Federation University Australia at IIBIT (Sydney)

School of IT

Sydney Campus

Assignment Cover Page: Group Work

Course Number : **ITECH 7400**

Group Members

SL	Last Name	Given Names	Ballarat ID	UB ID
1.	Khadka	Bikash		
2.	Jaiswal	Bishal		30358366
3.	Khadka	Nikita		
4.				
5.				

COURSE NUMBER AND NAME:_____

PROGRAM OF STUDY:

TUTORIAL GROUP : **DAY/ TIME:**

LECTURER:

TUTOR (if applicable):

TITLE OF ASSIGNMENT/ PROJECT/ CASE STUDY:

WORD LENGTH: DUE DATE: DATE SUBMITTED:

DECLARATION:

We have kept a copy of this assignment/work so that we can produce it if the original is lost or damaged. We hereby certify that no part of this assignment/work has been copied from any other student's present or previous, published or unpublished, professional or amateur work or from any other source except where due acknowledgement is made in the assignment. We further certify that no part of this assignment/work has been written/produced for us by any other person except where such collaboration has been authorized by the unit/subject lecturer/tutor concerned.

Signature of Student(s)

Note: It is necessary to sign the above declaration. A lecturer/tutor or an examiner reserves the right not to mark this assignment/work if the declaration has not been duly signed.

Abstract

According to the requirement of ITECH 7400, IT Service Management and Professional Culture, under the Federation University, IIBIT, Sydney, this report has been conducted to analyze the use of IT Service management in a big organization as "Telstra" which became a boon for them. This report is comprised of the topics which we have covered from our lecture weeks 1 to 8. By the help of this report, we were able to deal with different topics as the history, SWOT analysis, the service management system of Telstra including the Deming Cycle and other more terms. Moreover, we were able to focus on the risk's management mechanism and the continual improvement process, which Telstra has been implementing.

Table of Contents

List of figure

1. Introduction

Telstra is one of the most leading organization in terms of technology. It has been providing good services regarding the telecommunication as well as information services. Telstra has been competition throughout Australia serving their customer with good range of telecommunication facilities. Basically, the main tasks that Telstra provide is the telephone services in business and to homes. Telstra can provide their customers with the service to make international calls and is established for mobile communication services. Not only limiting to this, Telstra has been actively providing internet as well online services in an affordable range to other service provides too. Telstra is considered as the largest telecommunication provider overall Australia, providing GSM as well as CDMA networks which has been including almost 95% of the population (Ross, Peter & Bamber, Greg, 2019).

As the world is in its technological era and every technology has been advancing, Telstra is continuously enhancing its capabilities to compete with modern technologies. Since, they realized that data service is now at the top of the world, so they have been more focused on transforming their business to meet the customers goal and with a motive to provide their customers with more advanced form of technological use. They are manually upgrading their network system, which is also increasing their flexibility and facilitating their customers with high range of expanded products with better services. Thus, with a realization, that the pressure will increase as they grow, they are more targeting to improve their efficiency and being more customer focused. Some of their initiatives includes enhancement of the efficiency and flexibility of their networks and systems, more improved work practices and review of their cost structures with their mechanism in delivering satisfiable service to their consumers in a systematic manner. All these works were possible because of the use of IT Service management in their organization (Telstra practices, 2019).

According to the official website of matrix software, given is the most shocking transformation found in Telstra, which shows that the number of the digital customer transactions was found to be doubled within three years only (More, Elizabeth & Mcgrath, Michael, 2011).

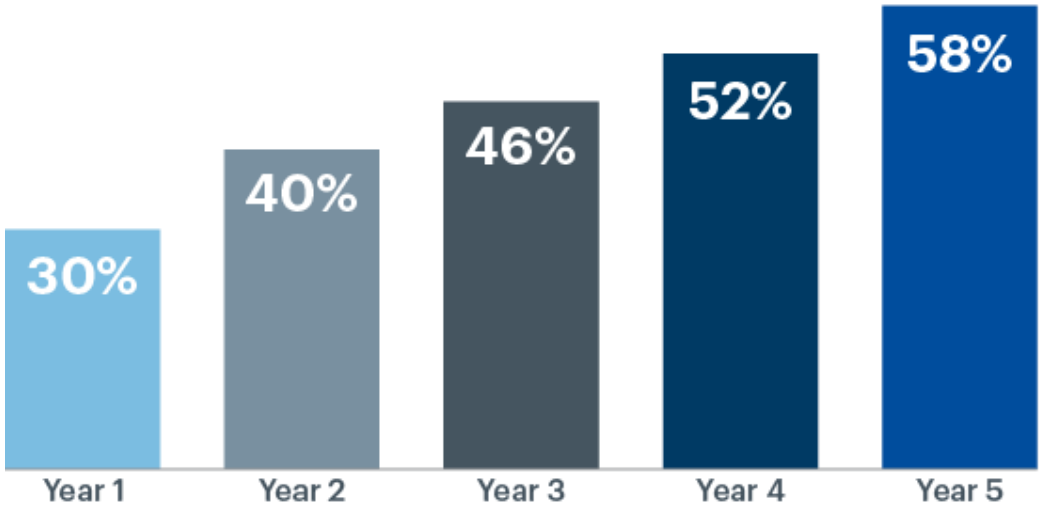

Figure 1.1: Telstra digital customer transformation [Retrieved from: https://www.matrixx.com/customers/telstra/]

