CAB240 Information Security - Semester 2 2021

Assessment Task 2: Information Security Risk Report

Part B

Group 110 Members:

Reagan Marshall

Hari Markonda Patnaikuni

Brandon Farmer

[Introduction 3](#_Toc85991154)

[Client organization 3](#_Toc85991155)

[Importance of mobile phone security 3](#_Toc85991156)

[Purpose 3](#_Toc85991157)

[Limitations and assumptions made 4](#_Toc85991158)

[Discussion 4](#_Toc85991159)

[Context Establishment 4](#_Toc85991160)

[Hardware 4](#_Toc85991161)

[Overview of Device Usage 5](#_Toc85991162)

[Mobile application 6](#_Toc85991163)

[Mobile device operating system 7](#_Toc85991164)

[User Behavior 8](#_Toc85991165)

[Physical threats to mobile devices 9](#_Toc85991166)

[Privacy impact analysis 10](#_Toc85991167)

[Privacy policy summary 10](#_Toc85991168)

[Risk treatment and countermeasures 12](#_Toc85991169)

[Mobile device application (Facebook) 12](#_Toc85991170)

[Mobile device operating system 14](#_Toc85991171)

[User behaviour 15](#_Toc85991172)

[Physical threats to mobile devices 17](#_Toc85991173)

[Information security issues related to user privacy 18](#_Toc85991174)

[Recommendations 18](#_Toc85991175)

[References 19](#_Toc85991176)

[Appendices 21](#_Toc85991177)

[Appendix A 21](#_Toc85991178)

[Appendix B: 22](#_Toc85991179)

## Introduction

## Client organization

All-Gas Pacific is a family owned 100% Australian independent supplier of house gas and commercial LPG bottles. Quoting many years in the gas industry competing with multi-national companies, All-Gas Pacific saw a need to provide customer service far beyond what is experienced in the industry. All-Gas prides itself on free same day delivery servicing Southeast Queensland including places such as Moreton Shire & surrounding areas and Hinterland.

Products supplied by All-Gas Pacific includes

* residential gas at 45kg
* helium kits for up to 2,000 balloons
* AAA Propane for forklifts using 15kg Aluminum gas cylinders, reducing overall forklift weight, and keeping the same capacity as traditional steel.

The role of Depot Manager is one of the most critical in the company. The objective is to refuel drivers as efficiently as possible while complying with guidance outlined in the safety data sheets. Company policy states that a depot manager must be on premises during any fueling. In the past, Depot Managers would only be responsible for their assigned depot, but with opportunities for expansion and a new push to run lean, travel is a requirement to cover time off and holidays.

## Importance of mobile phone security

The Apple iPhone 12 128GB issued is connected to All-Gas Pacific’s intranet via a mobile app connected to a web portal. Depot managers access a digital vault storing the passcodes to assigned depots. Passcodes are changed at random intervals and it is vital that the depot manager is onsite for various procedures requiring authorization.

All-Gas Pacific’s policy allows for limited personal use by allowing one to sign in with their Apple ID and offers the use of biometrics to secure the device when not in use. The two methods of authentication to access the device is the Face ID and PIN.

## Purpose

This report will address the risks associated with social media applications and the potential to use social engineering to gain unauthorized access to the All-Gas Pacific facilities and resources.

## Limitations and assumptions made

The risks being considered primarily applies to the Facebook application. We will also take into account that coworkers spend time with each other outside of the workplace and may communicate via social media as well. There can be a possibility that work related matters may be discussed outside of the workplace.

# Discussion

## Context Establishment

### Hardware

The mobile device used by the organization is an iPhone 12 128GB. This phone has a chipset containing an A14 bionic chip with 128GB of onboard storage. The storage and chipset on the phone will ensure that the phone will have ample storage for storing all the necessary data used by the depot manager and a powerful enough chip to run any applications that are needed to manage the depot manager’s tasks while working. (Apple, 2021) In addition to this, the phone has a 6.1-inch Super Retina XDR display which is an OLED display. (Apple, 2021) This large display will be perfect for the depot manager to read files and navigate applications on the go when working.

The phone has two rear cameras and one front facing camera. (Apple, 2021) In terms of battery capacity, the phone has up to 11 hours of streamed video playback. This should be plenty of battery power needed for a full workday of reading files and using the All-Gas Pacific app. (Apple, 2021) Also, the phone has communication features such as FaceTime video calling as standard over mobile network or Wi-Fi, and audio calling via FaceTime, LTE, and Wi-Fi. (Apple, 2021) This will be essential in managing the communication aspect of the depot manager’s job which requires contact with multiple employees to ensure all operations are running efficiently and on time.

