Email Security Solution Implementation

Author's Name Here

A Capstone Presented to the Information Technology College Faculty

Of Western Governors University

In Partial Fulfillment of the Requirements for the Degree

Master of Science in Degree Area HERE

Date of Submission Here

Abstract

PCP international has countless distribution centers across the USA with its headquarters located in Atlanta, Georgia. During the 1st quarter of 2017, an email supposedly sent from the firm's Chief Executive Officer requested for some funds to become transferred to an offshore account. The fraudulent wire transfer saw the firm suffering from financial losses as it lacked efficient and effective email security solutions. A third party conducted vulnerability assessment and the findings indicated there was a need to have an e-mail security solution to prevent such future security breaches. The implementation phases used in the process included;

Phase 1: Planning

- A third-party cybersecurity consultant conducted a vulnerability assessment
- Different technology tools that could perform the required functions were investigated.
- Estimated time for project completion was set.

Phase: Deployment

- All software and equipment required for implementation was procured
- The security tool was deployed first in a testing environment
- The tool was successfully deployed in the production environment it was successfully tested

All configurations and procedures were documented

Phase 3: Review

Deployment was reviewed to ensure the security tool was working as required

The email security tool provided a security layer that helped in the filtering and limitation of fraud and phishing numbers sent to the end-users.

Table of Contents

Email Security Solution Implementation

Introduction

Cybersecurity criminals have increased their attacks on businesses by coming up with new means of stealing company data, including finances. Over the years, email compromise breaches have tremendously increased. This calls for a need for organizations to come up with email security tools that will assist businesses in filtering and reducing the email related attacks.

Project scope

PCP International suffered a cyber-attack following the non-existence of an effective and reliable email security solution. The finances and information of a company must be protected and to prevent such future attacks; there was a need to implement a cybersecurity solution. The current project sought to explore the security threat's magnitude, identification of the various loopholes that allowed for the email breach and outline a solution that was cost-effective and feasible towards solving the email security threat. PCP International being a large company, indicated that the deployment of an email security solution was a complicated endeavour. The current project aimed at elucidating the implementation phases, evaluation of the proposed solution success and recommended various measures that PCP could engage in when monitoring its information integrity (Bloomberg Invest, 2019). The project also ensured that it outlined a cost-benefit analysis that was used in determining whether the implementation of the emails security solution was feasible or its costs outweighed the benefits. The project also researched other email security solutions and outlined why the selected proposal was chosen over the others. However, the project did not focus on the entire company's network and security models but was only limited to the email security solution.

Defense of the Solution

The number one communication method used by a good number of organizations, whether internal or external, is facilitated via e-mail. Nonetheless, e-mail is also the number one method that cybercriminals use when launching an attack in an organization. The methods used by a cybercriminal in email intrusion are growing more dangerous, sophisticated and targeted.

The implementation of email security can seem unglamorous and old hat to most people despite it being more crucial now than ever. One of the most common methods used in launching email-based attacks is phishing. Identity theft criminals and hackers who want access to personally identifiable information or financial data related to a company and its clients mostly launch phishing attacks (Gavett et al., 2017). The introduction of email security solutions will enable a company to avoid various business risks. A considerable number of risks mars the current business environment and thus, sending unencrypted emails is not an option. Any stranger can easily access unencrypted emails, and even competitors can use this information as a competitive advantage. Emails security solution will also help in the protection of private and confidential information (Nguyen, Rosoff & John, 2017). Personally identifiable information such as socials security number, bank account number, credit card information, among others, will be protected. Email security solution will similarly enable the repudiation of any messages sent using an email. An email security solution will help in preventing the likelihood of sending ransomware messages. Various ransomware can block one's screen and prevent one from accessing the computer until a ransom is made (Pope, 2016). An email security solution will also eliminate the likelihood of business email compromises. Business email compromise involves the hijacking of various business email accounts and allows for the possibility of facilitating fraudulent wire transfers. According to an FBI report, between 2013 and 2015, more than 7,000 businesses were

affected by Business Email Compromise, which saw them lose more than $750 million. According to Rader & Wash (2015), $12.5 billion was lost as of December 2016 due to email related fraud according to a report by the FBI. This indicates that through implementing and emails security solution, such losses will be minimized and eradicated

Methodology Justification

The email security solution methodology had to first comply with the various email compliance regulations. One of the regulations is the HIPAA Act that was passed into law in 1996. The HIPAA is the first law that aims at ensuring an individual's health information is protected. (Goldstein & Pewen, 2013). Organizations need to make sure that emails containing the health information of people are protected. The second law that the email security solution adhered to was the Gramm-Leach-Biley Act (GLBA) that was passed into law in 1996. The GLBA law aimed at ensuring that Nonpublic Personal Information is protected (Lin & Li, 2017). This includes the consumers' private financial data. The methodology had to comply with these two laws, as the risk of non-compliance is substantial. An organization is subjected to penalties and fines in case employees disclose customer information, the organization can suffer from reputation damages once it suffers from data breaches and the firm can lose money in the form of litigations.

After determining the laws that govern email compliance, the implementation methodology comprised of three key steps; Planning, Deployment, and Review. The planning phase was crucial as it enabled the setting of plans that assisted in guiding the team through the project execution and closure phases. The plans that were created during this phase helped in the management of time, costs, quality, risk, change, and other issues. It is at the planning phase that a third party conducted a vulnerability assessment, which made it easier to identify the issue affecting

PCP International. The second step of the implementation phase was deployment. In this stage, it saw the purchasing of the software and equipment that was used in implementing the security solution. The most important step in this phase is the testing of the email security solution. This process aimed at ensuring the solution had no vulnerabilities or unexpected errors during deployment (Uddin & Anand, 2019). The review phase was the final step of the implementation process. This step was crucial as it ensured that the tool was working effectively and meeting the business needs it was supposed to satisfy.

