- Lack of skilled personnel
- Vulnerable and outdated systems

B. Purpose of the project

The project will focus on JP Morgan Chase which was recently a victim of data security breach and look into problems at the company that caused the breach and ways that it can avoid a repeat of the same.

a. Lack of regular systems maintenance

Regular system maintenance is one of the things that companies overlook because of the costs associated with it but ends up costing them much more when they are compromised. Many IT departments are faced with many challenges due to the work they are expected to accomplish with very limited budgets which results to system maintenance being pushed to the bottom of the to-do list. When it comes to IT, one cannot secure a single element and leave out the rest. Maintenance must be done starting from the hardware, operating systems, databases and applications because it only takes a single vulnerable link to bring an entire information system to a halt. Instead of approaching system maintenance using a quick-fix approach, companies should look at software security as a broad and long-term process.

The costs of regular software maintenance may be high but is nowhere close to the costs that companies incur after a security breach. These companies lose many of their customers as they no longer trust in the companies' ability to safeguard their confidential information. The reputations of these companies are ruined and are forced to undergo serious PR campaigns to regain the public's trust. Considering such factors may help companies realize just how important and necessary regular system maintenance is and plan for it. It is extremely important at this time when security breaches are becoming increasingly common and more sophisticated by the day. Regular software maintenance will assure customers and the company itself that there data is secure (Madden, 2013).

b. Lack of skilled personnel

The most common route for cyber criminals to enter company systems is through computers in the company and if the users of those computers are unaware, it makes the job easier for the hackers. A tactic commonly used by cyber criminals called spear phishing that involves sending phony emails that appear legitimate to random employees within the company is one method that has seen many companies fall victim to hacking because the employees are unaware of such things. Lack of skilled personnel leaves an open door for cyber attacks because they are clueless about factors such as improved password protection, malware or phishing. One click ends up wrecking havoc on an entire institution due to an employee's lack of knowledge.

It can be very dangerous to grant access to a company system to an employee without IT skills especially on data protection. Most hackers have improved their methods such that their attacks come in very innocent and seemingly legitimate ways and unskilled employees fall into these traps very easily. Investing in effective employee training can help prevent great disaster. Companies should also limit access to systems and only grant access to specific resources that employees need to do their job. Doing this limits the number of possible opening for cyber attacks as only very few highly-skilled employees will have special all-access privileges (Randi, 2015).

c. Vulnerable and outdated systems

Although most people understand the value of keeping systems updated, this task is often foregone due to the high costs associated with it. The use of outdated systems in the name of saving costs has proven to be a huge mistake for both small and large businesses that have seen their information systems compromised. Hackers put a lot of efforts in identifying vulnerabilities in systems particularly those in outdated versions that have not been updated. Updating outdated software ensures that any weak points are identified and reinforced to prevent hackers form using them to plant malware.

Old hardware brings with it new vulnerabilities for hackers to exploit. Most manufacturers of both hardware and software work under the assumption that their customers will update their assets to the latest versions as they come. The latest version are equipped with upgraded security features and once the new versions are designed and released, all the focus is put into making them better and the older versions receive less and less support or even none at all. It is difficult enough having to worry about cyber criminals creating windows of opportunity to hack without having to think that one could be compromised by simply using their hardware or software, just because it is outdated. The longer a technology asset has been available in the market and to the public, the longer cyber criminals had to identify their vulnerabilities which means users of such systems are less likely to have the ability to protect themselves from system security breaches. Considering all these may make the cost of acquiring new versions of systems more than worthy(Solutions, 2016).

II. Company overview

Background

JP Morgan Chase & CO is a global leading finance firm and one of the largest banking services provider in the United States, with operations in different parts of the world. The company has various clients ranging from governments, global corporations, institutional investors and individuals. The type of business JP Morgan deals with requires a lot of confidential information such as customer names, phone numbers, addresses and emails. In 2014, the company suffered a security breach in its systems which left over 76 million customers' information compromised (Silver-Greenberg, 2014).

For a company such as JP Morgan Chase which is in the finance industry, the issue of data security is very sensitive. The company holds confidential information to millions of consumers and any breach in its information system would have tremendous effects. The project will show how such breaches can be anticipated and prevented. In the case of JP Morgan, the breach was discovered a month later after it had started, a situation that would have otherwise been avoided. JP Morgan prides itself in holding its business to high standards through strengthening, growing and safeguarding the company. In order to uphold these standards, its systems should be reinforced to ensure that customers feel safe and believe in the company's ability to secure their information at all times.