Software

Applications preloaded onto the phone include FaceTime, Safari, Messages, Calendar etc. In addition to this, the software that might have been installed by the organization All-Gas Pacific include, a communication app such as Messenger by Facebook for use in communicating with employees, and the All-Gas Pacific app which allows the depot manager to keep track of their assigned depots and know which drivers need refueling in real-time.

It is expected that since the depot manager is using a work phone with some limited personal use granted by the employer that they can store personal apps or photos. Hence, it can be assumed that this functionality is not restricted by the employer. In addition to this, the usage of the phone may be monitored by the employer via an app that logs what the depot manager uses the phone for daily. This can reduce the instances of the depot manager using the phone for personal uses instead of work. Also, it is expected that the phone is updated regularly by the user, so the chance of security incidents is reduced.

Data

It is expected that the data stored and used on this phone will contain sensitive corporate information which should be encrypted via the All-Gas Pacific app. Data such as personal phone numbers of employees, PDF datasheets of inventory, and maybe personal photos or apps used by the depot manager may be present on the app.

Hence, in the event of a data hack regardless of intention the organisation must have a data retention plan and encryption of messages sent by employees and employers. The iPhone comes standard with iCloud backup which can be enabled by the employee to back up their data.

In addition to this, the volume of data stored on the phone may be substantial depending on how unwanted data is managed. If the data is not deleted when not needed anymore this can start to compound and result in the phone storage reaching its limit. Hence, the organisation may need to use a cloud based storage solution with multiple backups in case of data loss.

### Overview of Device Usage

The iPhone 12 issued to the Depot Manager is one of the most critical assets to the company. Reliable access to the All-Gas Pacific application is needed to track efficiency and make improvements. It allows the manager to have a small workstation on their person and seamlessly use collaboration applications such as Microsoft teams. This can be used to communicate with counterparts in various parts of the organization.

It is expected that the Depot Manager would use the applications that come preinstalled on the iPhone 12. Applications such as Contacts would be used to communicate with drivers and other employees in the company. (Apple, 2021) The Depot Manager would need to consider what contacts are shared with applications that do not involve the organization. Weather would be used to plan daily maintenance checks and adjust workload to help prevent safety hazards that could arise in events such as heavy rain. (Apple, 2021) Facetime could be used to assist in receiving real time reports in the field and provide solutions to employees. Use of the Camera application can be used to record details of incidents and field inspections. Calendar can be used to plan tasks and track the availability of employees. (Apple, 2021)

Frequent social media use is expected in regard to communicating with loved ones and of interests outside of the organization. The information shared on applications such as Facebook could reveal the movements of the depot manager such as lunch breaks and when the manager is off site on company business. The depot manager should be aware of what information about the organization is confidential. Applications such as Notes application could be used to record information needed for a later time. Information on the Notes application may be saved to the cloud or locally on the device. (Apple, 2021) The Depot manager would need to be careful with what information is saved and shared to the cloud if the iCloud functionality is enabled. Users may take advantage of Apple’s mobile payment system with Wallet to store credit card information, rewards cards, and payment details to transfer to other users. (Apple, 2021)

Risk Assessment

### Mobile application

Title: The Facts On News Reports About Facebook Data

Article:

Clark, M. (2021, 9 19). *The Facts on News Reports About Facebook Data*. Retrieved from NewsRoom: https://about.fb.com/news/2021/04/facts-on-news-reports-about-facebook-data/

Author: Mike Clark, product Management Director

Summary: In April the 3rd A business insider made it public knowledge that 530 million users’ data had been compromised. The article then goes on to describe how anonymous attackers were able to create a bot program to scrape data from user’s public profile pages by abusing the contact importer feature on Facebook. In saying that user data was compromised the article does specify that things like financial information, health and password data was not leaked however the article does not go into depth on what exact information was leaked.

Information assets: Attackers were able to scrape anything that was made publicly available by users, this might include things like phone numbers, full names, locations, user history or emails. And while the article does go on to state that the vulnerability was patched it does not say how.

Threat: Attackers with the intent to obtain information, such as date of birth, full first, middle, and last names, email addresses and other such pieces of information successfully scraped Facebook.