Organization of the Capstone Report

The systems and process audit section will highlight the audit process that was carried out before the project design phase. This section will not only highlight a technical audit but also the business audit process. This process will also contain the problem statement, the causes of the security problem, the business impacts of the security problem and a costs benefit and risk analysis of implementing the solution.

The functional requirements section will outline the requirements used in the designing, developing, and imp of the project. This section will outline the various features that the end-user will have access to and the standards, restriction an, technical and operational features that the project must be met.

The methodology section will outline the various phases that were used in the implementation of the email security solution. It will include the following subsections; explanation of the approach and defense of the approach.

The project design section will include the various steps used in the designing, development, testing, and implementation of the email security solution. The project design phase will

include the scope, assumptions, project phases, timelines, dependencies, resource requirements, risk factors, important milestones, and deliverables.

The project development section will outline all the details of the entire development stage, and they will include drafting the various hardware, software, architecture method dodgy, resources, and results of the email security solution, both intangible and tangible.

The quality assurance section will focus on the various methodologies used in maintaining quality control and will include the following subsections; the quality assurance approach, and testing of the solution. Other sections will consist of the implementation plan that will outline the project rollout steps and resources used, the risk assessment section, post-implementation support and issues and conclusion, outcomes and reflection about the entire project.

Systems and Process Audit

Audit Details

Following the security breach at PCP International, there was a need to carry out an audit and determine the cause of the security breach. The security audit was enabled by carrying out a vulnerability assessment that would help in the identification of all the loopholes that were exploited to allow for the security breach. The results from the vulnerability assessment were later used in identifying and prioritizing the threat areas and hence knowing what was to be fixed. According to the vulnerability assessment results, the security breach was enabled through a phishing email attack. The email was sent to one of the company employees purporting to be a request from the CEO’s office. According to the message from the email, it requested the employee to make a wire transfer to an unknown offshore account a request that the employee adhered to. An audit of the finance department also revealed that the company lost some money after it was transferred to the offshore account.

Problem Statement

Cyber-attacks have been on the increase over the years. The primary tools used in gaining access to information or finances from the organization has been the use of phishing emails (Kleitman & Law & Kay, 2018). PCP International is a perfect example of an organization that suffered a security breach resulting from a phishing email attack. According to Norris, Brookers & Dowell (2019), the determination of the legitimacy or maliciousness of phishing emails is not easy, and this is what has made them the most prevalent cyber-attacks tools. Phishing emails have been crafted in such a manner whereby they appear to come from legitimate sources, and this is what has determined their authenticity hard.

Problem Causes

The unavailability of an emails security solution at PCP International was the root cause of exposing the firm to the negative impacts of phishing emails. Phishing emails appear as though they have come from legitimate sources, and this makes it hard for one to determine which is illegitimate or malicious (Kleitman et al.,2018). The employee, therefore, could not pin-point the email's sources due to the lack of and end-point authentication protocol (Williams, Hinds & Joinson, 2018). The employee thought that he/she was following a directive from the CEO to send the money, and this laid down a foundation for the occurrence of fraudulent under-takings at PCP International.

Business Impacts

There is an increasing prevalence of email-related security frauds according to many studies that have been carried out related to the impacts pf phishing emails. According to Ward-man (2016), organizations have suffered from numerous losses amounting to millions of dollars over the years. In 2013, there were over 450,000 phishing email related frauds according to the

RSA, and this saw the companies losing more than $5 billion. The negative impacts of phishing email attacks on companies do not just bring about monetary losses but also reputational damages and increased operational costs (Ragucci & Robila, 2006). A perfect example of financial loss is the one encountered by PCP International after money was sent to an unknown offshore account. A surge in operational costs resulting from an attempt to remove the phishing mail from the domains is also brought about an increased financial burden. The answering of requests from customers regarding the phishing email suspicion also brought about an increased financial burden to PCP International (Jones et al., 2019). Reputational damage also affected PCP International as customers felt that their information was not safe.

Cost Analysis

The costs that were used in running the entire project were classified as labor, external services, and IT operational expense that were grouped in system and software maintenance. According to Stine & Scholl (2010), the complexity and size of the network determined the maintenance costs of the entire system, which was estimated at $20,000- $2,000,000. Mizza (2010) cites that other expenses that would be incurred by the firm include administration and users setting expenses that amounted to $5,000. The email security deployment costs formed the user setting expenses. Exception and delegation management expenses also formed part of the costs incurred by the firm. The procurement of the equipment required for effective and efficient deployment of the email security solution amounted to $100,000. The DNS record configuration and installation costs amounted to $20,000. The total costs incurred to deploy the email security solution amounted to $127,000. The project also incurred other costs, which included labor expenses and payments to the third-party firm that carried out the system audit. The payment rates for the project team members included; project manager ($20/hr.), software administrator ($15/hr.), in-

formation technology specialist ($10/hr.), and database administrator ($8/hr.). The project also had two user experience professionals ($5/hr.). The project required the project manager for 700 hours, software administrator 700 hours, information technology specialist 500 hours, database administrator 400 hours and user experience professionals 200 hours and this would lead to the following costs;

Team member	Cost per hour ($)	Number of hours	Total cost
Project manager	20 (Farok & Garcia, J. 2016).	700	14000
Software administrator	15 (Ruiz, R. 2016)	700	10500
Database administrator	8 (Dube, N. 2016)	400	3200
Information technology specialist	10 (Dube, N. 2016).	500	5000
User experience professionals	5 (Ghaffarianhoseini, et al 2017)	200	1000

Therefore, the total resource cost for the project team was $14,000+ $10,500+$ 3,200+ $ 5,000+ $1,000=$38,700. Additionally, the hiring of third party services to carry out the system audit was added to the overall expense. The entire system audit period took a total of 14 days and the firm was paid $500per day. For the14 days, the firm’s accumulated costs were $ 7,000. Similarly, other miscellaneous costs were estimated at $3,000 and these included meals, purchasing notebooks, pencils, erasers, laptops, and modems.

