*A brief description of the information assets* – describe your phone

The mobile phone in question is the iPhone XR which was released by Apple at the World Wide Developers Conference (WWDC) on the 12th September 2018. This iPhone is considered by many people as the best iPhone to hit the market with the perfect balance between its hardware features and its software features compared to the iPhone XS and the iPhone XS Max, the iPhone XR’s two older brothers.

The display of the phone is a 6.1-inch all-screen LCD Multi-Touch Liquid Retina Display with IPS technology measuring at a resolution of 1792 x 828 pixels with a pixel density of 326 pixels per inch (Nations, 2019). The display has one of Apple’s latest display innovations called the True Tone Display (Nations, 2019). The True Tone display ensures that the colour temperature of the display is well adapted to the surroundings (E.g. When its sunset, the colour temperature switches to warm and when its sunrise, the colour temperature switches to cool automatically) (Nations, 2019). This feature is especially useful if your one of those people whom use your phone the very first thing in the morning and the very last thing at night (Nations, 2019).

Furthermore, the iPhone XR boasts a new processor under its hood, the A12 Bionic Chip is made on the newest architecture of chip design, the 7nm chip design process (Fingas, 2019). The renowned Neural Engine still holds a special spot since the days of the first iPhone with facial recognition, the iPhone X (Fingas, 2019). The new A12 Bionic Chip can handle up to 5 Trillion operations per second as compared to the previous generation A11 Chip which could only handle up to 600 Billion operations per second (Fingas, 2019). At the centre of all this performance boost, is a six core Central Processing Unit with two of its six cores being high performance cores (Fingas, 2019). The result is a 15% increase in overall performance and a 40% decrease in overall power compared to the last generation A11 Chip (Fingas, 2019). The 4 low performance cores handle the bulk of the everyday tasks (Fingas, 2019). With this brand-new chip, in the newest iPhone models, Apple, also announced a faster Security Enclave that mainly serves the purpose of doubling the speed of facial recognition in the iPhone XR (Fingas, 2019).

The brand-new iPhone XR also boasts three new internal storage capacities (64GB, 128GB and the 256GB) (Welch, 2019). This enables users to have less of their personal data (E.g. Banking Credentials and even some photos) backed up to the cloud, and rather, have the bulk of it stored locally on the device (Welch, 2019). In addition, as app data is usually stored locally on the device by default, users can now download more apps that would dramatically improve their productivity at work or even at home (Welch, 2019). The 3GB of RAM available to all users who purchase the iPhone XR also dramatically improves application launch speeds from rest and significantly decreases the boot up time of the phone (Welch, 2019).

The most outstanding feature on the iPhone XR is its Camera. It may only be one camera, but it most certainly packs a punch. It’s a 12-Megapixel wide-angle camera with an f1.8 aperture and optical image stabilisation (commonly known as hardware induced stabilisation). It also has auto image stabilisation (commonly known to many as software induced stabilisation). The f1.8 aperture means, that the lens opens up really wide, allowing plenty of light to hit the sensor embedded within, thus increasing the brightness of the photo taken especially at night or in dark environments. The optical image or hardware induced stabilisation does a very good job at taking crisp shots when you may expect motion blur perhaps due to a fast-moving subject. Besides that, the iPhone XR has features in its camera app that make it a fully functional portable DSLR, except one thing, it’s a lot easier to master, especially for someone just getting into photography all without breaking a hole in

the user’s pocket. Furthermore, the camera lens allows for 5x digital zoom, enabling the user, to get really up-close to the subject.

The iPhone XR has impressed many with its exceptional battery life ("iPhone XR - Technical Specifications", 2019). Due to Apple’s implementation of the new A12 Bionic Chip, reducing power by 40%, almost half ("iPhone XR - Technical Specifications", 2019). This has caused an increase in the time you are able to spend with your iPhone off the charger. (E.g. Up to 25 Hours of Talk time, Up to 15 Hours of Internet use, Up to 16 Hours of Video playback and lastly but most certainly not least, Up to 65 Hours of Audio playback) ("iPhone XR - Technical Specifications", 2019). In addition, if you do happen to run low on battery as you use your mobile device, you can just plug it into the wall and charge it up to 50% in under 30 minutes ("iPhone XR - Technical Specifications", 2019). Lastly, it supports wireless charging, for those users whom are crazy about wireless charging ("iPhone XR - Technical Specifications", 2019).

