MOBILE PHONE SECURITY INVESTIGATION

Information Security

RONA ROSAL
N10360387

Preliminary Executive Summary

This report will showcase the information asset of my personal mobile device, it will discuss its hardware, software, and data features how it is used and what purpose does it bring to me as a user. In addition, this report will also highlight the importance of mobile security, provide situations that talks about its threats, vulnerabilities and attacks. Moreover, this report will also cover the privacy policy of my most used social media application Facebook. The primary aim of this report is to highlight the importance of mobile security, how to protect information asset and cover different scenarios that relates to security confidentiality, integrity, and accessibility. Furthermore, it talks about the process of data storage, collection, usability, and transmission of Facebook. The methods used that can be seen in this report is a combination of Qualitative and Quantitative type of data analysis. Qualitative for the descriptive section and user experience with the mobile application and mobile device itself. On the other hand, Quantitative for some of the statistical aspect of the report such as the amount of time of using the mobile device, storage, and data.

This report is limited to the discussion of Mobile security, my personal Mobile device and its information asset, security issues that comes along with the different aspect of mobile device and application. Moreover, the privacy policy of Facebook and its risk analysis. In addition this report will also discuss the control/counter measure of the identifies risks.

As such, at the end of this report it is expected that the reader will have a better understanding on mobile security, Facebook’s privacy policy, and control/counter measures of the identified risks.

Table of Contents

Introduction

According to Peck (2020), Mobile devices may experience security breach due to users may not taken to consideration that these devices are also vulnerable to attacks.

Mobile security has been overlooked and some users may not realize that these devices that are not protected by firewalls like computers in a work setting may give attackers the opportunity to make a move. It is stated that 80 percent of work on a daily basis are used in mobile devices. In addition, mobile devices are linked to documents or sensitive files related to work through work emails that may cause additional damage in an occasion of an attack. Some damages that could cause these are confidentiality and integrity breaches of sensitive information from a company. Moreover, attackers may used endpoints of devices and use this as a vulnerability to attack the user and retrieve information.

Therefore, it is important to always keep mobile devices updated to improve security and bug fixes, this will elevate the sense of security for the mobile device and hopefully lessen the risk of attacks.

The purpose of this report is to highlight the importance of mobile security, identify security breaches, and provide risk assessment on mobile security issues related to my installed mobile applications, operating system, user behaviour, and physical threat to my mobile phone. It will cover and discuss each security issues' threats, vulnerability, and security attacks.

Moreover, this report will also talk about the importance of privacy policy of my most used mobile phone social networking application which is Facebook.

The purpose of the privacy policy section is to discuss and investigate how Facebook collects, stores, transmit, and allow third party applications to its user's personal data. It will cover the importance of privacy policy, the type of data to be collected, how it is shared, used, and handled. In addition, the articles used in this report uses a combination of qualitative and quantitative type of analysis. It will measure the likelihood of risks reoccurring and what mitigation strategies are available to improve mobile security.

Moreover, the contribution of this report is to provide a deeper understanding of security issues associated with a mobile devices, applications, and what are control/ counter measure that may be undertaken to minimize risk and consequences.

This report is limited to discussing the importance of mobile security, information asset of my mobile device, risk assessment of mobile security issue. Moreover, the privacy policy section of this report is limited to discussing privacy policies of Facebook. In addition, the risk control/counter measure section is limited to discussing the types of measures that can be undertaken, its degree, and limitations. Moreover, conclusions and recommendations for the identified risks are also discussed.

Context Establishment

I. Information Asset

a. Hardware

In 2014 according to (The unofficial Apple Keynotes channel, 2014, 1:24), Apple has created yet the biggest advancement in the history of iPhones. Since the first launch of the iPhone (first generation). The latest release is a primitive model of the previous model but the improvements have been said to be pushed to its limits (Gilbert,2017).

Moreover, some of the noticeable improvements that the new iPhone 6 that Apple created for its users is the overall change of the phone's physical appearance, created with a complete stainless steel that comes with two display sizes equipped with retina HD display. In addition, over 1 million pixels is incorporated in it. Furthermore, iPhone 6 is also measured at 6.9 mm thin allowing the phone to be recorded the thinnest phone apple has even made. According to (iPhone 6 Specifications, n.d) The iPhone 6 is composed of a 1.4 GHz which allows it to have a total of 1,4000,000,00 cycles per second. At the moment, the fastest range a phone can have is a GHz from 1.8 – 2.0, However, anything above GHz is an acceptable speed for a phone. In addition, it is also installed with a 1 GB RAM. Moreover, Apple has offered its user the ability to choose from 16, 64, and 128 GB for the internal storage of iPhone 6. This allows users to store more files and download more applications. iPhone 6 is equipped with a Lithium Polymer type of battery which according to CED Technologies (2010) Lithium Polymer batteries are 4 times the energy of density of nickel cadmium or nickel metal hydride batteries. These batteries are lightweight and may be trimmed down or scaled up to any size. In addition, these batteries may also be used for laptops.