Risk Analysis

There is a variety of email security solutions available in the market that could be deployed at PCP International. Despite the email security solution preventing users from phishing email attacks, it leaves them exposed to other forms of cyber-attacks. This is an indication that the end-users were left exposed to a high number of other online-related attacks despite the solution being cost-effective. The mitigation of the other online-related threats requires a holistic and sophisticated security solution in addition to the email security solution. The maintenance of the email security solution also needed additional resources and a dedicated security team. The likelihood of the solution being declared ineffective was also high in the event the company did not involve itself in regular security patching, periodic testing, and system maintenance.

Detailed and Functional Requirements

Functional (end-user) Requirements

According to Alsaleh & Haron (2016), the end-user requirements encompass what a user would want the system to do. The email security solution must be user-friendly, an indication that it must be easy to use. The user must have the ability to have quick access to standard features and various commands. The system will also be one that does not malfunction or crash but rather reliable. Similarly, the email security solution will be one that allows the users to use a single sign-on session using one set of login credentials such as name and password to access the email and other applications. This will enable the organization to mitigate the management of multiple passwords and usernames. The email security solution should be one that will provide a critical security layer when receiving and sending sensitive information. This will see the email inbox is loaded up with an end-to-end email encryption service. Once an email is sent, a user must first receive a private key that is unique to an account and use it in decrypting the email.

Detailed Requirements

The new email solution will use the TCP/IP protocol. This network internet protocol is used in specifying data exchange over the internet by providing end-to-end communications. The main for relying on this type of network protocol is that it requires minimal central management, and in case of any network or device failure, it has an automatic recovery process. The TCP/IP protocol uses the client/server network architecture model, which was applied in the connection of the hardware to the company network. The email solution will also be operated on the Windows XP, Windows 7, and Windows 7 operating systems.

Existing Gaps

The main issue affecting PCP International is the lack of an email authentication protocol. Authentication refers to the process whereby an application can tell a user who the current user is and if or not, they are who they claim to be. The authentication protocol will be able to inform one various attributes about the sender of specific emails and reveal their identity. In most cases, in case the email fails the authentication process, it is filtered as a spam mail or rejected. The lack of an email authentication protocol at PCP International is what allowed for the sending of phishing emails. However, the email security solution aimed at ensuring that PCP International has an email authentication protocol in place. The answer will ensure it blocks malicious or fraudulent emails such as spam and phishing. The email authentication protocol will relay in basic standards such as DMARC, DKIM, and SPF and will help in supplementing the basic protocol used in sending emails at PCP International and other organizations, the SMTP protocol.

Project Design

Scope

The project consisted of creating an email security solution for PCP International following a security breach. The project was completed on September 30, 2019. The project will only include proving an end-point authentication email protocol to protect the company from future breaches. However, the project did not include providing PCP International with an entire system network security plan.

Assumptions

The major assumption made by the project was that an end user at PCP international could not differentiate between a legitimate and malicious email. Therefore, the employee at the company ends up opening an email or responding to the email despite it containing a malware that is used in accessing the company information.

Project Development Phases

The project comprised of many phases that ensured the implementation of the security solution was effective. The first phase involved conducting a system audit by a third party that would enable one to ascertain the full extent of the breach and its cause. The second phase was requirements gathering, which involved the creation of a concise and clear agreed set of requirements gathered from various stakeholders that were used in determining their needs (Hassan et al., 2016). The design phase involved determining the primary elements, success criteria and deliverables that would make the entire project attain its goals. The development phase indicates that the project has already commenced and it is at the implementation and testing stages. The quality assurance phase was used in testing the security solution and ascertain whether indeed it is meeting its intended goals (Javed et al., 2012). The implementation stage saw the introduction

of the email security solution at the PCP International network to prevent future attacks. The final step was the post-implementation support that ensured there are continued support and maintenance of the email security solution.

Timelines

Phase	Start date	End date
System audit	1st February 2019	14th February 2019
Requirements gathering	20th February 2019	7th March 2019
Design	10th March 2019	10th April 2019
Development	15th April 2019	31st April 2019
Quality assurance	2nd May 2019	14th May 2019
Implementation	20th May 2019	20th June 2019
Post-Implementation support	1st September 2019	

Dependencies

The requirements gathering phase cannot begin before the system audit. It is crucial to determine the security problem at PCP International before finding out the needs of the various stakeholders. The design phase is reliant on the requirements gathering and system audit phases. The design phase must have all information related to the security breach, which is provided by the system audit phase. The data from the requirement-gathering phase will enable the design phase to lay down plans and determine the number of resources required in meeting the stakeholder needs. The development phase is dependent on the design phase for, after planning, the

solution is now put into action. The quality assurance phase is dependent on the implementation phase for the solution must first be implemented before its ability to perform the expected function can be determined.