Vulnerability: This could cause another security breach or even facilitate impersonation attacks or allow confidence tricksters to use the information they have just collected to perform scams that would otherwise have been impractical.

Attack type: This was a active attack where attackers were able to use a script/bot to scrape or harvest information users were storing on their Facebook page. Furthermore, this attack was being conducted by anonymous individuals whose intent was most likely malicious.

The impact of these vulnerabilities, threats and attacks are that This breach seriously damaged the confidentiality of data for users as while some of the information was publicly available. In addition, the availability was compromised as attackers were able to gain access to information when they should not have been able to do so. Furthermore, money and manpower were and will be invested in fixing vulnerabilities. In addition, Facebook has been investigated for potential liabilities and the consequences of potentially having been negligent (maybe being fined/sued for damages). This can potentially have significant impacts on the profitability of the company and may in a worst-case scenario seriously hurt the ability of the company to function.

### Mobile device operating system

Title: Researchers find new Pegasus spyware hack targeting iMessage on Saudi activist’s iPhone

Author: Mitchell Van Homrigh

Reference: Van Homrigh, M. (2021, 9 14). Researchers find new Pegasus spyware hack targeting iMessage on Saudi activist’s iPhone. Retrieved 9 14, 2021, from news.com.au: https://www.news.com.au/technology/online/hacking/researchers-find-new-pegasus-spyware-hack-targeting-imessage-on-saudi-activists-iphone/news-story/dc5ed151272805b8a2eb62e7b5f332d6

Brief Summary: The above article from news.com.au details a vulnerability in Apple’s iOS operating system which led to the spying of iPhone user’s phones via the app iMessage. Researchers from the University of Toronto’s Citizen Lab discovered the significant flaw in the operating system. (Van Homrigh, 2021) The iMessage app’s software contained a vulnerability that allowed the spyware Pegasus to spy on Apple users' phones without the users opening any links via the app. Pegasus is zero-click spyware created by an Israel based counter-terrorism company NSO. (Van Homrigh, 2021)

Information Asset: The information assets that are compromised in this incident are the user’s phone’s cameras, microphones, location data, messages, call logs, and emails. Which can all be sent to the NSO’s client whoever it may be. (Van Homrigh, 2021)

Security Issue

Threat: As described by the article, the attacker deploys the spyware on the iMessage app via a loophole in iOS’s software and can control a wide array of the phone’s features. This threat can be thought of as compromising the confidentiality of the user’s privacy as they are disclosed to the attacker without the consent of the consent user.

Vulnerability: The researchers notified Apple of this security vulnerability in iOS. In response to being made aware of this security flaw, Apple released an iOS security update urging users to update their phones. (Van Homrigh, 2021)

Security Incident/Attack: The attack aptly named ‘Forcedentry’ is deployed to the users iPhone via iMessage which does not require any action from the user to enable it hence, the hack is described as zero-click. Hence, the attack can be classified as passive. This attack can be described as a major privacy violation by the users of the iPhone.

### User Behavior

Title: Apple says iOS 14.4 fixes three security 'actively exploited' by hackers

Author: Zach Whittaker

Reference: Whittaker, Z. (2021, 1 27). Apple says iOS 14.4 fixes three security 'actively exploited' by hackers. Retrieved 9 17, 2021, from TechCrunch: https://techcrunch.com/2021/01/26/apple-says-ios-14-4-fixes-three-security-bugs-under-active-attack/

Brief Summary: The above article by TechCrunch explains 3 new security updates made to iOS and iPadOS 14.4 which fixed vulnerabilities that were taken advantage of by hackers. (Whittaker, 2021) It is unclear the extent of the attacks and how many users were affected by them. However, it is explained that two bugs were found in the WebKit the engine that powers the Safari browser. (Whittaker, 2021) This is linked back to an older article published by TechCrunch which discussed the lacing of websites with malicious code to spy on Uygur Muslims by the Chinese government. (Whittaker, 2021) This suggests that the hack relies on user behavior to wrongly distinguish real websites from laced websites. It is also pointed out that the laced websites can be accessed by any iPhone user hence, they can be used to spy on users from other countries.