2. The Service Lifecycle for Telstra

According to the lecture slide of Week 1 of IT Service Management and Professional Culture, the service lifecycle is one of the mechanisms of IT service management, which is mainly focused on the importance of the collaboration of various functions and systems which are responsible to manage the IT services lifecycle. The IT Service lifecycle is mainly comprised of 5 phases as, Service Strategy (SS), Service Design (SD), Service Transition (ST), Service Operation (SO) and Continual Service Management (CSI) (Telstra practices, 2019).

Service Strategy mainly deals with establishing an idea or strategy to use IT services. Service Design helps to find out the solutions which meets our requirements. Service Transition manages the overall transition throughout the lifecycle. Similarly, Service Operation manages the IT services and CSI checks for the improvement to an IT Services and IT Service Management processes (Telstra practices, 2019).

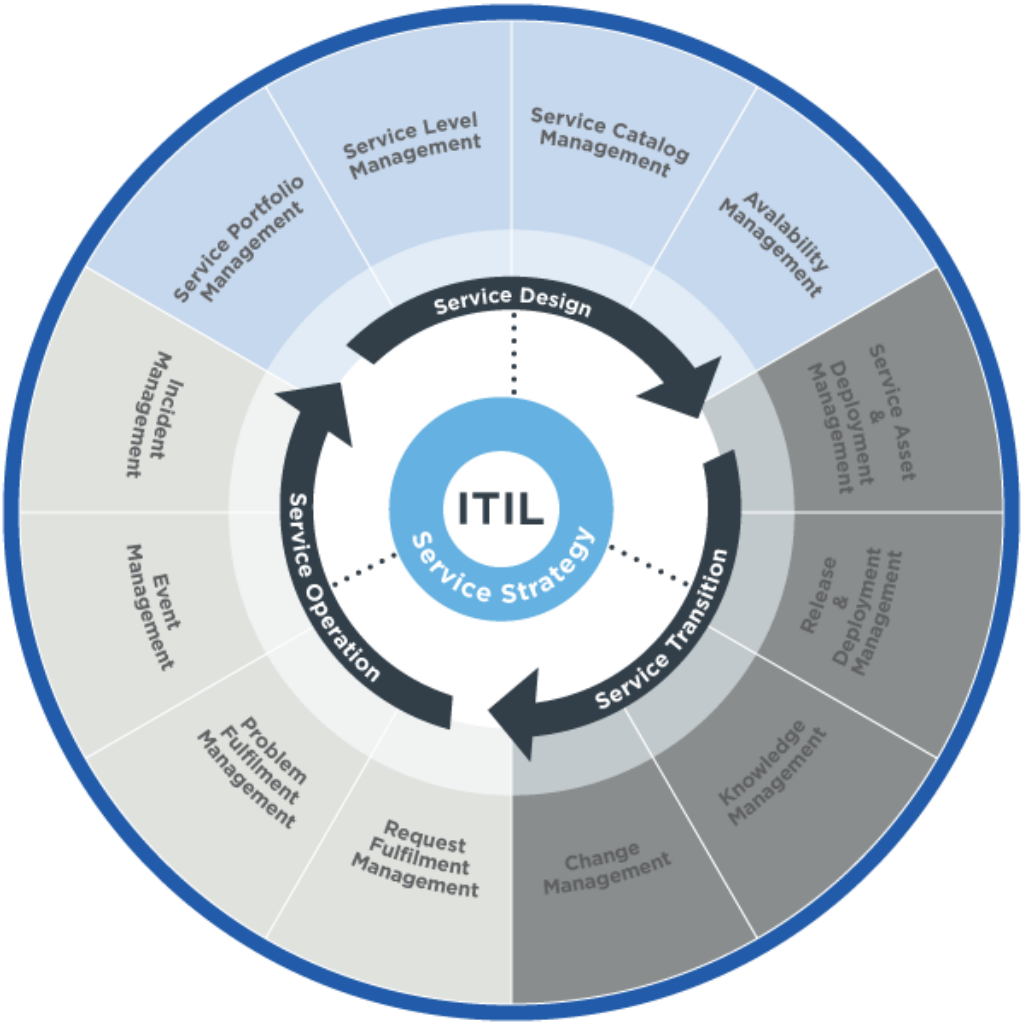

Figure 2.1: Overall IT Service Management Lifecycle [Retrieved from: https://www.cherwell.com/library/essential-guides/essential-guide-to-itil-framework-and-processes/]

Such as other organizations, Telstra has used the ITSM lifecycle to achieve their goals. In order to get fruitful result, Telstra has been collaborating with many other multinational companies, so that they could make a proper plan and utilize them in an appropriate manner (Telstra practices, 2019).