In addition, according to iPhone 6 specifications (2010), some of the communication components that the new phone provides its user are LTE category up to 150 mbps, modem features such as GPRS, EDGE, and LTE, and as well as Wi-Fi and Bluetooth features. The phone also has a Type C USB cable for charging and connecting purposes.

Moreover, the iPhone 6 has a A8 chip with 64-bit architecture and a M8 motion coprocessor.

b. Software

The latest iOS/ operating system that is supported by my iPhone 6 are iOS9 – iOS 12. The current version installed is iOS 12. 4.8. According to Apple (2020), some improvements made by Apple to the new iOS 12 are an upgrade to emoji's and text messages to provide a more lively and entertaining environment and creative ways to express user's messages, Siri, considered as the intelligent assistant of apple users were also improved to make searching more efficient, the intelligent assistant is now more sensitive with the "Hey Siri" command. Moreover, Augmented Reality was also included as an advance feature, and finally, bug improvements and security upgrades were also updated to provide a more user friendly and secured mobile software.

My mobile device is mostly used for recreational and social networking purposes. Some of the most used applications on my device for social networking are Facebook, Instagram, Twitter. This helps me stay connected with loved ones and be updated to current news. Furthermore, I use the Clock, Camera, Gallery, Maps, Weather, and Text Messages application daily as well to help me with my personal activities and errands.

On the other hand, the least used application on my Mobile devices are stocks, Find iPhone, Voice Recorder, and Travel Applications.

a. Data

The phone has a maximum 64 GB storage memory and currently hold

478 videos, 1,358 photos, 46 applications. In addition, other important data that is store in my mobile device are contact information of family and friends. My social

media applications are also linked to my sensitive data information which can be critical when breached. The total used data storage is 58.4 GB. Other entertainment files such as music is stored in the application Spotify and not on the phone itself

II. Device Usage

a. Sensitivity, criticality, and importance

Information stored in my mobile phone is highly sensitive and valuable. Some of these data cannot be duplicated and would cause serious damage when breached. Some of the data that is stored in my mobile device that I consider highly critical are photos, videos, contact information, social media and bank accounts. These accounts are linked to my bank account and may potentially cause serious damage such as financial loss if it falls into the wrong hands. Furthermore, the social media applications installed in my phone are automatically logged-in into the accounts, in an occasion that my phone gets lost or stolen the attacker may have access to these accounts which will cause to a breach in my confidentiality, accessibility, and integrity. Moreover, I use my mobile device almost 24/7 for daily errands such as communicating with loved ones, checking emails, paying bills, getting news updates

b. Applications

The screen time statistics for my mobile device shows that I used my phone on an average of 35 hours and 21 minutes for social media and networking alone, with an average of 7 hours per day. Some of my most used social media application are Facebook, Twitter, and Instagram. I used these applications mainly for communication purposes and to keep track of daily news.

Risk Assessment

I. Security Issue associated with mobile device application.

Title: TikTok is facing a global backlash over security concerns. Should we be worried about it here?

Author: Cameron Wilson

Reference details: Wilson, C. (2020 July 8). TikTok is facing a global backlash over security concerns. Should we be worried here?. ABC News. Retrieved from https://www.abc.net.au/news/science/2020-07-08/tiktok-national-safety-china-social-media-ban/12434308

Date Issued: July 8, 2020.

Brief summary: The video sharing platform 'Tik-Tok' has received scrutinization globally due to information breaches and security concerns. Countries are worried that the communist government of china may use information worldwide to make attacks to foreign countries.

Information asset: The information involved in this issue are the movement of Tik-Tok users in the application. In addition, sensitive information such as contact details and location may be exposed and may be considered as a breached in user confidentiality.

Security issue

Threat: The threat that may be used in this issue is a human deliberate action. The reason why this have been a big issue to other countries is due to the system that the china government runs. The Chinese government can anytime have access to sensitive information from Tik-Tok users.

Vulnerability: The vulnerability of this does not lie on the application itself, but to the government and authorities that controls how information is stored and used. According to ABC News (2020), In 2017 China has implemented a law that compels individuals and companies to turn over collected sensitive and personal data when needed by the government.