Resource Requirements

The system audit phase required financial resources that were used in paying for service costs to the third party organization. The requirement gathering phase financial resources necessary used in catering for the entire process in the form of funding for the project team's daily expenses. The requirements gathering phase also needed human resources in the form of the project team and laptops used in recording the data. The design, development, and implementation phases required necessary hardware required during the project included 2GB RAM, Intel Pentium Processors, mouse or compatible pointing device, 256-colour or higher VGA monitor, WI-FI routers and USB devices. The software included a firewall, antivirus, and email security gateways. The team members included a project manager, software administrator, information technology specialist and database administrator. The phases also required financial resources amounting to $127,000. The post-implementation support and maintenance required financial resources that would be used in employing two employees who would ensure the email security solution is always up-to-date.

Risk Factors

The major risk factor that affected the situation was compatibility. The likelihood of this risk was 40%, and in case it occurred, it would force the company to purchase another email security software, and this would bring about additional costs. Some email security solution software has limited OS support. Some of the software may end up not supporting server OS but are only limited to client OS. Another risk factor is that the effectiveness of the email security solu-

tion is highly reliant on its ability to detect emails with malware or from unknown sources. The probability of this risk occurrence was 50%. The email security might still not flag some emails as spam, and once an employee opens such emails, it would see the firm suffering from another security breach. The security solution might, therefore, overlook some emails despite them being suspicious.

Important Milestones

Milestones are vital, as they will give the project team and management some visibility on the achievements made by the entire project's progress (Umar & Alaskar, 2018). In case a set milestone is not met, it will indicate the project is not adhering to the set plan, and thus, the management must implement corrective actions. When placing a milestone goal, it must be verifiable. Unverifiable milestones will make a project to lose its visibility and control. The significant milestones for the project will include the following;

1. Concept Approval

Following the system audit by a third-party, the cause for the system breach was determined as being intrusion via a phishing email. The project team laid down various solutions to solve the security breach. The management had one week to decide which was the best solution for managing any future security breaches. An approval from the management allowed the project manager to process to a more detailed requirement definition. A project schedule was used in ascertaining the success of this milestone as a response was required within a week (Eik-Andresen et al.,2016).

2. Requirements Review

For the solution to deliver its services, it must first be decomposed into requirements. The requirements will include the capabilities needed by a user in meeting his/her needs (San Cristo-

bal et al., 2018). The requirements management milestone would ensure that any changes, refinement, documentation, and elicitation to the requirements are sufficiently managed during the entire project lifecycle. The requirements review will take 21 days to ensure that all the user needs and wants are fully documented and all necessary changes are made. The measurement criteria for the requirement review will be requirements traceability. Through this process, it allows one to understand why the particular requirements exist, the effect of any changes made, determining the requirements are complete and prioritization of the requirements.

3. Preliminary Design

The requirements approved will be used in designing the solution's architecture and determine whether it is the most suitable solution. In case the solution fully meets the user requirements, it is input into the detailed design process. The preliminary design process will take 21 days after the approval of the requirements and a project schedule will be used in measuring the success of this milestone.

4. Critical Design Review

In this milestone, the detailed design of the solution is fully implemented into the system architecture and thus it is approved and suitable for input into the development of the solution's code. The critical design review will take one month and a project schedule will be used in determining the success of this milestone.

5. Test Plan and System Test Review

There is a need to test the solution and ensure that the solution fully meets its intended goals. This milestone will see the formulation of test cases and test procedures. The measurement for the test cases and test procedures will be determined by inputting them into an integration testing. This process will take 14 days. Once the system has passed the testing procedures, it is now

suitable for input into acceptance testing. The Plan-Do-Check-Act (PDCA) method will be used in measuring the success of this milestone. The main reason for using this methodology is that it allows for continuous improvement by resolving any problems that may arise in a process (Sokovic, Pavletic & Pipan, 2010).

6. Operational Readiness Review and Solution Roll-out

Once the solution passes the acceptance testing, it is now suitable for deployment into its target environment. The solution rollout will take one week to ensure that it is effectively and efficiently installed into the company's computer network.

7. User training

Training users on how to use a new system is vital. The training will ensure that any form of resistance developing among users is eliminated, and thus, they can embrace the new system. The training process will take 14 days from the last system rollout day.

Deliverables

The email security solution was provided in form of a software product. The post-implementation support and maintenance were to be provided in the form of a document, which was subject to review after every six months. Likewise, the employee-training manual on how to use the email security solution was provided in the form of a document and a set of procedures that were to adhere strictly.

Methodology

Approach Explanation

The implementation methodology comprised of three key steps; Planning, Deployment, and Review. The planning phase was crucial as it enabled the setting of plans that assisted in

guiding the team through the project execution and closure phases. The second step of the implementation phase was deployment. In this stage, it saw the purchasing of the software and equipment that was used in implementing the security solution. The most important step in this phase is the testing of the email security solution. This process aimed at ensuring the solution had no vulnerabilities or unexpected errors during deployment (Uddin & Anand, 2019). The review phase was the final step of the implementation process. This step was crucial as it ensured that the tool was working effectively and meeting the business needs it was supposed to satisfy.

Approach Defense

The methodology selected for the implementation of this project is one that allowed for the efficient maximization of time and resources. This approach provides a secure path for the flow of information and secures client and company confidential information.

The approach is cost friendly as compared to implementing the entire security system in an organization which can be very costly. This makes it more preferably as cutting costs is concerned.

Its stronger as compared to installing antivirus in the system. Malicious software attacks from the internet can’t affect the system unlike the antivirus installed programs which can prove to be a weak point for intrusion.