IV. ANALYSIS

Analysis can be described as a detailed examination or assessment of the elements of something, mostly to be used as a foundation for interpretation or detailed discussion. This is the basis for understanding where a company's strength lies in order to recognize important strategies that need to be formulated to help achieve company goals and objectives (Cadle, 2010).

The main objective of this paper is to analyze issues that affect JP Morgan and how it can overcome them by making use of the opportunities and strengths that it has. These issues will be investigated using two analysis tools; SWOT and Porter's five forces analysis. The SWOT analysis is aimed at helping the management of the company identify internal and external factors that may affect the future performance of the company. On the other hand, the five forces analysis or porter's analysis will help give an insight into the forces that shape competition within the finance and banking industry. This will in turn ensure JP Morgan maintains its competitive edge. Through these two analyses, the company will be able to fix any weaknesses it may have and exploit its strengths in order to maintain or improve its position in the market and within the industry it operates.

SWOT Analysis

SWOT analysis or SWOT matrix is a structured framework or planning technique that is used to assess specific elements of a company; strengths, weakness, opportunities, and threats. Although it may look simple, SWOT analysis is a very useful framework if used effectively. It is a great tool that aids in informed decisions that can see a company escape many future challenges and emerge successful (Valentin, 2001).

Strengths.

This is the first part of SWOT analysis. Strengths of the business are those components that perform well and are under their control. The strengths of JP Morgan are as follows:

A leading provider of global financial services.

JP Morgan Chase is one of the largest banks in the United States and widely recognized globally for provision of financial services. The company has operations in over 60 countries and serves various customers comprised of individuals, governments, institutions and even businesses. JP Morgan Chase has built a financial brand name known for provision of various services such as asset management, security services, investment banking and hedge fund among others. The years the company has served in the fiancé industry makes it a trusted brand name.

Strong liquidity and capital

The liquidity and capital positions for JP Morgan Chase are very strong. Between the years of 2008-2013, JPMC's loans decreased while their deposits increased hence increasing the company's deposits-to-loans ratio to 174%. The company is also functioning really well in the areas of assets, sales, profits and market value.

Diversified revenue streams

JP Morgan Chase does not rely on a single source of revenue which is how it has been able to remain successful for so long despite changes in the financial market. The company has a diversified stream of revenue that arises from its various business segments which are: investment and corporate banking, asset management, commercial banking, consumer and community banking and corporate entity. All these areas ensure the continuous flow of revenue for the company no matter the situation of the market.

Good and effective management

The company obviously has good management which is able to run its large network spread out all over the world and still maintain exemplary performance and customer service. The company has over 250,000 employees across the world and is able to manage all of them effectively due to its experienced management team who use the best management styles to ensure maximum productivity with little supervision.

Weaknesses

This refers to areas that the company needs to work on to better its performance in now and also in the future. They include:

Over-dependence in particular markets.

JP Morgan is heavily dependent on the United States for the major portion of its revenues (more than 65%). Although it is a good thing that it has great results where it is based, this can greatly affect its performance as it makes the company vulnerable to any economic recessions in that market. Having a business depend too much on a particular market means it is more likely to suffer huge losses in case of any shifts in that market.

Fluctuating markets

Just like other businesses, JP Morgan Chase experiences the effects of fluctuating markets and suffers from lack of stability that is caused by fluctuations in the markets in which it operates.

Increasing expenses

In the recent years, JPMC’s expenses have shown an upward trend. The company’s operational as well as non-interest expenses keep increasing year after year. In 2013 alone, JPMC’s non-interest expenses made up around 72% of total net revenue.

Opportunities

Opportunities refer to areas that JPMC can exploit to enhance its performance. These include:

Growing the credit card market

The rate at which people all around the world are using credit cards keeps increasing by the day. The rate of credit card circulation is even higher in the United States and because of this, chase cards are also being used more. JPMC can also benefit from this growth.

Potential growth in asset management

Asset management as an industry is estimated to reach $102 trillion come 2020 with a compound annual growth rate of up to 6%. Considering how JPMC is performing currently in its asset management segment, it is bound to benefit from the growth in the asset management industry in the future if it maintains or even enhances its current performance.

Geographic expansion

People are always on the lookout for a good and reliable provider of financial services. JP Morgan already has a good reputation for reliable and custom-made financial solutions to cater to various customer needs. It would benefit JPMC greatly to expand its geographic reach to enable it to cater to more emerging markets hence increasing its market presence.