Security incident /attack: There have been no signs of attack from china through Tik-Tok to other countries but it is clear and evident that china has a strong desire to retrieve personal information of people from other democracies and it own citizens. In addition, it was stated that organization funded by the Chinese government has been behind attacks on financial institutions, travel records, and university records. These information is seen as a massive threat to security for other democratic countries.

II. Security Issue associated with mobile device operating system

Title: Apple iOS 13.1.3 is causing some of iPhone 11's to fail.

Author: Gordon Kelly.

Reference details:

Gordon, K. (2019). Apple iOS 13.1.3 is causing some iPhone 11's to fail. Forbes. Retrieved from https://www.forbes.com/sites/gordonkelly/2019/10/20/apple-ios-13-1-

3-u1-ultra-wideband-failure-iphone-11-pro-max-update-iphone-xs-max-xr-upgrade/#4eac37c11c4c

Brief summary: Apple has released a new update on its operating system called iOS 13.1.3, hoping to improve the phones system with newly built in functions and bug fixes. However, it has caused more damage than good due to a chip failure that caused users to replace the entire device.

Information asset: The information asset involved and compromised in the situation was the overall database of the phone. Asset is disrupted when the user updates the phone and the Ultra wideband U1 chip failure pops-up.

Security issue

Threat: The threat that can be observed in the situation is an internal undeliberate threat due to the malfunction was caused by the system and not by human action. This may compromise the security goal availability: once the user updates its iPhone to the new version, there is a possibility that the update might go on a complete failure causing the phone to be unresponsive and remain on a loop. Therefore, the company is forced to replace the entire device with a new one leaving the user with no choice but to lose current data stored in the old device.

Vulnerability: The vulnerability was the incompatibility of the U1 chip to the new software update. Although Apple claims that this update failure is cause by the hardware, it has caused many users damage in their assets and lose sensitive and important data.

Security incident /attack: One user stated that one of the problems that they have experienced was the failure to transfer files from one mobile device to the other through Air Drop, the connection fails to send information to receiver. When the user tried to resolve the problem to reset and setup nothing was achieved causing the user to return/ replace the device.

III. Security issue associated with mobile device user behaviour.

Title: GAO Report: Expired Certificate Allowed Extended Exfiltration

Author: Robyn Weisman

Reference details: Robyn Weisman (2018, November 09). GAO Report: Expired Certificate Allowed Extended Exfiltration. Venafi. Retrieved from https://www.venafi.com/blog/gao-report-expired-certificate-allowed-extended-exfiltration-0

Brief summary: In the year 2017, one of the most controversial data breached happened when Equifax announced a breached that expose personal information of 147 million people. This happened due to an expire certificate.

Information asset: The information asset involved in the situation was the personal and sensitive information of people involved on the breach.

Security issue

Threat: The threat involving the breach may be considered as deliberate human attack, no one can really be sure that the breach was done unintentionally. This threat is a damage to the asset's confidentiality and integrity to the company involved.

Vulnerability: Lack of employee training and following of protocol. The system should have been updated and secured regularly to prevent disruption in the system. The attackers saw an opportunity when they realized that expiration dates were incorrect.

Security incident /attack: The employee/company involve fail to correctly manage the expiration date of certificates, it was stated that the expiration date happened 10 months ago before the breach was recognized.

IV. Security issue associated with physical damage.

Title: Dodgy Xiaomi Smartphone bursts into flames.

Reference details: Richards, D. (2019 November 20). Dodgy Xiaomi Smartphone bursts into flames. Channel News. Retrieved from https://www.channelnews.com.au/140834-2/.

Brief summary: Unauthorized Xiaomi phone sold in an Indian market burst into flames. It is strongly advised that customers should only purchase at a legitimate reseller of the phone such as JB Hi-Fi.

Information asset: Aside from the important and sensitive data that can be found inside the phone, one more asset that is damaged by the event is the physical phone itself which can be called a property asset.

Security issue

Threat: The threat that can be observed involving the incident would be integrity and availability due to the company that is selling the phone would be in charge of the damages done. In addition, the official company stated that they will not be liable for the damages due to it was not their original product that was marketed. On the other hand, the availability of asset is also damage due to the explosion of the physical asset.

Vulnerability: It was stated that the batteries used in making the class A Xiaomi phone were not approved to be used for charging in Australia.

Security incident /attack: The attack happened when Mr Ishwar had his phone unattended for charging and after a few hours noticed a smoke coming from the device along with a burning plastic smell then after a few minutes blew up in flames.