This project contains a server which acts as the central point of the entire organization, and this makes it easier for a software administrator to control data security and resources. Therefore, this approach defends and secures the most confidential mail passages keeping the organization data safe. Which makes it the best tool for data protection and security of an organisation.

Project Development

Project development is a crucial phase in the entire project. The initial phases lay down a foundation for the entire email solution development. To ensure that the development phases s a success, there must be a detailed and comprehensive set of design specifications and proper tools, standards and processes. The following deliverables will be required from the software development phase;

Test data and analysis report

There is a need to ensure that sample test data is availed that will be used in testing the email security solution. A record of the test, capabilities, and deficiencies of the system are reviewed

Integration document

It will outline the interaction and assembly of the software, hardware and other system components to ensure there is proper functioning.

Updating the conversion plan

Following the introduction of the new system, there is need to outline how the data from the old system will be migrated/converted into another software and hardware environment.

Updating the implementation plan

This will identify all the procedures that should be undertaken to ensure the email security solution is implemented in the PCP International computer network.

System operations manual

The operations manual will be developed for the system administrator, which will outline how the client/server applications will function with the new email security solution.

Release notes

The notes will include summary information related to the current release of the new email security solution and it will include any workarounds, problems, changes and new features.

Maintenance manual

There is a need to ensure that the system maintenance team has all the information necessary to ensure the system is effectively maintained.

Training plan

There is a need to outline all the user training and technical requirements related to the new system. The training needs will include determining how to operate, maintain and implement the email security solution successfully.

User manual

It is vital to ensure that a user manual is developed to make sure that the users are conversant with the new system. This will provide a step-by-step procedure for accessing and using the system

Hardware

Hardware
Processor-Pentium 4 or higher, Speed- 1 gigahertz or higher 32 bit or 64-bit processor
RAM- 1GB RAM for 32 bit and 2GB RAM for 64 bit
Display- 1024*768 resolution

Graphics Hardware- DirectX 10 graphics card
Hard Disc Capacity- Approximately 3 GB

Software

Software
Windows XP Professional Edition (only 32 bit) Windows Server 2012/2012 (64 bit only) Windows Server 2008 (32-bit and 64-bit) Windows 7 (32-bit and 64-bit) Windows Vista (32-bit and 64-bit)
Avast antivirus software
Firewall
Email security gateways

Tech Stack

In order to set up a strong email security defense system, OSI information exchange protocols were employed. The OSI protocols comprise seven layers each having its protocols and functions.

Number	Layer	Protocols	Description

1	Physical	Bluetooth, IEEE.802.11, DSL, OTN	This layer is mainly focused on the hardware element of networking.
2	Datalink	IEEE.802.3, HDLC, ARP, ATM, SLIP	The physical layer sends data to this layer
3	Network	IGMP, AppleTalk, IPv4	The devices used in this layer include the switches and routers. It is the most important OSI layer as it allows for transferring of data from one node to the other.
4	Transport	SCTP, DCCP, SPX, TCP	It enables the transmission of data to the destination nodes from the source.

5	Session	L2TP, SAP, NetBIOS	It allows for the creation of a session involving the destination and source nodes and ends the communication process.
6	Presentation	MIM|E, SSL, TLS, XDR	It allows for encryption and decryption. It allows for data conversion into a format that the application layer can read.
7	application	SMPP, SMTP, FTP, HTTP	It is located at the user end and allows the user to interact with various applications. The major applications in this layer include email and file transfer

Architecture Details

A client/server architecture was used in configuring the hardware and network. In this type of architecture, the resources and services consumed by the client are managed, hosted and delivered by a server. All the computers are connected to a central server via an internet connection. The server acts as the heart of the entire organization, and this makes it easier for a software administrator to control data security and resources.

Resources Used

During the implementation of the project, various resources were used. A resource is defined as an item or person that is needed for project execution. Multiple resources can be used to ensure a project is a success. (Selaru, 2012) The project used the following resources; services, labor, equipment, materials, and money.

Services

The project required to hire a third-party service provider who would carry out the system audit process to determine the cause of the security breach. Before outsourcing for a third/party, there is, need to carry out a cost/time analysis and ascertain which tasks can be done in-house and which require external providers. The outsourcing of third party providers falls under the type of services or resources.

Labor

The labor resources comprise of the various staff who were used during the project. However, not all the staff will be used for the entire project and some will only be required during certain phases of the project (Ballesteros-Perez et al., 2012). However, the project manager will be involved from the start until end of the project. The other human resources required during the

project included; software administrators, user experience professionals, information technology specialists, and database administrators.

Equipment

The equipment included the various items that were needed to see the project is a success. These included interactive whiteboards, monitors, computers, keyboards, servers, desks, office furniture, telephones, and vehicles.

Materials

Material resources comprise of the consumables used during the project. They can also form part of the project deliverables and in this project, office stationery was the main materials used. Fuel was also used in transporting the third-party staff to and from the premises. Other materials used included the food that was consumed by the project management team.

Money

This forms the most common secondary type of resource in projects. It is used in the purchasing, acquiring and maintaining all the other resources. The money used in the project was based on a calculated budget estimation, which was set at $169,000.

Final Output

The tangible final output of the entire project was the formal acceptance from the client. The official acceptance of the project is the acknowledgment of the project client or sponsor that the required deliverables of the project have been met (Loudon, 2012). The formal project acceptance included the;

The Scope Statement

This outlines what the project was required to do, and it has four sections, justification of the project that describes the business solution the project aimed at addressing. The second sec-

tion is the project description that offers a summary of the project's outcome. The third section is the project deliverables that outline the various phases that were undertaken to ensure the project was a success (Fernandes, Ward & Araujo, 2013). In this case, they included a user manual and tutorial that would enable PCP International employees to understand how to use the new system. The fourth section is the project objectives that outlines measurable criteria that ascertain whether the project was a success.