Information Asset: As discussed in the article by TechCrunch it was revealed to TechCrunch that the hacks were conducted by the Chinese government to spy on Uygur Muslims. (Whittaker, 2021) This was linked to another article by TechCrunch which explained that the laced websites contained code that was able to hack into a user’s iPhone to read their passwords, messages, and track their location in real-time. (Whittaker, 2021)

Security Issue

Threat: As discussed in the two articles the attacker can create a website that loads malicious code into the user’s phone just by visiting one of the websites. The information asset compromised in these hacks is the confidentiality of the user.

Vulnerability: The vulnerability of user behavior not being able to visit these laced websites proved to be highly accurate as these websites had thousands of visitors per week. To fix these obvious violations to user confidentiality Apple released these security updates to iOS and iPadOS five years later. (Whittaker, 2021)

Security Incident/Attack: These attacks which can be classified as major confidentiality violations are active or passive attacks that require the user to visit one of the laced websites. Hence, this is a user behavior powered hack.

### Physical threats to mobile devices

Title: Juice Jacking: Beware Of Rogue Power Sources

Author: David Braue

Reference: Braue, D. (2021, 4 7). Juice Jacking: Beware Of Rogue Power Sources. Retrieved 9 15, 2021, from CYBERCRIME MAGAZINE: https://cybersecurityventures.com/juice-jacking-beware-of-rogue-power-sources/

Brief Summary:

The above article by Cybercrime Magazine explores the issue of public charging stations and how they can be vectors for deploying malware to a user’s phone. As discussed in the article, charging stations, although not the most obvious place to hack your phone, is still one users should be concerned about. This type of hack known as ‘juice jacking’ involves an unsuspecting victim who likely acts out of desperation to charge their almost flat phone in a public charging station. The potential attacks resulting from this action include the direct transfer of information assets from the charging phone to the attacker via the charging cable and the deployment of malicious software that can hack the phone. (Braue, 2021)

Information Asset: The information assets that are compromised in ‘juice jacking’ are personal information such as private photos, or even sensitive corporate or government information. (Braue, 2021) Hence, the simple act of charging your phone in a public charging station can be a physical threat to your data on your phone.

Security Issue

Threat: As discussed in the article the unsuspecting act of charging your phone in a public charging station can lead to the deployment of malicious code into your phone which can result in data transfer to the attacker. Hence, this attack can be thought of as an active or passive attack that violates the confidentiality of the user’s data.

Vulnerability: The vulnerability that mobile devices are exposed to in public charging stations is significant and users should be cautious when deciding whether to charge their phones in such stations. Hence, the lack of a proper solution to this problem means the user should be diligent in protecting their data by creating backups and finding alternative methods to charging their phone such as carrying a power bank.

Security Incident/Attack: The potential attacks carried out in public charging stations are active or passive attacks that can result in data loss and transfer of information from the victim to the attacker. Hence, this attack is powered by the physical vulnerability of the mobile device.