V. Personal information summary

Based on the situations stated above, as the owner of the mobile device the asset that I consider the most at risk and valuable would be the applications. Most valuable information such as social media and networking sites can be found here. This is also the only way I can connect with my family overseas without any hassle, meaningful and sensitive conversation are all part of this asset. One of the vulnerabilities that could exploit and disrupt this valuable asset would be a lack of security feature in it. Usually, social media application installed in a mobile device are automatically logged-in into the owners account so it is very crucial to have a security code even before having access to the social media account. One way to strengthen the security of a social media application is by applying Two - Authentication code that I use in all of my applications. This allows unrecognized log-in to be double checked by me for verification in case anyone tries to access my account. In an event this asset is damaged, security breaches such as confidentiality, integrity, and even availability may occur.

Privacy Analysis

I. Privacy Policy Summary

a. Name of App: **Facebook**

According to Web-wise (n.d), Facebook is a social networking platform where users are able to find people, share, communicate, and build business with each other. Furthermore, it is one of the most used social media platform with a record of over 1 billion users.

The details stated below are information taken from Facebook's privacy policy section provided by the said social networking platform. The privacy policy is available at https://www.facebook.com/full_data_use_policy.

b. The type of information collected

- **Information the user provides / Personal Information** - upon the sign-up application in the on the Facebook application, the user must provide personal information such as name, email address, password, residential address, and even a picture to create an account. These are all kept by Facebook for them to provide suggestions based on the personal interest of the user.
- **Networks and Connections** – Facebook collects information that is associated or link to the users existing information to make it easier for user to search for specific things on the platform such as pages, people, and other interests.

- **Application usage** – Facebooks keeps tracks on how the user makes use of the application by keeping records of the users search history, liked pages, and many more.
- **Transaction information** – Facebook may be used as a business platform. One new feature added by Facebook was a section called ‘marketplace’ where users/ business owners are able to showcase their products to the the general public. In exchange to this facebook provides the user an option to add in their debit/credit card details to be saved to their account so that transactions between buyer and seller are easier to manage.
- ***Other information provided by friends* –** Information provided by people and businesses connected to the user is also kept by Facebook, some of these data are comments, uploaded and tagged photos, messages and other contact associated with the account.

c. *Collection Method*

Facebook collects information through information given by the user. Upon registering and making an account the application asks users for personal information such as name, address, email, password, etc. Once information is given by the user, Facebook collects additional information through a connection with the users logged-in device. Retrieved information across device used by the user is the gathered by Facebook linking it to the user. In addition, user search history is also taken into consideration. Moreover, the application asks users if it allows linking/collection of other personal information.

d. *When the information is collected?*

Information is collected every time a user takes action within the application. Furthermore, information is also collected when using other linked social media account linked to the Facebook account. In addition, personal information of the user is collected when the user provided his/her details from the creation of the account. Furthermore, some information is collected through the users search history.

e. *How relevant information is to your app?*

Information such as personal/ business detail is very relevant for the application due to it is a social networking site. This means a user are recognized behind an account which will help other user identify each other. This is very relevant when it comes to finding other users within the application and communication purposes.

f. *How information is used by app providers?*

Facebook uses this information in a variety of things, these information are used for the following:

- **Information Across Facebook product and devices -** Facebook makes use of personal account information to provide user a complete experience of the application. Users often links their Facebook account to other social networking site accounts such as Twitter or Instagram, Facebook then uses the information gathered from these linked account (such as search history / people a user may know) to make suggestions to the user, providing the user a smoother more efficient experience in the their Facebook account.
- **Location related information** – Facebook uses location features that allows users to share their exact location through post or direct message.
- **Ads and other sponsored content** – related to search history, Facebook uses the gathered information to filter ads that would best suit the user.

Based on the search history, likes, and interest of the user, this allows Facebook to prioritize products that should appear on the users timeline.

g. *Information Storage*

According to the data policy of Facebook, data is stored as long as it is necessary for the application and its services. However, Facebook does not implicitly state how long data is stored in the application.

h. *Use of Encryption*

According to Zuckerberg (2016), encryption is used for a wide range of information in the platform such as messages, bank credentials, and its history data. Moreover, the encryption process is observed when a user sends a message to another user, the encryption happens during the transferring of message and other data.

i. *Information Sharing*

Facebook clearly states that they don't sell any information obtained from their users and has strict restrictions on how data is used and shared. Here are some of the third parties that Facebook share data information:

- Partners / Marketing Purposes / Advertisers – Facebook share analytics to partners for business purposes. It does not show directly a user's information such as name, email address, or account. Instead, it juts provide analytics to help business know how consumers interact with their products and how many people it reaches to improve their arketing.
- Researchers and academics – Facebook shares dara information to help improve research and provide advance knowledge with regards to general social welfare, technological advancement, public interest, health, and well-being.