Threats

Threats comprise of any elements that hinder JPMC to reach its full potential. These include:

Regulatory Changes

Constant changing of regulations is a factor that affects many financial institutions and JPMC is no exception. Regulatory changes result in increased compliance costs which in turn affect operating margins. Considering JPMC has operations in over 60 countries, it experiences the effects that come with regulations of all these different countries.

Threat of financial crisis

A scenario where an economy faces a financial crisis greatly impacts financial institutions the most hence any recession is bound to affect JP Morgan Chase.

Instability of the Mortgage market

JP Morgan Chase operates and serves different clientele in the mortgage market which is notorious for instability. The high levels of instability of this business segment of the company mean that the company is also at risk and can cause great damage.

Competition

JPMC faces competition from other companies in the financial industry which pose a threat. Some of the company's major competitors include the Bank of America Corp (BAC), Citigroup Inc, Morgan Stanley and American Express Company; just to name a few. The company has to fight to stay above both its local and international competitors.

Five forces analysis (Porter's analysis)

Porter's five forces analysis is an analysis tool used to assess the competition of a business or company. According to Porter, the model draws from the five major forces that determine an organization's competitive intensity (Porter, 2008). An analysis of JP Morgan Chase based on Porter's five forces is as follows:

Competition from Industry Rivals

This is the strongest force for JP Morgan Chase. The company faces a lot of local and international competition from rival companies within the finance and banking industry. One of the elements that intensify competition among financial institutions is the relatively low switching costs particularly in commercial and retail banking. Along with that, major banks are continuously creating offers to attract customers to their banks. In order to stand out from its competition, JPMC attempts to stand out on the basis of its many years of experience and a recognized brand. The company's history of acquiring smaller banks also plays in its favor as well as its long-standing provision of affordable services that ensure customer convenience.

The bargaining power of customers

JPMC caters to various customers ranging from individuals, governments, institutions, and businesses. Individual customers, especially in retail banking, have little bargaining power since the loss of a single account will have a very minimal effect on the company's bottom line. However, on average, the bargaining power of customers is high because the bank cannot afford to lose many depositors. On the other hand, high net worth individuals or businesses have greater bargaining power due to their sizeable accounts whose loss would greatly affect the company's profit margins. JP Morgan attempts to handle this by frequently extending offers to potential clients. For the case of existing clients, they are encouraged to open additional accounts or buy more services which increase their switching costs hence making it costly for them to transfer to other banks.

The bargaining power of suppliers

The main suppliers of a bank are employees who offer labor and depositors who supply capital. Like shown in the negotiation power of customers, individual depositors, unlike corporate depositors, have little bargaining power but as a whole, they have great bargaining power. In attempts to handle this force, JP Morgan Chase works tirelessly to bring in new clients and increase the capacityin which existing clients hold funds and buy services through JPMC. In the case of employees who provide labor, although ordinary employees with lower positions have little bargaining power compare to executive employees, the company must work to address its overall bargaining power by providing appealing salary and benefit packages to motivate their employees and retain the best.

The threat of substitute products

In past years, it was a belief that companies in the banking industry were not experiencing the effects of this force but this is not the case today. The threat of substitute products has become an increasing cause for concern as more and more companies outside the banking industry have started to offer financial services that were originally only accessible from banks. Some examples of such substitute products include prepaid debit cards, Apple Pay, PayPal and online peer to peer lenders such as LendingClub.com. Intrusion from these products has seen JP Morgan and other financial institutions suffer huge losses. In order to minimize this threat, JPMC has created initiatives that support elements such as small business lending, and even created its own digital wallet service known as Chase Pay.

The threat of new entrants

As a force in the banking industry, the threat of new entrants is quite a small one. A threat can only be significant if a company sets to compete directly with JP Morgan or any other major banks in the United States. It is also difficult for new companies to pose a significant threat since customers in this industry go for something they know and trust. They are more likely to go for a company like JP Morgan, which has been in the industry for more than 15 years. For a company to compete in this industry effectively, it must spend a lot of money which means it must be making a lot too which favors JP Morgan as it has a high revenue rate due to its diversified revenue streams and global operations. Another obstacle for new entrants is the numerous government regulations that apply to financial institutions. Although JP Morgan may not experience threats in the industry at this time, the company should prepare for future competition from developing economies. Currently, the company gets to make maximum use of the opportunities it has to expand its market presence and create more consumer-friendly products and services that will see its brand continue to rise for years to come, with or without new entrants. These will increase its stability in any market that the company chooses to venture into in the future.