## Privacy impact analysis

### Privacy policy summary

1. **App Name:** Facebook (a social media platform that has its own application that allows users to communicate with others, share pictures and play small games.)
2. **Type of information collected:** When users sign up for an account, create or share content, message, or communicate with others, location of a photo and/or the date a file was created, accounts details, hashtags, affiliated groups, address book or call log or SMS log history, types of content users view or engage with, the actions you take on Facebook, frequency and duration of your activities, information about purchases or transactions.
   1. From Facebook’s policy page:
      1. Device attributes: information such as the operating system, hardware and software versions, battery level, signal strength, available storage space, browser type, app and file names and types, and plugins.
      2. Device operations: information about operations and behaviors performed on the device, such as whether a window is foregrounded or backgrounded, or mouse movements (which can help distinguish humans from bots).
      3. Identifiers: unique identifiers, device IDs, and other identifiers, such as from games, apps or accounts you use, and Family Device IDs (or other identifiers unique to [Facebook Company Products](https://www.facebook.com/help/195227921252400?ref=dp&refid=41) associated with the same device or account).
      4. Device signals: Bluetooth signals, and information about nearby Wi-Fi access points, beacons, and cell towers.
      5. Data from device settings: information you allow us to receive through device settings you turn on, such as access to your GPS location, camera or photos.
      6. Network and connections: information such as the name of your mobile operator or ISP, language, time zone, mobile phone number, IP address, connection speed and, in some cases, information about other devices that are nearby or on your network, so we can do things like help you [stream a video from your phone to your TV](https://www.facebook.com/help/276515126152168?ref=dp&refid=41).
      7. Cookie data: data from cookies stored on your device, including cookie IDs and settings. Learn more about how we use cookies in the [Facebook Cookies Policy](https://www.facebook.com/policies/cookies/?refid=41) and [Instagram Cookies Policy](https://lm.facebook.com/l.php?u=https%3A%2F%2Fwww.instagram.com%2Flegal%2Fcookies%2F&h=AT1FPgeGm5X8XKtgcX5i-rUis6bi0BrYXoPYMSciBTsXGw8rrNt8eptHzj5UtA5kKKGBo5Motn8n-YIKlSbMxa-6DExxwCf9psvpoMOgMn4_WdeT-3Fv3Jlt6p8iYIbGLHws4Q). (Facebook Data Policy 2021)
3. **When is the information collected?** Information collected mostly comes directly from the user but the Facebook app also analyzes how the user interacts with Facebook, for how long users spend on activities and which advertisements work best for each user. Information is mostly collected from when the application is open however, there is a Off-Facebook activity part of Facebook that does track and use information while you view other sites. (Facebook Off-Site 2021)
4. **How relevant is the collected information to your use of the app?** Most of the information is relevant to the function that Facebook is used for which in this case is social media and communication. However, information such as the device you are using, your location via accessing your GPS and browser history with the off Facebook functionality is not related to social media and while it does serve a purpose it may not be needed or wanted by most users. Furthermore, most of these settings are enabled by default and unless users go through and manually decline these “features” they may have their information harvested and stored in a database without their knowledge.
5. **How is the collected information used by the app providers?** Information is collected by Facebook and then stored/used with the intent of either making the user experience with the core purpose of Facebook better by making relevant material appear in users' feeds, showing tailored information to users depending on what they enjoy etc. They also collect data for the purpose of advertisements so that the company can make revenue.
6. **Information storage:** As users stay with Facebook all relevant information is stored indefinitely unless users ask for it to be deleted, and if the information is “deleted”, Facebook stores a copy of the data for up to 3 months. (Picchi, 2018)
7. **Use of encryption:** Data is encrypted using AES-256 end-to-end encryption for data transmission. (Corpuz, 2021)
8. **Information sharing:** Yes, it is shared with third parties. They share info with other Facebook companies such as WhatsApp and oculus. It also shares data o with advertisers. (Facebook Data Policy 2021)
9. **App user access to information:** Yes, the app has access to the information the user provides and there is a process that can be completed if users wish to see what information has been collected by Facebook. The process to find the information can be found here:
   1. <https://www.howtogeek.com/708912/how-to-see-what-data-facebook-has-on-you/>

## Risk treatment and countermeasures

### Mobile device application (Facebook)

Overview of security issue from Part A: Mobile device application

Treating the risk

**Suggested control measure and explanation:**

Users can potentially limit the content posted and shared with Facebook which will limit what is collected by Facebook. To do this, users can limit permissions the application has such as preventing the camera and microphone being used while the application is idle or force the app to request access from the user every time it wants access to non-essential pieces of hardware. Another suggestion could be to prevent the application from having access to features and components of the device that could be used to build a profile of the user’s movements and habits. (Gralla, 2019)

Users can also change permissions on who can see posts and who can view personal information that initially could appear innocent such as location of suburb or date of birth ect. This kind of information can be combined to build a profile by a malicious third party for use in a more targeted attack. This could be achieved by attackers by scraping publicly available information and compiling it into a database.

**Type of control measure:**

Limiting the content shared with Facebook is preventative and could easily be used to prevent the unwanted disclosure of personal information assuming the application is working as intended. As if the application has no important information to be scraped there is no risk.

Changing permissions is also preventative and effective in preventing information existing personal information from being harvested by malicious third parties. This can also assist in preventing Facebook from taking information that can be stolen later.

**Degree of protection provided:**

Limiting the use of Facebook could provide a minor degree of protection in the unwanted disclosure of private information.

Changing permissions provides a minor degree of protection and depends solely on what the user chooses to disclose on the platform and the permissions allowed on the device. Methods of attacks such as scraping are only useful for harvesting information that is already visible to all users. If the information is made private by the user, theoretically a third party should not be able to access sensitive information and reduce the likelihood of a full profile. Changing permissions does not have any effect on the likelihood of the account being compromised through means such as a weak password or a single form of authentication. Furthermore, malicious third parties who may have compromised a user’s account will not be able to easily access the information they want as easily if this form of mitigation is used however it is not impossible to get around this and access the Facebook database and compromise the confidentiality of the users information that way.