Work Results Description

The final acceptance documentation includes the work results descriptions, which will describe what the project produced.

Inspection procedures details

This will include documentation of what was done to ensure that the project fulfilled the original scope. This will outline that the project has effectively been assessed and verified being operational.

Solution acceptance form

This is a form that acknowledges the sponsor or clients accepted the work results of the solution. The form requires the client o sign off, and it beats the clients and project manager's signatures.

Quality Assurance

Quality Assurance Approach

The Plan-Do-Check-Act (PDCA) method was the core quality assurance methodology employed in the project. The main reason for using this methodology is that it allows for continuous improvement by resolving any problems that may arise in a process. The first phase is Plan, which involved identifying and analyzing the problem that might result from the solution and de-

ciding which one to be tested. The DO phase involved testing the potential solution and measuring the respective results. The Check phased determining to study the outcomes and measuring whether they are effective and if the solution is efficient or not, and in case the solution was effective, the solution implemented in the Act phase. The acceptance criteria used during this process was that

- Scenario: User logs into the email

  Acceptance Criteria: Given that I am in a role as a registered user

  When I open the “Email” page

  Then the system shows me the list of all the sections

  In addition, the system shows the “SPAM: folder on the left side of the screen.

  When I click on the SPAM folder, I should be able to see a list of all suspicious emails

Solution Testing

Before carrying out the testing procedures, detailed user story and acceptance criteria were first developed (Pandit & Tahiliani, 2015). The testers used the user stories in formulating test cases. The test cases were later used in formulating workflows, boundaries and scenarios that cover far what one thought possible. Benchmark testing was used in determining the performance abilities of the new email security solutions. The performance measures were captured each time a load test was carried out to allow for the making of any changes to the system with an aim of determining whether there is an improvement to the system or degradation. When benchmarking the system, user loads were loaded into the system amalgamated with security violations to determine its performance benchmark.

Scenario: Users send malicious emails to the system

Acceptance Criteria:

As registered users, malicious emails were sent to selected employee inboxes

once an employee opens the “Email” page, the interface should display various email components.

The user opens the “SPAM” folder.

It should contain a list of spam mails.

If this is not the case, the solution is ineffective, and its performance is poor

Implementation Plan

Strategy for the Implementation

There are varieties of project implementation strategies, and some of them include; agile, scrum, Kanban, Lean, waterfall and PMBOK/PMI. Selecting the best project methodology is key to the success of the entire undertaking. In case of a waterfall, it is a traditional-based methodology, and this makes it inefficient in modern-day and age. The methodology selected for the implementation of this project is one that allowed for the efficient maximization of time and resources in this case Agile methodology. Agile allows for the breaking of the entire project into smaller phases and they are later prioritized by the project team depending on their level of importance Agile project methodology is value-driven and it is all about embracing change. Being a software-related project, it can constantly change, and through agile, one can make the changes even during the development phase. The focus of the team when using agile methodology is a continuous adaptation, rapid feedback and adhering to a committed schedule that ensures the entire project is delivered on time

Phases of the Rollout

The rollout phase is the final phase of any IT related project cycle. The first step of the roll-out phase is identifying the inputs, and they include; the conversion plan, operations instructions, rollout plan, and end user documentation. The second step is conducting the key activities, and they include performing a readiness check, conducting the system conversion, performance of production monitoring and documentation of potential enhancements. The third step is creation of the outputs, and the final step is meeting the milestones after the post conversion review document is completed.

Details of the Go-Live

The project manager will create the outputs with the first phase being change requests that outline any documentation that will outline procedures for system enhancement and problems that might be encountered. The post-conversion review document will describe how the system conversion process went — following the completion of the post-review completion document, meeting the milestone. At this point, the conversion team and end-users signed-off the post-conversion review document to indicate that the system was converted successfully. This is the final step of the rollout phase, and this showcases that the project manager has completed the project, and it is given to the client.

Dependencies

The email security solution had to be implemented and be operational before the employees could access their emails. No employee was allowed to reply or open suspicious mail before the security solution was implemented. Such emails had to be forwarded to the system administrator and software administrator.

Deliverables

The intangible deliverables included an email security solution, increased employee confidence and job satisfaction, reduced company operational costs, increased and more positive public image, and reduced cyberthreats. The tangible deliverables included gap analysis reports, design presentations, inspection reports, Gantt charts and a whitepaper developed by the project team to help stakeholders understand how to use the new features.

Training Plan for Users

The employees at PCP International were trained on how to distinguish between legitimate and malicious emails. They were also trained on the importance of maintaining information security and how they can help to ensure the company is not affected by future security breaches. The project manager, the system analyst, conducted the training sessions and software administrator one week after the project was completed.

Risk Assessment

Quantitative and Qualitative Risks

With the implementation of the new solution, it will introduce additional work features and the likelihood of employee resistance to the solution is very high. Similarly, the inability to detect some legitimate emails is still probable though the risk is moderate. There is also a 50% probability there will be a need to increase the operational budget at PCP to cater for the new employees and maintenance of the system. The risk of hackers getting past the email security solution has a 25% of occurring.