The iPhone XR has the latest version of Apple’s proprietary software installed, iOS 13 ("iPhone XR - Technical Specifications", 2019). This software boasts a bunch of new features under the hood such as better performance when paired with Apple’s new security enclave and better general task management due to highly optimised resource allocation algorithms ("iPhone XR - Technical Specifications", 2019). Another great feature is improved background process efficiency (E.g. The ability to offload an app when it is not being used, optimises resources and saves power) ("iPhone XR - Technical Specifications", 2019). Lastly, but most certainly not least, processor cache is now more efficiently shared across all processor cores ("iPhone XR - Technical Specifications", 2019).

As with every mobile device, the iPhone XR being no exception, it comes with its preloaded apps ("iPhone XR - Technical Specifications", 2019). Some of the preloaded apps are like (E.g. FaceTime, Calendar, Photos, Camera, Mail, Clock, Maps, Weather, Notes, Reminders, Stocks, News, App Store, Books, Health, Home, Wallet and Settings) ("iPhone XR - Technical Specifications", 2019). Some of the other apps I have installed on my iPhone XR include ones that I use to improve my navigation around Town (E.g. Google Maps and TransLink) and also to improve my overall productivity (E.g. Notes, QUT App, TED, YouTube, Gmail, etc…) ("iPhone XR - Technical Specifications", 2019). Considering I am an international student studying in Australia, and fly back home regularly during the long breaks, I also use apps to track the price of flights in and out of Australia (E.g. Qantas, Malaysian Airlines, etc…). I also have apps that I use regularly for professional development (E.g. Linked-In) and some social media apps for relaxation (E.g. Instagram, Facebook, Messenger, etc…) ("iPhone XR - Technical Specifications", 2019).

With regards to types and volume of data I have stored on my iPhone XR, there are Photos, Contacts, Notes, Reminders, E-Books and plenty more ("iPhone XR - Technical Specifications", 2019). Most of the 64GB in phone is taken up by the number of apps I have stored on the device ("iPhone XR - Technical Specifications", 2019). Other types of data, such as the Photos, Contacts, Notes, E-Books and Reminders are backed up to I-Cloud, Apple’s cloud service provider ("iPhone XR - Technical Specifications", 2019). By default, all iPhone users are only given 5GB of cloud storage, but because of the nature of my work as a photographer and also as a full-time student, I opted to pay a fixed monthly rate and get the 2TB’s of cloud storage. Although, all the Photos, Reminders, Contacts, Notes and E-Books are loaded on the phone, they are actually in sync with the cloud and when used, downloading and uploading information between the iPhone and the cloud in real time ("iPhone XR - Technical Specifications", 2019). All in all, I have about 17.1GB of Data on my iPhone. Most of the apps I

have loaded on my device regardless preloaded or third party, store a certain amount of background data ("iPhone XR - Technical Specifications", 2019).

This background data depending on the app, can be either a lot or a little. Other types of apps like (Google Maps, TransLink, etc…) which I use to navigate around town, store location data in the background when the app is in use ("iPhone XR - Technical Specifications", 2019).

b. An *overview of your use of the device* – what really matters to you, and how do you make use of your phone?

Grading Criteria:

1. Through overview of your use of the device including the evaluation of:
   1. Level of criticality of all items / applications and data.
   2. The sensitivity of the data items included in the description with respect to confidentiality, integrity and availability.

Firstly, as a street photographer, my mobile device becomes my primary camera when I am on the move. The next biggest problem for most photographers, is storage. For me, the iPhone’s internal storage of 64GB is plenty, and if that weren’t enough, most of the photos I take on my mobile device get synced with iCloud, Apple’s cloud service provider.