Figure 2.2: Telstra's initiatives for IT Service Management [Retrieved from: https://www.flycastpartners.com/itil-service-lifecycle-guide/]

With the vison to enhance themselves as the top leading information service organization and to expand themselves in an International market Telstra made some strategies to fulfill their requirement as:

- ➔ Optimization of their returns from traditional telecommunication services
- ➔ To focus more on the growth opportunities through mobile and internet services
- ➔ Transformation of old traditional cultures to more improved productivity
- ➔ Simplification of their product offerings by eliminating customers difficulty level and creating more digitalization
- ➔ Simplifying the way to provide services to their consumers
- ➔ Maintaining a customer portfolio and cost reductions programs

Telstra gave a clear look to their strategies made. They were able to create some service target and prioritize their requirements. They tried to design some efficient and cost-

effective services and some policies which they upgrade in a continuous manner. Designing is all about planning and organizing with the depth of the strategies. According to the objective of the design phase they were more focused to find out the solutions to meet their goals. They deal with the identification of appropriate suppliers and do some work on capacity management plans. They identify their threats and security challenges, which could lead them to be backward (Greene, n.d.).

Regarding the service operation, Telstra mostly was based on delivering services to their authorized users in tackling in a fast-paced environment. They acted as according to their service level agreements with optimize cost and better-quality systems. Till then they are capable of building customer satisfaction supporting high level performance. Telstra has so far managed its service transition from one phase to another. They came up with a proper transition planning supporting a good level of change management. They assured their demand as well as capacity management, which seems to be an important term in any organization. Their resource management capability has shown an outstanding result as they have already switched to the nbn internet services (Greene, n.d.).

The Continual Service Improvement mainly deals with extracting the opportunities for further enhancement. Telstra has been comparing its current services with their customer satisfaction and working to rebuild a system with more advance processing. Telstra has been evaluating its current processes and taking more initiatives to take their system to the next level and stand as a world's best evergreen telecommunication company. They have a proper improvement plan and a team of hardworking members to ensure that their service is functioning well and is on the way to achieve their goal (Greene, n.d.).

3. Financial Management

The main purpose of financial management is to manage financial resources wisely. It gives the detailed idea about the expenses, incomes, and cost. All the incoming and outgoing finance are evaluated and monitored so that the cost and value of any process or system can be improve. Telstra financial improvement can be seen by following figures:

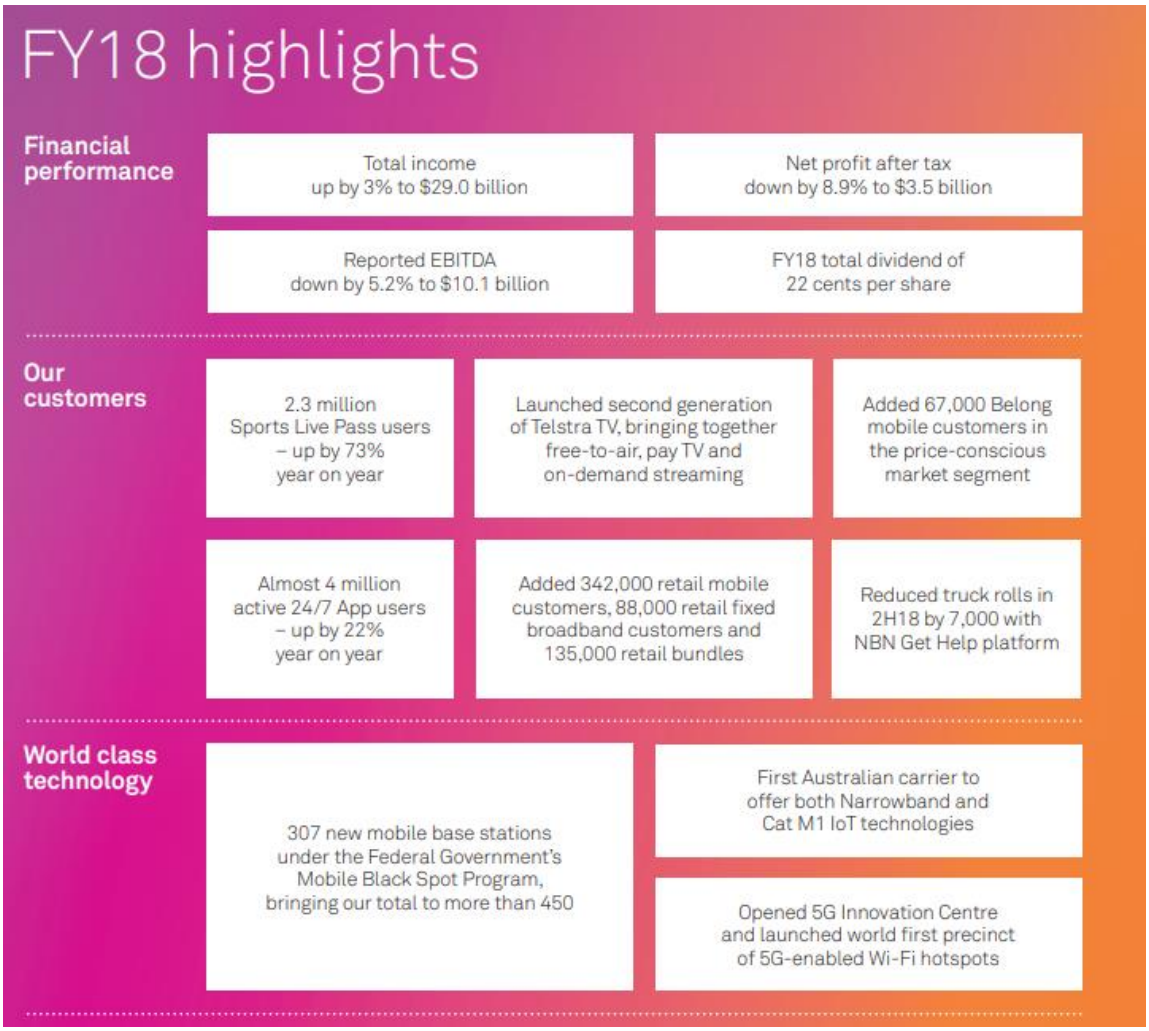

Figure 3.1: Financial description for year 2018 [Retrieved from : https://www.telstra.com.au/content/dam/tcom/about-us/investors/pdf%20F/2018-Annual-Report-singlepages.pdf]

4. Demand Management

Telstra has shifted its aim from becoming technological organization to customer focused company by introducing successful implementation of demand management, also known as Market based management (MBM). It has adopted MBM technology to give the customer different experience on their user satisfaction. In today's changing telecommunication industry, Telstra has its all concentration on user satisfaction. Telstra has done various research to adopt changes in its customer need by implementing various process.

- Technology

  Telstra has implemented various technology to meet its customer satisfaction. With the growing marketplace and competition, they have successfully implemented technology like Chabot, AI enabled interaction system. These system helps Telstra to manage the demand of the customer and current competitive environment. These AI enabled system allows Telstra to reduce human resources and also at the meantime, making customer services more flexible and reliable.

- Competitor Analysis

  As market area increase, the challenges faced by any organization also increases. As a result, the understanding of competitor is very important to change the system in order to attract more customer. Telstra uses various analytics methods like Telstra location insights, cross sell suite, churn predicting models which makes Telstra unique to adopt the changes to bring demand management in action.

- Cross functional teamwork

  Telstra has implemented this approach of working together, sharing information and building interactive network to solve problem arises by any customer. The main aim of this collaborative approach is to give customer a greater and positive experience.

The overall success rate can be seen by using following figure.

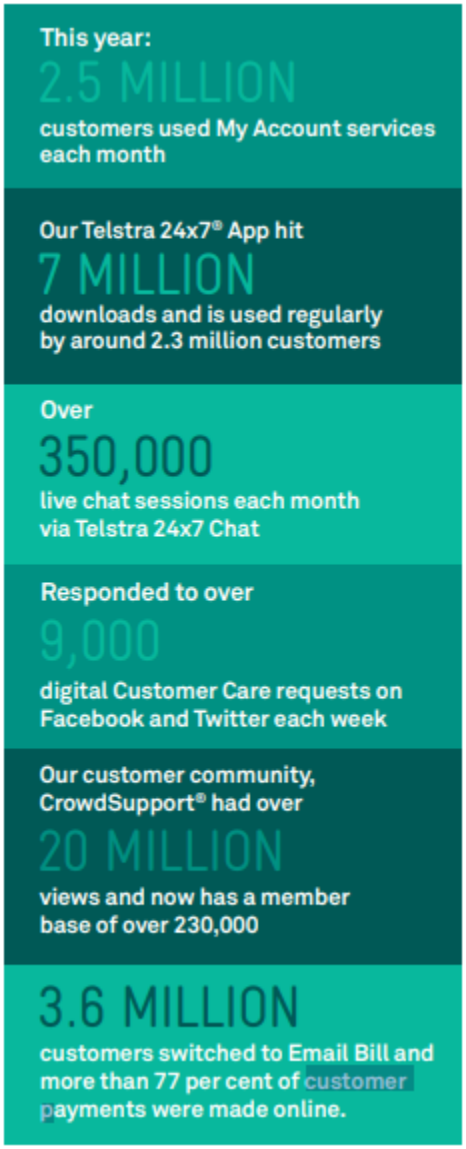

***Figure 4.1: Result of demand management* [*Retrieved from :https://www.telstra.com.au/content/dam/tcom/about-us/community environment/pdf/sustainability-report-2015-customer-experience.pdf*]**

5. Customer Relationship Management

Customer relationship management (CRM) is a method of managing good relationship with existing or possible future customers. Through CRM principles, company can use various sources of data to extract information so that company can focuses more on solving issue of customer and giving them more care. In order to maintain such relation, Telstra has invested nearly 40 percent of its budget to CRM (Cameron, 2019).