- Law and legal purposes – Facebook only shares data when needed and required by the law.

j. *App users access to information*

Facebook allows its users to have access to their own collected data.

In the general settings section of Facebook, it has a section/ feature wherein the user is able to download all existing data related to his/her account. This may take roughly 10 mins or more depending on how large the accumulated data is.

II. Privacy risk identification and risk analysis

a. *Which sort of analysis can you perform*

(Tulane University School of Professional Advancement, 2020) shows several list of risks that can be found in using social media:

- **Data Mining** – Companies may use information from a user account on a social media platform such as Facebook to achieve better target in advertising without their consent. According to IEEE Xplore (2003), attackers ay use data mining to gather large amount of data and patterns from Facebook's database and use the user information to their advantage resulting to a breach in confidentiality.
- **Phishing Attempts** – this type of attack is very prevalent on Facebook. Attackers uses links/message/emails to trick their target, once the target has click on the sent link, it allows the attacker to know sensitive information about the target such as social media emails and passwords and have access to the targets account resulting to a breach in confidentiality, integrity, and accessibility.

- **Malware Sharing –** This type of attack is interconnected to the phishing attack, once the attacker has gained sensitive information for the target through phishing, the target’s social media is now then use to distribute malware viruses to the targets Facebook friends resulting to a breach in confidentiality and integrity.
- **Botnet Attacks –** an automized attack used to have access to sensitive information from a user such as their email and passwords, send spam messages and even launch a denial-of-service attack to a user resulting to a breach in confidentiality and accessibility. Moreover, according to Akamai (n.d), one of the most used botnet attacks to steal information is by using trojan viruses or web application attacks to steal user information. The attacker targets the computer security system before implementing malicious activities and gathering data.
- **Identity Theft –** An attack that targets in getting the personal and sensitive information of a user. Such information includes name, address, government document details, place of birth, family member details, and online account username and login details. When these information are collected the attacker may user it to his/her advantage and may be a breach in confidentiality, availability, and integrity of the victim.
- **Financial Loss –** Some Facebook account are linked to a user’s credit card details. In an event an attacker gains access to that users account the attacker may be able to have access to the users credit card information and use it to his/her advantage.

Using a Quantitative analysis for assessing the risks and evaluating the potential damage of the impact of the attacks will give the user a detailed and scalable measurement for decision making. In addition, According to Goodrich (n.d) quantitative analysis can be more suitable and more realistic when assessing the likelihood and probability of the risks mentioned above. This can be achieved by performing scale check which will require a huge amount of data from the user and the system. Moreover, this will help the risks to be categorized to give the user a clear perspective of the impacts and perform deeper analysis of the problem which leads to a well thought out solution.

b. *Limitations and difficulties encountered*

The difficulties encountered in the making of this report is identifying privacy risks that a user may encounter on Facebook, I found it difficult to look for references with highly relevant examples that associates with the risks of using the application.

Privacy Summary

Facebook has become one of the most used and most important application installed in my mobile device. The average time usage for Facebook on a daily basis would be 7 hours, it has become my primary medium to communicate with distanced family, friends, and also allowed me to discover and meet new people. Moreover, I also use this application to stay updated with current news.

Facebook is not limited to being a communication / social networking platform, it may also be used for business purposes such as marketing, and may be also be a tool to help in gaining knowledge through the use of researches to help improve social and technological advancement by using the data it collects.

The collection of data is performed by the input of its users, interests, search history, and other accumulated data related to the user's account. The information collected are the user's personal information such as their name, email address, location information (if the user permits access), and other information associated to the user's account such as other linked accounts and information gathered from friends.

Gathered information can be highly sensitive due to if it is breached it can cause a breach in confidentiality , availability, and integrity due to the it contains personal messages, email address, password, and even address locations. In addition, financial disruption may also take place if the attacker aims to steal the users identity. Considering the assets involved in the risk identification, some of the assets that are of great risks are the personal information of the user and financial credentials linked to the application.

Based on the privacy policy given by Facebook, it can be seen that the application follows the proper handling of user data required by the Australian privacy legislation such as the collection, use and disclosure, and even access to the user's collected data.

III. Risk treatment and countermeasures

I. Mobile device application (Risk assessment)

Overview of security issue

In the risk assessment associated with mobile device application, the vulnerability in the 'TikTok' application regarding security concerns

(Wilson,2020) was discussed. This has raised a global concern due to the application was rumoured to be using user data for the benefit of the government. This has risen concern due to the application was developed in China which is also known to be a communist government. The application is said to collect data such as user email, activities, and locations. This compromised the security goal confidentiality: ausers personal information such as emails, phone numbers, and location may be exposed to unauthorized third parties without the users consent.