**Limitations of this control measure:**

Limiting the use of Facebook does not prevent the disclosure of sensitive information given willingly by the user. It also does not prevent pieces of information already collected by Facebook from malicious third parties. Furthermore, it does not prevent the collection of data already present on the website.

While changing permissions does have a reasonable degree of security when it comes to excessive data leakage, it has no effect if the website is hacked or if a vulnerability is exploited and the permissions are bypassed. As a result, this preventative measure is only effective if the application is working as intended.

### Mobile device operating system

Overview of security issue from Part A: Mobile device operating system

Treating the risk

**Suggested control measure and explanation:**

Users can avoid the risk of having the Pegasus spyware installed on their devices by not clicking on foreign links sent to them by either unknown entities on applications such as WhatsApp or Messenger. This can be enforced with a device policy for devices issued by the organization. In addition, if the user trusts the person sending the link, they can alternatively simply type the link manually rather than clicking on the link which could risk installing the Pegasus spyware.

An additional method of avoiding the Pegasus spyware via hardware to attempt to change user behavior. Users could potentially have multiple devices, one for business and one for social use. As a result, if one device is compromised both one device will be safe. Another option could be for users to refrain from using the default browser that comes preinstalled with the operating system of the phone. There have been instances where the Pegasus spyware was not capable of installing correctly due to incompatibility with the browser type. Having a different and updated browser could help some cases. (Intercept Security Team, 20)

**Type of control measure:**

Not clicking on unknown links as a control measure is inherently preventative as it simply reduces the risk of unsuspecting victims accidentally installing the Pegasus in the first place.

Having a multiple device policy as a control measure is also preventative, this is done by spreading vital information about the individual across different devices so that regardless of which one is attacked not enough information can be collected to launch an attack. Or one phone which is less important can be used to test if links are valid/safe and so long as it is non-essential it will not leak important information to third parties.

**Degree of protection provided:**

There is a significant degree of protection to the organization if the user does not click on any foreign links because the primary way spyware is installed. Lack of knowledge could lead a user to a malicious website that has the potential to bypass the operating system’s security functions.

There is a moderate degree of protection provided when users have a separate device for work and personal use when it comes to the likelihood of installing spyware and its impact. This can be combined with the previous control measure mentioned above to further increase the degree of protection. In speculation based on a small sample size, if the Pegasus installation cannot take place with non-default browsers such as Google Chrome, this could potentially provide an enhanced security posture against this kind of spyware. (Intercept Security Team, 20)

**Limitations of this control measure:**

Training and awareness when it comes to interacting with others digitally does not provide complete protection and there have been instances of users not being prompted to install software, or potential malware, on their device. This method doesn’t provide a method of detection to alert a user of the problem or spyware installed on the device. However, if the usage of links can be minimized to only typing out trusted links the safety of the users information can be improved greatly. (Backhouse, 2021)

Separating devices as a control measure does not completely prevent the user from having their devices infected. It only reduces chances of spyware installing on a device that could impact the organization if an appropriate device policy is implemented.

### User behaviour

**Overview of security issue from Part A: User behaviour**

As discussed in Part A the user behaviour issue of malware-laced websites is a high priority when it comes to information security. As described, a vulnerability in iOS enabled the deployment of spyware onto victim’s phones which could read their passwords, messages, and tracking their location in real-time. (Whittaker, 2021)

This occurs when victims are not able to distinguish fake websites with malformed URLs and weak security, from the real websites by organizations they are intending to reach. In addition to this, the hacks were supposedly conducted by the Chinese government to spy on Uygur Muslims. This type of hack can be considered as a breach of confidentiality which results in the unauthorised disclosure of sensitive information to a third party.

Referring to the All-Gas Pacific, an attack from a laced fake website could result in the breach of the user’s confidentiality, employees of the company, and confidentiality of the organization itself.

**Treating the risk:**

**Suggested control measure and explanation:**

A control measure that can be utilised for the user behaviour vulnerability is to educate employees using work phones on how to distinguish fake websites from real websites. There are many nuances within fake websites that can be easily overlooked in a fast-paced environment. Practices such as checking the URL for https and providing the least amount of information possible online can moderately decrease the impact that data leakage may have to the organization. Ensuring that communications are conducted on official channels can also reduce impact to the organization as well.