Cost/Benefit Analysis

There will be a 95% decrease in malicious attacks at PCP, and in case PCP does not prevent the malicious attacks, it will bring about a 35% increase in its operational costs. Increased

operational costs will force PCP International to cut down on the number of its employees by 25% if it wants to make profits. However, this is not expected as the firm will have gained a negative public image and it is expected to see a 10% decline in its customer numbers every two months. However, by implementing the system, PCP International will witness an increased customer number of 25% after three months and a 15% increase in its quarterly revenues.

Risk Mitigation

The prevention of employee resistance will be mitigated by ensuring they are part of the entire process from the planning until the implementation phase. This will make employees feel like they are part of the entire project. To prevent an increase in the operational budget, there will be a need to ensure that the email security solution is meeting its goals and objectives. The only rollback plan to the original implementation plan is implementing an entire company-wide information security system. The main advantage of this is that it will protect the entire system form all forms of attacks. However, the disadvantage is that it will be more expensive to implement and will take more time.

Post Implementation Support and Issues

Post Implementation Support

The new system will feature an automatic installation of the new version before the end-of-service date of the current system being used at the organization. There will be a continuous checking for bugs and vulnerabilities in the system and necessary patches made to ensure the system can prevent any phishing emails from reaching the company employee inboxes.

Post Implementation Support Resources

There will be a need to have financial, software and human resources. The financial resources will be used in purchasing a new version of the software and paying for the required li-

censes. Similarly, there will be a need for having the respective software that acts as an email security solution. The human resources will be required to ensure there is continued maintenance of the software, as cyberattacks tend to become sophisticated daily hence a need to ensure there is an effective email authentication process (Al-Mashhadi & Albeich, 2017).

Maintenance Plan

The short-term maintenance will feature three types of maintenance; corrective, adaptive and perfective. Corrective maintenance involves the correcting of any discovered errors in the software immediately; it has been delivered (Singh & Goel, 2007). Adaptive maintenance involves ensuring that the software is still operational within a changing environment. Perfective maintenance involves the improvement of the software attributes, enhancements for users, and software maintainability (Hatton, 2007). Long-term maintenance will include ensuring there is an upgrade to a new version after every six months. Testing of the software will also be carried out after three months to check for bugs and vulnerabilities.

Conclusion, Outcomes, and Reflection

Project Summary

Cyber-attacks are the major impediments towards organizational success in the current technologically driven world. PCP International suffered from a major security breach that saw it lose its finances to criminals. This project aimed to formulate and implement an email security solution that would prevent any such future happenings at PCP International. The implementation of the email security solution was divided into various stages. During the system audit phase, a vulnerability assessment was carried out to determine the cause of the security breach at PCP. The audit revealed that a phishing email was used in causing fraudulent undertakings at PCP International. Requirements gathering phase allowed for the collection of information form

stakeholders at PCP, in this case, the management and employees. The design phase was used in laying down a foundation for the implementation and determining all the resources that would be required during the entire project. The quality assurance phase allowed for assessing the quality of the entire solution and ensuring it would perform the required function. The last phase of the project was the post-implementation support and maintenance that would ensure there was a continued and continuous review of the solution and ensure it is updated to meet its goals and objectives.

Deliverables

The major deliverables submitted with the project included the network architecture that was used in configuring the hardware and network at the company. The company employed a client/server network architecture that allows clients to receive and send requests from and to a central server. The sever awaits for a client to make a request and responds to them. The client/server network architecture does not requires a user to have an awareness of the various hardware or network providing the respective service. The clients are mostly located at workstations while the servers are located in other locations at the network.

Outcomes

Following the loss of money at PCP international, a substantial number of employees feared to access their emails. This saw the company operations facing huge backlogs from client requests and even orders. However, after implementing the project, the employees were confident in accessing their emails, and thus the firm resumed back to its normal day-to-day operations. The company was able to prevent any more cyber-related attacks associated with phishing emails. The company also had a platform upon which they could authenticate the various emails getting into the employee mailboxes and ascertain whether they are legitimate or malicious.

More importantly, the company was able to resume back its public reputation as clients and customers were confident in the organization's ability to protect its information from cyber-attacks. The project was also able to prevent any financial losses resulting from fraudulent activities and increased operational costs. The successful implementation of this project was one of the most significant breakthroughs I have made this year.

Reflection

From this project, I have learned how one can drive change and build something from scratch. It is also vital for one to break large work processes into small processes and organizational structures to get the desired results. I have also learned how people adapt to change and for one to become a champion in any project, being action-oriented and anticipating problems much earlier is vital.

References

Alkhuraiji, A., Liu, S., Oderanti, F. O., & Megicks, P. (2016). New structured knowledge network for strategic decision-making in IT innovative and implementable projects. *Journal of Business Research*, *69*(5), 1534-1538.

Al-Mashhadi, H. M. & Albeich, M. (January 01, 2017). A Survey of Email Service; Attacks, Security Methods and Protocols. *International Journal of Computer Applications, 162*, 11, 31-40.

Alsaleh, S., & Haron, H. (2016). The most important functional and non-functional requirements of knowledge sharing system at public academic institutions: A case study. *Lecture Notes on Software Engineering*, 4(2), 157.

Ballesteros-Pérez, P., González-Cruz, M. C., & Fernández-Diego, M. (2012). Human resource allocation management in multiple projects using sociometric techniques. *International Journal of Project Management*, *30*(8), 901-913.

Bloomberg Invest. (2019). *PCP International LLC*.

Dube, N. (2016). *Evaluating the impact of the project implementation profile (PIP) tool on interface management in public sector projects: case study KZN Department of Health Facilities* (Doctoral dissertation, University of Cape Town).