V. RECOMMENDATIONS AND IMPLEMENTATIONS

After review of various resources such as journals and websites, the researcher identified three main problems faced by JP Morgan Chase. It was clear that JP Morgan faces issue on system maintenance. The training of the personnel was also minimal within the organization as well as the development of a schedules system upgrade for their software updates. Within the advancing information technology industry the three problems will lender any company into challenging operation period. In an attempt to solve these issues, this project designs three recommendations and three implementations for each recommendation.

These are the recommendations that can help secure JP Morgan’s information systems:

- Regular system maintenance.
- Training personnel on data security.
- Upgrading all outdated software.

The recommendations named above aim at creating ideas on how JP Morgan can further secure their information systems to avoid any future system security breaches. It also places JP Morgan in a more competitive position in the market. These recommendations are each explained further together with their implementations as follows:

Regular System Maintenance

Through an increase in the number of times that system maintenance is done. Consistent maintenance services on software by IT experts will ensure that any unauthorized activity going on is spotted and stopped immediately. Failing to conduct regular maintenance services is what saw JP Morgan get compromised. The hack began in June but was not identified until July. That is a very long time to have a company's system opens to hackers. The hackers had ample time to go through and copy sensitive data concerning the company's operations and also that of its customers. The rate at which technology is growing only makes breaches more likely to occur since cybercriminals also upgrade their tools hence the need for vigilance and regular maintenance (Adeoye, 2012). For this recommendation to be useful, the following implementations must take place:

i. Training employees on the importance of doing system maintenance regularly.

Employee training on the importance of carrying out system maintenance regularly will ensure accountability together with responsibility for everyone in the company. Training of employees should include assessments done by experts to determine areas of vulnerabilities that employees should watch out for. Additionally, these assessments will allow all the departments to create new policies for incidence response, should a breach occur. Having formal procedures will reduce the impact of a security breach, and allow everyone involved to act immediately, without uncertainty about the correct steps to take (Crosman, 2016).

ii. Setting aside resources for system maintenance.

System maintenance requires funds since it is not a cheap affair. Therefore, setting aside resources for system maintenance ensures they are not foregone no matter what. Just like any other project in a company, system maintenance should be treated with the same seriousness and budgeted for. JP Morgan Chase should implement effective ways for fund allocation that will enable system maintenance to be done on a regular basis as opposed to when they are affected with cyber-attacks (Jiang, 2006).

iii. Policy design on system maintenance.

There are different policies that a company can formulate to ensure efficient system maintenance. For the case of JP Morgan, this can be done by implementing two policies: to protect and proceed as well as to pursue and protect. Through regular system maintenance, JP Morgan Chase will be in a position to detect attempts of cyber-attack or still the company will be in a place to acknowledge that there was an attack on their system. Protect and Proceed strategy should be used by JP Morgan Chase anytime they fear that their systems can be attacked. After the management of the company detects these attacks, they should actively impede penetration of the intruder, prevent further infringement, and start immediate damage evaluation and recovery. Secondly, the company should implement and Prosecute strategy whose only aim will be to permit invaders to continue accessing the system until they are known and have a proof regarding their unauthorized activities gathered against them. JP Morgan Chase should, however, take precaution, with this strategy because their system and information will still be open to prospective damage when the company is again attempting to unmask the attack source (Mohammed, 2015). Apart from regular maintenance, employees should be trained on other methods to ensure data and general system security.

Personnel training on data security.

Apart from IT experts within an organization, all personnel in a company should receive training on data security. One of the most significant risks for companies is not the technological part of the environment, but the action of unskilled employees that may result in security breaches. For training to be adequate, it is crucial to base instruction on employees' job functions. Various topics on security of information systems can be included or expanded on depending on the levels of responsibility and roles that each employee has in an organization. Some of the ways that can be used to create security awareness include formal training, memos, notices, emails and bulletins among others. In order to increase the efficiency of training, the security awareness program or training should be included in the hiring process so that new employees joining the company are trained too (Council, 2014). Some of the main issues that can be implemented to help achieve this recommendation include:

i. Investing in effective training methods and trainers.

The best practices for system maintenance can best be implemented in the company through effective training by top information technologists in order to ensure maximum results. Employees at JP Morgan Chase should undergo a thorough training on cyber-attack. The company should first launch written policies regarding data security then communicates them to each employee. Next, they are supposed to get skills on types of information that are confidential or sensitive and their obligations regarding the protection of data (Siponen, 2010).

ii. Set guidelines for appropriate use of work systems.