By utilising this control measure, the organization can reduce security incidents with a few hours of training employees on best practice with employer issued devices. If the organization chooses not to prioritise a control measure such as this, there could be serious implications such as intellectual property theft, ransomware attacks, and privacy breaches from compromised devices connected to the organization’s network.

Another control measure which can be implemented into the company’s mobile phone policy is to use alternative browsers when using the internet on the work phone. Browsers that include a Hypertext Transfer Protocol Secure(HTTPS) only connection option may reduce the chance of mobile surveillance from potential attackers. These browsers often include an option within the settings to only connect to websites which are secured with HTTPS. (Gatlan, 2021) Websites which are secured with HTTPS encrypt data in-transit, validates who is sending data and receiving it, and much more. (Roomi, 2020)

**Type of control measure:**

This control measure is preventative in which it reduces the likelihood of security incidents occurring while employees are browsing the internet on the employer-issued device. In addition to this, the control measure of using only HTTPS connections enabled browsers on work phones is also preventative in nature.

**Degree of protection provided:**

Training on best practices with mobile devices provides a substantial degree of protection to the employer as employees are more informed on how to distinguish fake websites from real websites. However, this training does not guarantee that the company will be immune from attacks; instead, the probability of such incidents occurring will decrease. In addition to this, the degree of protection provided by using browsers which only connect to HTTPS websites is considerable due to the browser itself preventing the user to connect to non-HTTPS certified websites.

**Limitations of this control measure:**

A limitation of the control measure on educating employees on how to distinguish a fake website from a real website is that it is entirely based upon the individual’s ability to distinguish the two. Additional measures should be taken to account for the possibility of human error and should be used in conjunction with other control measures such as limiting the work device for personal use.

In addition to this, the control measure of using only HTTPS secured websites also has a limitation. This control measure can be disabled by the employee via the settings of the browser without the authorisation of the employer hence, utmost care must be taken when accessing websites which are not secured by HTTPS.

### Physical threats to mobile devices

**Overview of security issue from Part A: Physical threats to mobile devices**

Referring to Part A of the report, the risk of juice jacking was discussed and how the deployment of malware can be delivered via the charging cable of a mobile device. This physical threat involves an unsuspecting victim charging their phone in a public charging station in which the attacker uses it as a vehicle to deploy malware to the user’s phone. (Braue, 2021)

In addition to the deployment of malware, the attacker can also directly transfer sensitive information assets via the charging cable. Hence, juice jacking attacks can breach confidentiality regarding a user’s personal information. In relation to the All-Gas Pacific, if an employee is a victim of juice jacking not only is their personal information compromised but possibly the intellectual property of the organization that owns the device. This is exacerbated further if the device isn’t wiped before assigning to a new employee and goes undetected. Hence, it is important to raise awareness of these threats and how to mitigate them.

**Treating the risk:**

**Suggested control measure and explanation:**

A control measure to combat juice jacking is to educate users about how attackers can exploit convenience and the security implications of these types of threats. Juice jacking is an active attack which involves an unsuspecting victim attempting to charge their phone in a public charging station. When the victim makes the connection with their device, the attacker can deploy malware via the charging cable without the victim being aware.

This can be especially problematic for a device used by a depot manager at All-Gas Pacific as a work and limited personal use phone. The device may provide an entry point to the organization’s network or give an attacker credentials to launch a more sophisticated attack. Thus, the vulnerability exists that the manager may charge this phone at a public charging station for convenience purposes, increasing the likelihood of security incidents occurring due to juice jacking. Hence, it is recommended that the employer advises the manager to charge their phone in safe areas only such as at home or work and know what is on the other end of the device when connected. In addition to this, it is recommended that the manager carry a power bank for the possibility that a charger or power outlet is not available.

**Type of control measure:**

This control measure is preventative as the employer educates the employee on how juice jacking takes place and measures that can be taken to eliminate the likelihood of the attack occurring. By educating the employee on the dangers of public charging stations, informed decisions can be made to reduce the likelihood that the employee will use a public charging station.

**Degree of protection provided:**

The degree of protection this control measure provides is significant as the threat of juice jacking can be essentially eliminated by the employee not connecting the device to public charging stations.

**Limitations of this control measure:**

A limitation of this control measure is that it assumes that the employee will make the decision to not use public charging stations. The phone is both a work and limited personal use phone so tracking the battery life may not be a priority for the user. Hence, a situation may occur where an employee needs to charge the phone in a public charging station due to low battery out of desperation leading to a potential security incident.