Treating the risk

- ***Suggested control measure and explanation***

  According to Matsakis (2020), users may see blocking the application as a way to control or completely terminate its security concern. Furthermore, outlawing the application may also be an option but taking that action would only consider the US government similar to the laws of China. One effective way of control the security concern for TikTok is to strengthen its rules for protecting user data by implementing laws that prevents companies from data misuse regardless of which country the application is developed.

- ***Type of control measure***

  This is a preventive control measure aimed at protecting the user information. It prevents government/ third parties from having the authority of pressuring and attaining user data from companies which breaches user confidentiality.

- ***Degree of practice provided***

  Strengthening the rules for user data will give the user the protection when it comes to companies or third parties trying to attain the data provided. Having a law that sides with user data confidentiality will almost eliminate or reduces the likelihood of companies or third parties attaining the user data.

- ***Limitations of control measure***

  The decision to strengthen the rules of protecting user data is up to TikTok and the government may also have a contribution in it. They have the authority to implement restrictions on who are able to have access to user data's. Furthermore, TikTok may strengthen their application security to prevent third parties and malicious hackers from accessing information. On the other hand, government have the authority to also strengthen rules that are directly associated with the law.

  This will provide user a more secure user experience. Moreover, no additional technical equipment is needed for this upgrade and would not introduce additional risks.

II. Mobile device operating system (Risk Assessment)

Overview of security issue

According to Kelly (2019), the newly released version of IOS 13.1.3 has caused the operating system of the iPhone models that supports it to fail.

This issue has caused users greater cost when attempted to download the new version of the operating system due to it damages that entire system of the phone due to bugs which causes the phone to not operate or function anymore. Moreover, it is said that one of the causes of this system failure is the incompatibility of the phone’s UI chip to the new operating system.

Treating the risk

- ***Suggested control measure and explanation***

  This type of problem is best solved by apple, it is a problem in the operating system that apple have developed and in order for this new operating to be useable to its users the bugs in the update needs to be fixed. Furthermore, another control measure that can be of use is to not update to version that has bugs until a new version with fixes is fixed. Moreover, according to Hiley (2019), not updating to the latest IOS version is not seen as a problem to the useability of the phone due to it will still work normally with older version of IOS.

- ***Type of control measure***

  The type of control measure for not updated a mobile phone is a preventive type. This prevents further damages to the operating system of the phones which can cause in-availability.

- ***Degree of practice provided***

  The user not updating to a corrupted IOS update reduces the likelihood of consequences to be attained due to it prevents the user having the corrupted system in his/ device in the first place. No damage might occur to the user's device.

- ***Limitations of control measures***

  The limitation of this control measure that could prevent the damage of assets is up to its users. The users are able to decide whether to update into a new version of the operating system, reading feedbacks and reviews will help in making the best decision possible. Furthermore, it is also the responsibility of the manufacturer to make changes and provide fixes to the operating system to provide a more efficient and good user experience.

III. User Behaviour (Risk assessment)

Overview of security issue

Treating the risk

One of the most controversial breached that happened in the year 2017 was when Equifax, a company that helps users asses credit scores announced a breached in personal information of 147 million users. The breached happened due to an expired certificate causing an alarm to its users.

- ***Suggested control measure and explanation***

  Strengthen the administration. Focusing on the improvement of training and awareness of staff and personnel that handles data may help in minimizing breaches such as this one. Moreover, having a good company policy and procedures with handling data will also prevent breaches to likely occur.

- ***Type of control measure***

  According to Kenton (2020), this type of control measure can be classified as a detective control measure, wherein the company aims to control internal problems that have occurred by conducting inventory checks, review if reports and certificates as well as current controls. This control is associated with quality checks, fraud prevention, and legal compliance.

- ***Degree of practice provided***

  The control measure provided will help the company reduce the likelihood of the incident happening again. Strengthening its workforce administration will help minimize the risk to a great extent.

- ***Limitations of control measure***

  The limitation of this control measure is up to Equifax, how the company will train their employees in handling data and in improving their system and inventory check in checking expired certificate to prevent future breaches from happening.

IV. Physical threats to mobile device (risk assessment)

Overview of security issue

Unauthorized and illegitimate Xiaomi phone have been prevalent. These phones have been seen to be explosive and dangerous to its users (Richards, 2020) causing great damage to their health and other assets. It is advised that consumers should only purchase devices from authorized and legitimate sellers.