Most data breaches result from employees visiting illegal sites on work servers. JP Morgan Chase should implement a policy of restricting employee utilization of computers for company purposes only. Therefore, the company must apply these strategies which will be helpful in protecting its website and software through blocking access from unauthorized intruders (Hazel, 2017).

iii. Conducting of random system drills.

In order to determine if the training conducted on employees is adequate, it would be helpful to have random system drills where staged cyber attacks are used to test the abilities of employees to detect and stop any unauthorized access to the company servers. Through such exercises, Young professionals who would be the future of JP Morgan Chase will be exposed to real cyber attacks scenarios. Through such scenarios they will understand cyber attacks and bein a better position to detect and curb such data security data breaches of the company in the future as it grows(Willard, 2006).

Upgrading of all outdated software and hardware

When calculating the costs of acquiring new software, most people forget that the main problem with using obsolete software is not the lack of updated security features, but the fact that it has many vulnerable points which are already known to the criminals within the cyber space. Using of outdated software creates a threat to the company as the software will no longer receive updates from its developers who spend their time and resources on the newer versions. A lot of valuable business information has its storage on the company servers such as accounting and financial information as well as client information. Using outdated software creates simple access points to the servers which once compromised leads to destruction and theft of data, disruption of network function or even a complete shutdown of the entire network. Even a single computer within a company that is using outdated software can pose a threat to a whole system because the computer lacks updated security features. Although there is much comfort that comes with using something for a while, it is important to remember that hackers have the same feeling of comfort and familiarity with the outdated software. It has been around for many years, and they have had plenty of time to be well-accustomed to it and understand its vulnerabilities (Kedgley, 2016). The following implementations can make this recommendation feasible;

i. Improving company software status by ensuring regular upgrades.

JP Chase Morgan Chase should first realize that using an operating system that does not receive security updates is a danger to the company. It forms a risk to the company as the holes that are left by this sort of outdated software allow hackers in leading to data breach. Therefore, the company should aim at implementing various measures to ensure updates take place regularly. Without patching, JP Morgan will become venerable to hackers. Thus, all systems at JP Morgan Chase should have automatic patching, and at the same time, the company should be ready to channel more time and resources to update their systems. Patching systems continue to be an ongoing maintenance issue that can be costly but is far less expensive compared to a data breach that JP Morgan Chase suffered (LaPiedra, 2002).

ii. Setting aside funds for acquiring new software and hardware

Enhancing system security through buying new hardware and software to replace the old ones is a brilliant business decision for any company that is worried about a data breach. Old equipment brings with it new vulnerabilities for hackers to exploit. Most manufacturers of both hardware and software work under the assumption that their customers will update their assets to the latest versions as they come. The longer a technology asset has been available in the market and to the public, the longer the time criminals within the cyber apace have to identify their vulnerabilities. Considering all these may make the cost of acquiring new versions of systems more than worthy (Solutions E. C., 2016)

iii. Creation of awareness on the benefits of regular upgrades.

It is vital for all employees at the JP Morgan Chase need to understand the importance of updating their systems as well as knowing the detrimental effects it could have on the company as a whole. JP Morgan Chase should then ensure that they upgrade all their departmental systems to more modern operating systems. The modern operating systems as opposed to the old systems allow regular security updates. With regular security updated the company has the ability to avoid bleach from cyber crimes. The modern systems are also easy to integrate into the company as personnel within the company are familiar with them. Regardless of the strategy JP Morgan Chase takes as a company, the implementations should be considered to avoid data breaches that could result in the business losing crucial data along with their customers (Marks, 2017).

VI. BENEFITS AND PROJECTIONS

Through the recommendations, the company can experience the following benefits:

- Data security will be improved hence ensuring customer satisfaction and helping the company rebuild its reputation (Milne, 2004).
- The company will avoid loss of millions of dollars that are lost every year through security breaches.
- Training of their personnel will help increase efficiency hence reducing the risk of security breaches.
- Development and acquisition of new software minimizes the risk of breaches hence protecting customers' data.
- Regular maintenance of company software will see the company's revenue increase by almost 30% due to reduced costs of purchasing new software that is damaged due to lack of proper maintenance.

With such benefits, JP Morgan Chase can be assured of the safety of their business and that of its customers from cyber attacks hence able to uphold its standards and mission of being the best in its industry when it comes to providing financial solutions.