But let’s not forget, I also a full-time student. For most students, we keep reminders in our phone, not to mention notes that contain important points lecturers, tutors or friends might talk about. But the one thing that students make the most use out of is the Calendar, to keep the due date of all assignments and examinations throughout the semester.

With reference to the two paragraphs mentioned above, the amount of information stored on my mobile device (with regards to the Reminders, Calendar Entries, Notes and Photographs) are incredibly important. Attackers that get their hands on any bit of these information could access all of my online accounts, modify my login credentials, falsify purchases under my name, impersonate me through identity theft and much more. The severity of all these unlawful actions being committed defies the 3 primary and most important security goals. Confidentiality, because now instead of me having access to my accounts and my personal information, its hackers from any part of the world who do. In addition, to being able to access my personal information, they can also modify it, locking me out of my own accounts and using my accounts to make unauthorized purchases further compromising the integrity and availability of my information and my personal identity.

With the photographs I capture and store on my mobile device, they end up going to the client whom have pad for them. If this data is compromised, one of two things can occur. Firstly, the client’s facial identity can be made to look like someone else, more commonly described as impersonation. This then breaches one of the very first goals of information security, confidentiality. In addition, impersonation of a client’s facial identity through photographs can also be done through masking, the process of making the original photo look like someone else. This unlawful act requires the original metadata of the photograph to be modified further breaching the second most important security goal, integrity and availability.

**Article 1**

Risk Assessment (Limited to one example for each of the following four categories) – use the template given and write concisely – try to keep to one page for each example

Question 1a: A summary of a recent article identifying a security issue associated with a mobile device application

* If possible, find an article about an application that you use, or a widely used app.

Grading Criteria: Comprehensive summary that correctly identifies the threats, explains vulnerability, describes the incident and identifies the security goals that have been compromised.

**Article Title**: Uber fined $148m for failing to notify drivers they had been hacked.

**Author**: The Guardian

**Reference details (if online article, give the URL and date accessed)**: Uber fined $148m for failing to notify drivers they had been hacked. (2019). Retrieved 16 August 2019, from <https://www.theguardian.com/technology/2018/sep/26/uber-hack-fine-driver-data-breach>.

**Brief Summary**: The article above is about how Uber had to pay a fine amounting to $148M for not informing their drivers, that their personal details had been hacked. According to Uber, they have been covering up this incident simply by paying the hackers who had compromised their driver’s information with a ransom to avoid the data being used inappropriately, and to even prevent the data from being sold to third parties which could lead to further problems such as identity theft and so on. This data breach, that had occurred to Uber had compromised the personal details and the credentials of almost 600,000 Uber drivers in the United States. Besides, the affected Drivers in the United States, around 57 Million people all around the world had their names, email addresses and contact numbers stolen too all through this hack. To make up for all this damage, Uber’s legal representative, has mentioned that the new settlement requires Uber to comply by ensuring all the personal information of their drivers and their riders are kept safe. In addition, it also mentions that Uber is to immediately inform the authorities if such a data breach is to ever occur again and last but certainly not least, stronger password protection policies are to be enforced by Uber. The total amount of money to be paid by Uber will be shared based on the number of drivers using the platform. One of the 53 states in the United States, Illinois’s, share was $8.5M. The total amount given to the other Uber drivers in the other states was about the same.

**Information asset**: 600000 Uber Driver’s personal information including their driver’s license information. In addition, the names, email addresses and contact numbers of around 57 Million riders around the world were also compromised. The information that was compromised was in its resting state.