Treating the risk

- ***Suggested control measure and explanation***

  A control measure for this scenario is to only purchase mobile devices or gadgets at the original store or authorized seller to prevent buying fake phones that could potentially explode. According to Richards (2019) these phones does not have C tick approval which mean that the supplied battery for the Xiaomi phones are not compatible to be charged in Australia.

- ***Type of control measure***

  This is a preventive control measure. Users who buy unauthorized or illegitimate device often encounter problems with the purchased product to which in this scenario may put their life at risk! If buyers do not patronize illegitimate phone, the damage of explosion could be prevented.

- ***Degree of practice provided***

  Not buying an illegitimate phone can completely terminate the probability of the consequences of this scenario. In addition, knowing the compatible batteries that can be used in an Australian setting will prevent the likelihood of damage.

- ***Limitations of control measure***

  The decision to prevent the scenario from happening is up to the user and also authorities. The user can make a decision on whether they will patronize and continue to buy illegitimate devices that could cause further damage to them. Moreover, authorities have the power to ban seller who does not sell original products by implementing laws that would prevent it.

V. User Privacy

- **Overview of security issue**

  In the user privacy analysis, Facebook revealed that the company follows the Australian privacy legislation on how to properly handle, store, and transport data. However, information shared on Facebook may still be subject to a breach in confidentiality due to malicious hackers. Hackers may obtain information through the use of Phishing attempt, data mining, malware sharing and more which could lead to identity theft and financial loss.

- **Suggested control measure and explanation**

  Limit the sharing of sensitive personal information to the social giant. This will minimize the consequences in an event an attacker has successfully gained access to the user account. Incomplete information and useless information would prevent the hacker from stealing your identity. Furthermore, another control measure that could be considered is for Facebook to improve their security to make it almost impossible for hacker to enter the system or network and have the opportunity to gather data.

- **Type of control measure**

  This type of control measure is preventive due to it minimizes the possibility of potential damage to the user assets by improving the system and procedure associated to the application.

- **Degree of practice provided**

  Limiting of sharing sensitive user information will minimize the likelihood of a hacker to steal sensible information and using it for malicious activities. Moreover, Facebook improving their security system will slow down and hopefully prevent hacker from stealing user information.

- **Limitation of control measure**

  The decision to limit the information shared is up to the user. Information shared on social networking site would be carefully thought of due to sensitive information is visible to other users and could be a great risk when it comes to identity theft. Moreover, improving the security system and network of Facebook is u to the company, this will help the users of the platform to be protected due to it prevents hacker from entering other users accounts unauthorized.

Conclusion

Overall, the most applicable control measure for the security issues is the preventive control measure. This aims to minimize the impact of consequences of the issues discussed through improvement of policies, standards, processes, and procedures.

Firstly, for the security issue regarding the application TikTok, elevating or improving its rules and regulation for the user data security will alter the risk greatly in a positive way due to the company will be forced to abide to its new set of rules and standard protecting the user. In addition, applying this counter measure does not require a skill set or equipment. This will only require the expertise of authorized personnel to make changes in the existing rules and regulation on how to store and handle data properly of TikTok.

Secondly, for the security issue regarding the operating system of apple. Users who does proper research before installing a newly released software will minimize the risk of damaging their assets. Moreover, it is understood that newly released software will always have bugs and would require further fixes. Furthermore, a damage in the user's asset linked to this scenario is costly. In addition, it would require a great amount of expertise in order to solve this security issue.

Thirdly, for the security issue regarding user behaviour. Improving the workforce will be a big help in the daily operations and accuracy of the company due to it will result to a more efficient operation and minimize the risk and consequences. However, this control measure would require time, expertise, and money due to it deals with people who will undergo training to improve.

Fourthly, for the security issue linked to the threat of physical device/damage. Following the control measure of not buying from illegitimate vendors will greatly alter the risk of asset damage of the user. Following this measure would be a bit costly due to the buyer will transition to a low quality device to a higher one, however, this will greatly benefit the user due to he/she can be sure that the device is safe.

Lastly, for the control measures relating to user privacy. Limiting shared data will lessen the risk of having attacker extract sensitive information due to its limited sources. In addition, having Facebook improve their security and network will also be an advantage for the user. However, making these changes and improvements will be time consuming and costly for the social media giant. Moreover, will require expertise with handling the system

Recommendations

- **Improve security –** One of the easiest way to elevate the security of a user’s device is to add a password, two-authentication, or install security applications. This will prevent hackers from having access to a user’s mobile data and attaining data. This is usually done in the early stages of data protection.
- **Limit storing sensitive data –** This process solely depends on the user’s preferences. However, it is safer to not store sensitive information to devices such as mobile phones due to this device are high risk of being stolen or lost to which when found data is exposed to

unauthorized people. This is done in the early stages of data protection.