### Information security issues related to user privacy

# Recommendations

# References

*NSO SPYWARE ATTACKS DISCOVERED AROUND THE WORLD*. Retrieved from The Intercept\_: https://theintercept.com/2021/07/27/pegasus-nso-spyware-security/

Apple. (2021). *iPhone 12*. from Apple. Retrieved 9 18, 2021, from https://www.apple.com/au/iphone-12/specs/

Backhouse, A. (2021, 7 19). *Pegasus Project: Massive global phone hack discovered targeting journalists and politicians*. News.com.au. https://www.news.com.au/technology/online/hacking/pegasus-project-massive-global-phone-hack-discovered-targeting-journalists-and-politicians/news-story/df3bc3e5c0b45e78f903a3678f5e34f7

Braue, D. (2021, 4 7). *Juice Jacking: Beware Of Rogue Power Sources*. CYBERCRIME MAGAZINE. Retrieved 9 15, 2021, from https://cybersecurityventures.com/juice-jacking-beware-of-rogue-power-sources/

Corpuz, J. (2021, 09 18). *Tom's guide*. The best encrypted messaging apps in 2021. https://www.tomsguide.com/reference/best-encrypted-messaging-apps

Facebook Data Policy. (2021, 1 11). *Data Policy*. Facebook. https://m.facebook.com/policy.php

Facebook Off-site Activity. (2021). *Off-Facebook Activity*. Facebook.com. Retrieved 9 17, 2021, from https://www.facebook.com/off\_facebook\_activity/

Gralla, P. (2019, 6 7). *How to protect your privacy on Facebook*. The Verge. https://www.theverge.com/2019/6/7/18654238/facebook-privacy-data-information-ad-settings-how-to-protect

Picchi, A. (2018, 3 23). *OK, you've deleted Facebook, but is your data still out there?* Cbsnew.com. https://www.cbsnews.com/news/ok-youve-deleted-facebook-but-is-your-data-still-out-there/

Van Homrigh, M. (2021, 9 14). *Researchers find new Pegasus spyware hack targeting iMessage on Saudi activist’s iPhone*. News.com.au. https://www.news.com.au/technology/online/hacking/researchers-find-new-pegasus-spyware-hack-targeting-imessage-on-saudi-activists-iphone/news-story/dc5ed151272805b8a2eb62e7b5f332d6

Whittaker, Z. (2021, 1 27). *Apple says iOS 14.4 fixes three security bugs 'actively exploited' by hackers*. Yahoo! finance. https://au.finance.yahoo.com/news/apple-says-ios-14-4-202910341.html?guccounter=1&guce\_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce\_referrer\_sig=AQAAAB55YW3A30Vp\_6AWQ6qzCKAeL7t5Otf79PoH6C04SFy8sw7cIE-olSBqUJxZyyv1EXPSMVkJAxAMy1WyH0zwwWU9lGDj586\_R1C1zVqmdV

Gatlan, S. (2021, 07 01). Google Chrome will get an HTTPS-Only Mode for secure browsing. Retrieved 10 24, 2021, from BLEEPINGCOMPUTER: https://www.bleepingcomputer.com/news/security/google-chrome-will-get-an-https-only-mode-for-secure-browsing/

Roomi, M. (2020, 08 12). 6 Advantages and Disadvantages of HTTPS | Drawbacks & Benefits of HTTPS. Retrieved 10 24, 2021, from HITECHWHIZZ: https://www.hitechwhizz.com/2020/08/6-advantages-and-disadvantages-drawbacks-benefits-of-https.html

# Appendices

## Appendix A

Mobile application risk assessment article: (clark, 2021)

Graphical user interface, text, application, Word

Description automatically generated

## Appendix B:

Mobile device operating system article(Van Homrigh, 2021): Graphical user interface, text, application

Description automatically generatedA close-up of hands on a keyboard

Description automatically generated with medium confidence

A person using a computer

Description automatically generated with medium confidence

Text

Description automatically generated with medium confidence

Appendix C:

User behaviour article(Whittaker, 2021):

Graphical user interface

Description automatically generatedGraphical user interface, text, application

Description automatically generated

Appendix D:

Physical threats to mobile devices article(Braue, 2021):Graphical user interface, text, application, email

Description automatically generatedGraphical user interface, text, application

Description automatically generated

Text

Description automatically generated