Eik-Andresen, P., Johansen, A., Landmark, A. D., & Sørensen, A. Ø. (2016). Controlling a multibillion project portfolio-milestones as key performance indicator for project portfolio management. *Procedia-Social and Behavioral Sciences*, *226*, 294-301.

Farok, G., & Garcia, J. (2016). Scope creep monitors level of satisfaction, cost of business and slippery slope relationships among stakeholders, project manager, sponsor and PMO to

execute project completion report. *Journal of International Association of Advanced Technology and Science (JIAATS)*, *2*(2), 15-23.

Fernandes, G., Ward, S., & Araújo, M. (2013). Identifying useful project management practices: A mixed methodology approach. *International Journal of information systems and project management*, *1*(4), 5-21.

Gavett, B.E., Zhao, R., Johan, S.E., Bussell, C.A., Roberts, J.R., & Yue, C. (2017). Phishing suspiciousness in older and younger adults: The role of executive functioning. *PloS One*, *12*(2), e0171620.

Ghaffarianhoseini, A., Tookey, J., Ghaffarianhoseini, A., Naismith, N., Azhar, S., Efimova, O., & Raahemifar, K. (2017). Building Information Modelling (BIM) uptake: Clear benefits, understanding its implementation, risks and challenges. *Renewable and Sustainable Energy Reviews*, *75*, 1046-1053.

Goldstein, M. M., & Pewen, W. F. (2013). The HIPAA Omnibus Rule: implications for public health policy and practice. *Public Health Reports*, *128*(6), 554-558.

Hassan, Z.U., Sattar, A. R., Zafar, M.R., & Abbas, W. Impact of requirement gathering techniques on software development. *Information and Knowledge Management*, *6*(11), 28-30

Hatton, L. (2007). How accurately do engineers predict software maintenance tasks? *Computer 40*(2), 64-69.

Javed, A., Maqsood, M., Qazi, K.A., Shah, K.A. (2012). How to improve software quality assurance in developing countries. *Advanced Computing*, *3*(2), 17.

Jones, H. S., Towse, J. N., Race, N., & Harrison, T. (2019). Email fraud: The search for psychological predictors of susceptibility. *PloS one*, *14*(1), e0209684.

Kleitman, S., Law.M.K.H. Kay,J.,(2018). It is the deceiver and the receiver: Individual differences in phishing susceptibility and false positives with item profiling. *PloS One*, *13*(10), e0205089.

Lin, J. H., & Li, X. (2017). Regulatory policies on Gramm-Leach-Bliley consolidation of commercial banking, shadow banking, and life insurance. *Journal of International Financial Markets, Institutions and Money*, *50*, 69-84.

Loudon, J. (2012). Applying project management processes to successfully complete projects in radiation medicine. *Journal of medical imaging and radiation sciences*, *43*(4), 253-258.

Mizzi, A. (2010). Return on information security investment-the viability of an anti-spam solution in a wireless environment. *IJ Network Security*, *10*(1), 18-24.

Nguyen, K. D., Rosoff, H., & John, R. S. (2017). Valuing information security from a phishing attack. *Journal of Cybersecurity*, *3*(3), 159-171.

Norris, G., Brookes, A., & Dowell, D. (2019). The psychology of internet fraud victimization: A systematic review. *Journal of Police and Criminal Psychology*, *34*(3), 231-245.

Pandit, P., & Tahiliani, S. (2015). AgileUAT: A framework for user acceptance testing based on user stories and acceptance criteria. *International Journal of Computer Applications*, *120*(10)

Pope, J. (2016). Ransomware: Minimizing the risks. *Innovations in Clinical Neuroscience*, *13*(11), 37.

Rader, E., & Wash, R. (2015). Identifying patterns in informal sources of security information. *Journal of Cybersecurity*, *1*(1), 121-144.

Ragucci, J, W., & Robila, S.A. (2006, June). Societal aspects of phishing. *In 2006 IEEE International Symposium on Technology and Society*, 1-5.

Ruiz, R. (2016). *Deployment of a software infrastructure for Ecommerce and business analytics in a small business* (Bachelor's thesis).

San Cristóbal, J. R., Carral, L., Diaz, E., Fraguela, J. A., & Iglesias, G. (2018). Complexity and project management: a general overview. *Complexity*, *2018*.

Selaru, C. (2012). Resource allocation in project management. *International Journal of Economic Practices and Theories*, *2*(4), 274-282.

Singh, Y., & Goel, B. (2007). A step towards software preventive maintenance. *ACM SIGSOFT Software Engineering Notes*, *32*(4), 10.

Sokovic, M., Pavletic, D., & Pipan, K. K. (2010). Quality improvement methodologies–PDCA cycle, RADAR matrix, DMAIC and DFSS. *Journal of achievements in materials and manufacturing engineering*, *43*(1), 476-483.

Stine, K., & Scholl, M. (2010). E-mail security. An overview of threats and safeguards. *Journal of AHIMA*, *81*(4), 28-30.

Uddin, A., & Anand, A. (2019). Importance of software testing in the process of software development. *International Journal for Scientific Research & Development*, *4*(1), 130-200.

Umar, A., & Alaskar, T. (2018). Understanding Relationship between Milestone and Decision-Making in Project Management: A Qualitative Study among Project Managers in Saudi Arabia. *International Journal of Business and Management, 13 (*8), 184-195.

Wardman, B. (2016). *Assessing the Gap: Measure the Impact of Phishing on an Organization*.

Williams, E. J., Hinds, J., & Joinson, A. N. (2018). Exploring susceptibility to phishing in the workplace. *International Journal of Human-Computer Studies*, *120*, 1-13.

Appendix A

Client/Server Network Architecture