- **Provide encryption –** encrypting data is one of the most effective and safest way to prevent breaches due to even when information is accidentally exposed, unauthorized people are unable to interpret the data. This is best done in the early stages of data protection.
- **Install Anti-Virus applications –** Installing anti-virus applications helps in detecting potential hackers and also it protects your device from malicious attempts. This serves as a support when protecting data. May be done in the early to middle stages of data protection.

References

Apple. (2015). About iOS 12 Updates. https://support.apple.com/en-us/HT209084#1248

CED Technologies. (2010 May 08). The Advantages and Limitations of Lithium Polymer Batteries. Retrieved from https://www.cedtechnologies.com/advantages-a-limitations-of-lithium-polymer batteries/#:~:text=The%20main%20advantages%20of%20LiPo,almost%20any%20size%20or%20shape.

Franceschetti D.R.PhD. (2018). *Principles of Programming & Coding*. Salem Press, 2018. Salem press. https://ebookcentral.proquest.com/lib/qut/detail.action?docID=5433876.

Gilbert, B. (2017). It's been over 12 years since the iPhone debuted – look how primitive the first seems today. https://www.businessinsider.com.au/first-phone-anniversary-2016-12?r=US&IR=T

iPhone6 specifications.(n.d). Retrieved from https://www.citewrite.qut.edu.au/cite/qutcite.html#apa-internet-webpage

Peck, B. (2020 April 20). Mobile Security – the 60 percent problem. Microsoft.com. https://www.microsoft.com/security/blog/2020/04/07/mobile-security-60-percent-problem/

The unofficial Apple Keynotes channel. (2014, September 10). Apple Special Event 2014 – iPhone 6 & iPhone 6 Plus Introduction. Youtube. https://youtu.be/0T2HCbv9FBQ. Tulane University school of Professional Advancement (2020).

Webwise (n.d). Explained: What is Facebook? . Webwise.ic. retrieved from https://www.webwise.ie/parents/explained-what-is-facebook-2/

Zuckerberg, M. (2016). A Privacy-Focused Vision for Social Networking. Facebook.com. Retrieved from https://www.facebook.com/notes/mark-zuckerberg/a-privacy-focused-vision-for-social-networking/10156700570096634/

Akamai (n.d). What is a botnet attack?. Akakamai.com. retrieved from https://www.akamai.com/us/en/resources/what-is-a-botnet.jsp#:~:text=Cybercriminals%20initially%20gain%20access%20to,activities%2

0on%20a%20large%20scale.&text=Web%20application%20attacks%20to%20steal%20data

Goodrich, B. (n.d). Qualitative Risk Analysis vs Quantitative Risk Analysis. PM Learning Solutions. Retrieved from https://www.pmlearningsolutions.com/blog/qualitative-risk-analysis-vs-quantitative-risk-analysis-pmp-concept-1

Matsakis, L. (2020)., Does TikTok Really Pose a Risk to US National Security?. Wired.com. Retrieved from https://www.wired.com/story/tiktok-ban-us-national-security-risk/

Hiley, C. (2019)., Should I updte my phone to the lates version of IOS?. USwitch.com. Retrieved from https://www.uswitch.com/mobiles/guides/should-i-update-my-iphone-to-the-latest-version-of-ios/

Kenton, W. (2020)., Detective Control. Investopedia.com. Retrieved from https://www.investopedia.com/terms/d/detective-control.asp#:~:text=A%20detective%20control%20is%20a%20type%20of%20internal%20control%20that,as%20assessments%20of%20current%20controls.

Appendices

Risk Assessment: Security Issues associated with mobile phone

I. Security Issue associated with mobile device application.

II. Security Issue associated with mobile device operating system

III. Security issue associated with mobile device user behaviour.

IV. IV. Security issue associated with physical damage.

V. Personal information summary

Privacy Policy: Facebook

I. App Name

II. Type of information collected

III. Collection Method

IV. When is information collected?

V. How relevant is the information?

VI. How is the information used by the app providers?

VII. Information storage

VIII. Use of encryption

IX. Information sharing

X. App user access to information

Risk Treatment and Countermeasures

I. Mobile device application

II. Mobile operating system

III. User behaviour

IV. Physical threat/ damage

V. User Privacy

VI. Conclusion

VII. Recommendations