Telstra has moved from its traditional marketing technique towards automation enabled technology. Telstra believes that it's not only about people but also about the

technology, process and investment. They have started the program like 'first 100 days' customer program which focuses mainly on customer engagement without considering the channel through which customer interacts with the company. In addition to that, data complexity of customer is another source to improve CRM.

6. Risk management and security threats

Telstra is one of the biggest telecommunications business in Australia. It allows individuals to communicate via portable telephones, have Internet connections, pay charges and use many more facilities. In a corporation with several founders, Telstra spent trillions of USD. Telstra involves billions of individuals and is mainly concerned with their security. Moreover, cyber risk is prime issues in corporate IT network sector where often used of the information technology such as , main banks and mostly the telecommunication retailers were faced enormous challenges for their business , although according to our research "Telstra" was also the target of the cyberattack and in 12th July 2011, Telstra faced the major mailing issue where, 60000 customer personal details and the other data information was exchanged with to the other telecommunication user. (Aylin et al., 2018).

6.1 Risk management at the Telstra telecommunication

In the trend of the innovation and technolgoes world the internet facilities and techno stuff were increase rapidly, although the IT industry were very aware and also projected the risk analyser and paln to mitigates the forcaste risk which are very inportant to consider as the business policy and the risk are like currency cost ,competative threats, aduit risk and technology trails & tribulations. Form these were the telstra company was face the risk (including any material exposure to economic, environmental and social sustainability risks) that is very cost burden to the company were they invest muvch more percentage share money in the developing the risk management frame work (Mehta, 2018).

However, the risk management is play the vital role for the company to indicate the company issues and plan the solutation for the long-term, so here is the telstra risk mangement framework which is very top notch for the analyse the risk regarding the internal aduit and the internal aduit risk.

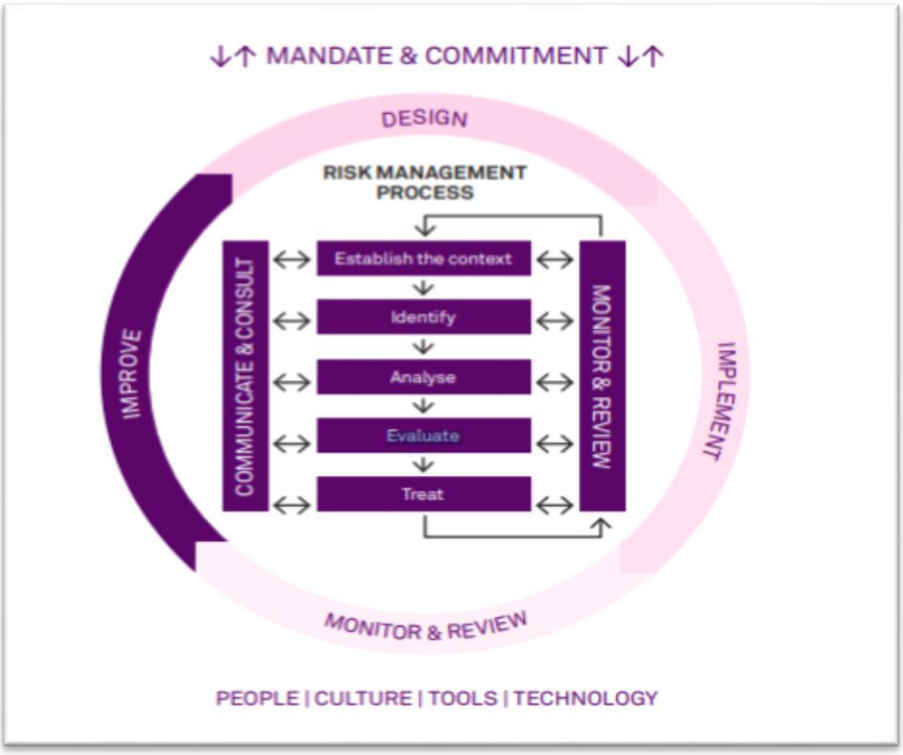

Figure 6.1: Telstra risk factor management framework [Retrieved from: **https://www.telstra.com.au/content/dam/tcom/about-us/investors/pdf%20F/2019-Corporate-Governance-Statement.pdf** ***]***

Moreover, according to this framework they can comprehend and analyses the risk and also help with the best strategy and business unbiased and the framework process gives the company a risk assessment method. Thus, they identify, monitor and report risks which prevent the achievement of our plans and objectives through this risk management process. This process were the risk leadership method guarantees that all kinds of inner and external hazards, including strategic, operational, financial and regulatory hazards as well as behavior, environmental and cultural development hazards are considered.

Furthermore, Telstra also take action to monitor and review our framework for risk management, ensuring it is functioning as intended. We perform assessments and self-examinations throughout our company at least annually and report the outcome to our Senior Risk Office and the Audit & Risk Committee. In order to recognize and execute possibilities for improving our structure, we use outcomes from these studies as well as suggestions from our 3rd line Internal Audit group (Governance at Telstra, 2019).