VII. Conclusion

Information systems security is an issue that is at the core of financial institutions and with every growing technology comes more risks of cyber-attack. The ability of a company to withstand cyber-attack places it in a very competitive place within the market. With a high competitive edge within the vast growing market will translate into higher clientele base improving the profit margins within the company. A more focus on the case study of JP Morgan reveres challenging issues within the company that leads to data security breach within the organization. The occurrence of a breach within the organization leads to customer base loss, translating into losses within the giant company. Through a highlight of the problems the JP Morgan Company faces we came up with recommendations and implementations to assist the company gain back its market share. It grows not only its customer base but also profits within its operations.

The recommendations and implementations discussed throughout this research are aimed at ensuring all employees at JP Morgan are made aware of the risks of cybercrime and receive training on how to best prevent and stop any hacking attempts made towards the company. Through the implementations of the recommendations discussed throughout this research, JP Morgan Chase can be able to plan for regular system updates by including it in their budget along with employee training to ensure they do not fall victims to cyber-attack in the future hence protecting their customers and the company too. The resources put into the training will be highly incomparable to the loss occurring after a data breach. It might take JP Morgan more than an year to establish all the new recommendations but it will serve into a more data secure future. With the growth in technology, it is only expected that cybercrime will also take a sharp incline which makes this study just what companies such as JP Morgan need. In the future JP Morgan should put in mind and study the market on developments within the data hacking business.

References

i. Adeoye, B. &. (2012). Customers satisfaction and its implications for bank performance in Nigeria. British Journal of Arts and Social Sciences, 13-29.

ii. Cadle, J. P. (2010). Business analysis techniques: 72 essential tools for success. BCS, The Chartered Institute.

iii. Council, P. S. (2014). Best Practices for Implementing a Security Awareness Program. Information Supplement, 1-6.

iv. Crosman, P. (2016, April 26). Where banks are most vulnerable to cyberattacks now. Retrieved October 30, 2017, from american banker: https://www.americanbanker.com/news/where-banks-are-most-vulnerable-to-cyberattacks-now

v. Hazel, D. (2017, June 5). How to make your staff cybersecurity aware. Retrieved October 30, 2017, from Telegraph: http://www.telegraph.co.uk/connect/small-business/business-networks/bt/how-to-make-staff-cybersecurity-aware/

vi. Jiang, Y. M. (2006). Risk-based resource optimization for transmission system maintenance. IEEE Transactions on Power Systems, 1191-1200.

vii. Kedgley, M. (2016). The Problem with Running Outdated Software. A New Net Technologies White Paper, 1-3.

viii. LaPiedra, J. (2002). The Information Security Process: Prevention, Detection and Response. Retrieved October 30, 2017, from giac org: https://www.giac.org/paper/gsec/501/information-security-process-prevention-detection-response/101197

ix. Madden, J. (2013). Avoiding Security Risks with Regular Patching and Support Services. Ovum, 1-3.

x. Marks, S. (2017, February 22). What Target Should Have Done to Prevent Their Security Breach. Retrieved October 24, 2017, from www.business.com: https://www.business.com/articles/target-done-prevent-security-breach/

xi. Milne, G. R. (2004). Consumers' protection of online privacy and identity. Journal of Consumer Affairs, 217-232.

xii. Mohammed, D. (2015). Cybersecurity Compliance in the Financial Sector. Journal of Internet Banking and Commerce, 1-17.

xiii. Porter, M. E. (2008). The five competitive forces that shape strategy. Harvard business review, 25-40.

xiv. Randi, P. F. (2015, March 9). Cybersecurity, Data Privacy and Information Management. Retrieved October 14, 2017, from Weil, Gotshal & Manges LLP: https://www.weil.com/~/media/files/pdfs/httpsinteractweilcomreactionmailings150309cybersecurityalert.pdf

xv. Silver-Greenberg, J. G. (2014). JPMorgan chase hack affects 76 million households. New York Times, 2.

xvi. Siponen, M. &. (2010). Neutralization: new insights into the problem of employee information systems security policy violations. MIS quarterly, 487-502.

xvii. Solutions, E. C. (2016, August 11). How Outdated IT Assets Can Lead to Security Problems. Retrieved October 14, 2017, from EZ Solutions: https://www.ezcomputersolutions.com/blog/outdated-assets-can-lead-security-problems/

xviii. Valentin, E. K. (2001). SWOT analysis from a resource-based view. Journal of marketing theory and practice, 54-69.

xix. Willard, N. (2006). Cyberbullying and cyberthreats. Center for Safe and Responsible Internet Use, 1-10.