6.2 Malware Threats and security trends at the Telstra telecommunication

According to the "Telstra security Report 2019" originate that Awareness to and understanding of the Strategic Importance of Security grew, with 84 percent of Australian companies saying that in the next 12 to 24 months they will increase security budgets to $900,000 a year, currently averaging more to combats the risks and the security threats. However, the risk and the security threats that they are still facing and planning to mitigate these kinds of the exceptions such as Email threats and phishing

campaigns, Human error major risk factor and Ransomware is the threats which is very frightening (Australian cybersecurity magazine, 2019).

- Email threats and Phishing campaigns

Emails continue to be the primary communication channel for businesses, and it is therefore not surprising that phishing emails are the most popular method of delivery for cyber-threats. Via fraudulent pages / URLs, the next most common shipping technique. The objective of opportunity full e-mails in phishing is to make a recipient click on a malicious link, and the malware is downloaded and running at the bottom point of the network. The malware will then be able to create a backdoor to the C&C server, get more privileges for users and then move lateral to the target data via its network.

In Australia, the cloud technology called “First Wave” around the 1.5 billion emails were skimmed the customer emails which was inbound and outbound from the user customer mail server and the inbound emails which estimate to 800000 were blocked suspiciously. According to these activities they clue the activities as the “Fileless Malware” which is also address to destroy the victim computer system were the application software(anti-virus) is already patched and installed to their system, such as macros and plug-ins, which try to downloading the attachment behind the access of the user system. In addition, these kinds of threats were also happened through the mobile device were company also faced the major challenge and investing the major sources of cost to mitigate the issue.

- Human error major risk factor

The study states that human error is a significant cause of danger to IT security, often triggered by insufficient business processes and by staff who are unable to understand the security policies of their organizations. Human error or a targeted attack on an employee were cited as the highest risks to IT security by 36 per cent of respondents. Apparently, it was the cyber problem, which was previously repeated in the year 2011, where the customer data exchanged with the other user customer (Australian cybersecurity magazine, 2019).

- Malware Ransomware and Crypto Mining

Another popular way of malicious software is ransomware. In order to deny the availability of critical data and/or systems it targets human and technical weaknesses. Ransomware is often distributed on different channels. Phishing is a most popular infection vector for ransomware, where users are encouraged to press an apparently regular e-mail attachment such as an invoice or payment. The victim is suddenly installed on the computer once the file is opened. This attack spreads rapidly and often unknown files encrypted on the victim's device, and through connected networks. In general, the offender will require the deposit of a ransom if the person can no longer enter his or her information. The common way of paying is through cryptocurrency, like Bitcoin etc. Often the opponent will guarantee that once the sum is compensated by a fixed time, the person will be given entry to their information. If the payment is not made, the encrypted files are not available (Telstra security report, 2019)

Australia was the major spot of the malware threat in year 2016 in the Asia Pacific region and also according to the Telstra security report 2018, discuss that

Campaigns aimed at people or particular sectors are moved from ' spray and pray. ' Ransomware, and other ransomware observation are included:

- Research in the social media has helped opponents recognize person staff or agencies operating within their destination businesses.
- Some kinds of malware try to find ways first to attack backup systems and increase the ransom price.
- Ransomware as a service has enabled malware designers to provide their malware products to others via the dark web as an important medium for delivery.

In contrary, according to 2019 research finding on the Ransomware in Telstra company:

- **Attacks are unavoidable:** well, 32 percent of the participants from Australia stated that their company was disrupted "on a daily or monthly basis" from ransomware threats, amongst the sub-companies we studied that were suspended owing to safety violations in the previous 12 months. As contrasted to other developed countries, such as the United Kingdom, Germany and France, Australia's proportion is seen to be comparatively large; reported at 19, 27 and 26 percent respectively. 81% of respondents in Australia reported a ransomware attack among a subset of organizations interrupted because of a safety violation in the past 12 months. This represents a 5% rise over the preceding year. In the same area, 83% of Singaporeans and 93% of New Zealand people have recorded ransomware assaults over the last year (Telstra security report, 2019).

- **Cost paid to Ransomware**: Around 50% of Australians who were ransomware recipients recorded receiving the bill. This is a year-on-year rise of 4%. That level is greater than in the APAC and the European areas, where 48% and 50% show a cash payment respectively. The ransomware attacks reported in both Singapore and New Zealand have been more severe and also have the highest rate of payment after an attack (61%, respectively) (Telstra security report, 2019).

- **Data retrieved by payment to ransomware:** mostly, 77% of Australian companies paying a ransom were able to retrieve their details after payment. That is a 9 percent reduction annually. In the APAC region and in Europe, the numbers in 2018 were both 83 and 88 per cent greater than in Australia. Focusing on Germany and France, the figure was substantially greater by 96% (Telstra security report, 2019).

- **Future Payment to ransomware:** Despite the smallest information recovery level following ransom payments, 79% of Australian interviewees said that if no back-up documents were provided, they would receive ransom again next moment. That is comparatively large in terms of 75% and 73% respectively, relative with other APAC and European areas. Furthermore, nations like Germany and France with greater achievement rates for

information collection after delivery of ransom both showed a reduced risk for delivery of a reward at 78% and 68% (Telstra security report, 2019).

In 2018, Telstra initiated the preparation of a safety policy research report for any company in a country. One of the primary safety challenges is identifying and responding to attacks. The safety study by Telstra, which was established in 2018, discovered that approximately 68% of businesses face difficulties all because of their safety breach (Thomas et al., 2018). The reasons for the violation of security have been found the same in all listed companies as, unauthorized system access, electronically stolen or lost data, cyber-attacks and much more.

Telstra then found that every enterprise system needs a better visibility and a better way to handle the threats that may develop with time and innovations in order to guarantee greater security (Beashel et al., 2018). They have thus formed a security monitoring service that has been able to provide a good visibility service through the detection and notification of safety vulnerabilities, provide customers with a security problem response service to identify risks and find ways to mitigate them. Their findings were cheaper and might extend to any client not even involved in Telstra. Expertise is the one that can save the company from hazards. In order to recognize the hazards and administer them, they partnered a safety squad as well as business experts and information researchers (Vaile et al. 2018). In addition to technology development, Telstra continually employs state-of - the-art Big Data analysis instruments to investigate potential vulnerability, to be prepared to combat all such hazards.

It is not only that, but Telstra has the excellent plans to offer greater safety. The image below shows this reality.

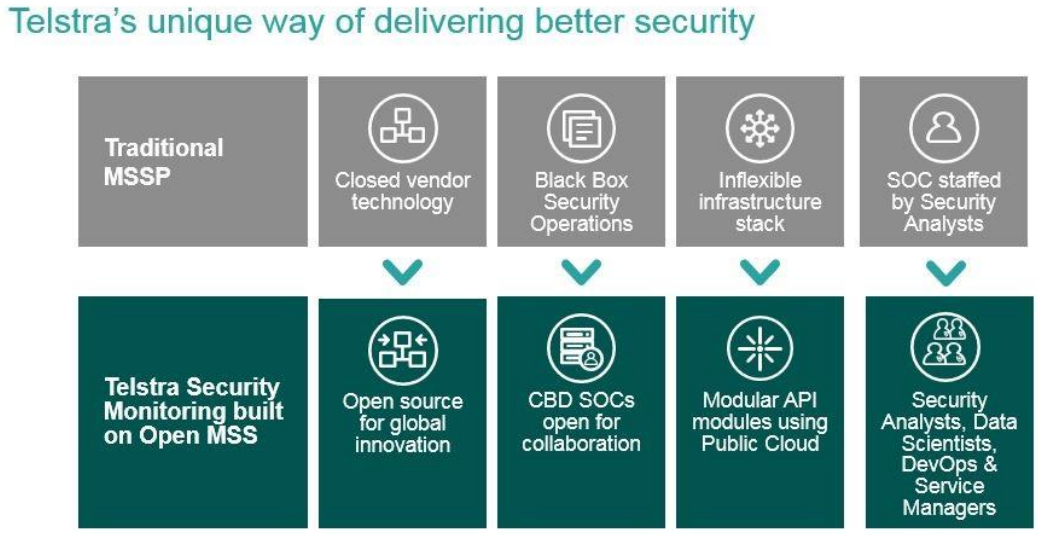

Figure 6.2: Telstra unique way of delivering better security.[Retrieved from:https://www.telstra.com.au/businessenterprise/solutions/security/security-monitoring]

Thus, it was rendered apparent by means of the case study on the safety strategy of Telstra that a remedy is available that can improve the company to all the risks. Other business systems can therefore also develop such technology to render themselves safer.

7. Continual Process Improvement Model

When focusing on continuous improvement, many strategies and methodologies can be used. It is important to find the right one for a industry as it will help maximize the results. However, making ongoing improvement in performance, commitment, strategy, and process all help build up the company's bottom line. This image also illustrates that any improvements in these four categories will also help build up improvement in the overall quality being produced by the facility.

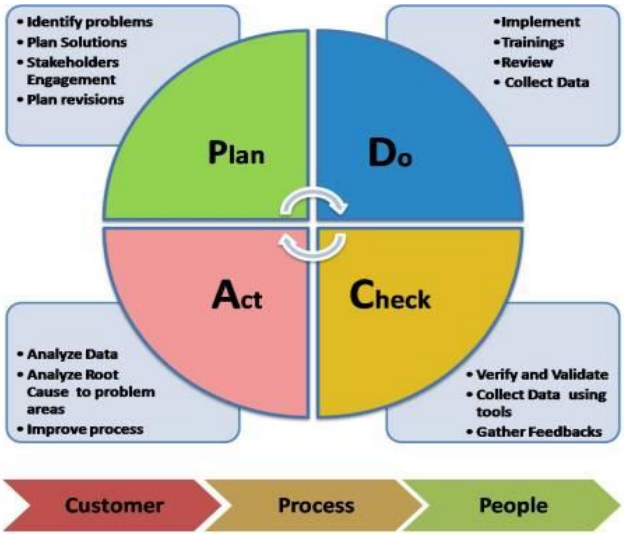

Figure 7.1: continuous quality management model
[Retrieved from: https://techdocit.wordpress.com/tag/pdca/]

Plan-Do-Check-Act

Another helpful concept is the "plan, do, check, act" process. This is a cyclical process that walks a company or group through the four steps of improvement. By continuing to cycle through these steps, improvement is always being worked on and evaluated (Desai, 2016).

Plan - During the scheduling stage, teams evaluate present norms, develop thoughts for changes, define ways of implementing these changes, set out targets and draw up the action plan (Desai, 2016).

Do - Implement the scheme creation in the first phase not only to change the process, but also to provide instruction, to raise consciousness and to add checks in order to prevent possible issues (Desai, 2016).

Check - New measures are an significant move in this regard to compare with the measures made before the shift. Analyze the findings and adopt any corrective or preventive measures to guarantee that the required outcomes are accomplished (Desai, 2016).

Act - The management teams analyze all the data from the change in order to determine if it will become permanent, or if further changes are required. The act features in the plan phase as it is time to start looking for fresh methods of doing further improvements once a shift has been completed (Desai, 2016).

8. References

Beashel, G., Simon, F. T. M., Males, E. W., Dan, C. E. O., & Galligan, A. S. M. C. (2019). NEWS IN BRIEF TELSTRA ANNOUNCES. Australian Canegrower.

Cameron, N. (2019). An insider's guide to customer marketing at Telstra. Retrieved from https://www.cmo.com.au/article/553661/_an_insider_guide_customer_marketing_telstra/

Cameron, N. (May 25, 2015). How Telstra is applying data analytics to customer experience. Retrieved from

https://www.cmo.com.au/article/574112/how-telstra-applying-data-analytics-customer-service/

Colley, A. (March 03, 2017). How big data analytics can help your business. Retrieved from https://smarterbusiness.telstra.com.au/trends/emerging-technology/how-big-data-analytics-can-help-your-business

Creative Safety Supply (May 3, 2017). Focusing on Continuous Improvement in the Workplace. Retrieved from https://www.creativesafetysupply.com/articles/continuous-improvement/

Desai, P. (July 11, 2016). PDCA – Total Quality management overview. Retrieved from https://techdocit.wordpress.com/tag/pdca/

Governance at Telstra (2019). corporate governance statement: Assurance and risk management, Retrieved from https://www.telstra.com.au/content/dam/tcom/about-us/investors/pdf%20F/2019-Corporate-Governance-Statement.pdf

Greene, J.(n.d.) The Essential Guide to ITIL Framework and Processes. Retrieved from https://www.cherwell.com/library/essential-guides/essential-guide-to-itil-framework-and-processes/

Mehta, A. (2018). Risky business: *Telcos' top 5 hazards - TM Forum Inform*. Retrieved from https://inform.tmforum.org/insights/2018/07/risk-business-telcos-top-5-hazards/

More, Elizabeth & Mcgrath, Michael. (2011). Strategic alliances as collaborative strategy or a method of implementing strategy: A case study.

Ross, Peter & Bamber, Greg. (2019). Changing employment relations in former public monopolies: Comparisons, contrasts and strategic choices at New Zealand Telecom and Telstra.

Thomas, J., Barraket, J., Wilson, C., Cook, K., Louie, Y. M., Holcombe-James, I, & MacDonald, T. (2018). Measuring Australia's digital divide: the Australian digital inclusion index 2018.

Telstra security report (2019). Summary report: security threats and trends Retrieved from https://www.telstra.com.au/content/dam/shared-component_assets/tecom/campaigns/security-report/Summary-Report-2019-LR.pdf

Telstra (n.d.) Research and Analytics. Retrieved from https://www.telstra.com.au/consumer-advice/your-information/research-and-analytics

Telstra (June 20, 2018) Telstra sets new strategy to improve customer experience, simplify structure and cut costs. Retrieved from https://www.telstra.com.au/aboutus/media/media-releases/Telstra-sets-new-strategy-to-improve-customer-experience-simplify-structure-and-cut-costs

Telstra practices (2019) Telstra global services practices. Retrieved from: https://www.telstra.com.au/content/dam/tcom/business-enterprise/consulting-services/pdf/telstra-global-services-capabilities.pdf

Vaile, D., Zalnieriute, M., & Bennett Moses, L. (2018). The Privacy and Data Protection Regulatory Framework for C-ITS and AV Systems Report for the National Transport Commission. *Report for the National Transport Commission, 2nd July*.

Warwick, B. (June 20, 2018). Creating industry leading cost and portfolio management | Telstra Exchange. Retrieved from https://exchange.telstra.com.au/creating-industry-leading-cost-portfolio-management/