**Security Issue**:

1. **If it is a security incident/attack**: The article describes that the incident that had occurred above is an attack which had led to 600000 Uber Driver’s personal credentials including their driver’s licenses getting compromised. The names, email addresses and even contact numbers of 57 Million other people around the world who use the ride sharing platform had also had their personal data hacked through this. To prevent the problem from escalating (E.G: The data getting misused inappropriately), Uber paid the hackers ransom so that the data that they had about Uber’s drivers and riders remained safe. This security attack can be further described as a passive attack as the attacker’s goal was to obtain information. In addition, the attacker’s do not alter the information system resources. A passive attack like the one described above is usually difficult to detect as there is no interaction with the attacker’s and the company attacked. The only way of stopping this kind of attack is by taking preventive measures.

**Article 2**

Risk assessment (Limited to one example for each of the following four categories – use the template given and write concisely – try to keep to 1 page for each example).

Question 1b: A summary of a recent article identifying a security issue associated with a mobile device operating system (The operating system, not an application issue).

* If possible, this should be for your phone operating system.

Grading Criteria: Comprehensive summary that correctly identifies the threats, explains vulnerability, describes the incident and identifies the security goals that have been compromised.

**Article Title:** New IOS 13 vulnerability allows access to passwords stored on your iPhone.

**Author:** Information Security Newspaper

**Reference details (if online article, give the URL and date accessed):** Bhatia, R. (2019). New iOS 13 vulnerability allows access to iPhone passwords. Retrieved 22 August 2019, from <https://www.securitynewspaper.com/2019/07/16/new-ios-13-vulnerability-allows-access-to-passwords-stored-on-your-iphone/>.

**Brief Summary:** This article basically states that those people who download the latest version of the beta iPhone operating system, appropriately named iOS 13 and use the password Auto-Fill feature are in serious danger of getting their accounts compromised if their iPhone gets in the hands of the wrong person who knows how to exploit this vulnerability. This attack provides hackers with data stored in the user’s iCloud Keychain, Apple’s password management system from which the Auto-Fill feature gets the necessary information it needs to fill out individual user’s account credentials. Moreover, the way this vulnerability can be exploited depends on two factors. The first factor, is the ability of the hacker to lay his hands on a physical unlocked mobile device which greatly increases the complexity of this attack, the second factor is the hacker’s ability to exploit the vulnerability itself. This vulnerability can simply be exploited by entering the Settings app, scrolling down and clicking on the Passwords and Accounts option and repeatedly tapping on the tab that states Website and Apps Passwords option. By doing this, the hacker will be able to bypass the message from either of Apple’s security technologies, FaceID and TouchID, and after more attempts, the hackers will have access to all the account credentials stored by the user on the system. Going further, the hackers can make modifications to the already compromised account credentials.

**Information asset:** The user’s personal data and all his/her account credentials stored on the physical mobile device.

**Security Issue:**

1. **If it is a threat:** This type of threat according to Week 2’s lecture can be described as a deliberate human action. A hacker would have to gain access to an unlocked physical mobile device to be able to gain access to a user’s account credentials and not to mention even his/her personal details like names, email addresses and mobile numbers.
2. **If it is vulnerability:** The vulnerability is that anyone hacker who manages to get their hands on a physical unlocked mobile device can easily access the Passwords and Accounts option from within the Settings app, tapping on the option that says Website and Apps password option, multiple times bypassing Apple’s built in security system, depending on the mobile device, either FaceID or TouchID, and gaining access to an individual’s account credentials and even going to the extent as to modify the account credentials, compromising the user’s accounts.

**Article 3**

Risk assessment (Limited to one example for each of the following four categories – use the template given and write concisely – try to keep to 1 page for each example).

Question 1c: A summary of a recent article identifying a security issue associated with mobile device user behaviour.

* Focus on what the users do or fail to do that causes the security issue.

Grading Criteria: Comprehensive summary that correctly identifies the threats, explains vulnerability, describes the incident and identifies the security goals that have been compromised.

**Article Title:** More than Half of Consumers Don’t Password Protect their Mobile Devices

**Author:** Security

**Reference details (if online article, give the URL and date accessed):** (2019). Retrieved 24 August 2019, from <https://www.securitymagazine.com/articles/89220-half-of-consumers-dont-password-protect-their-mobile-devices>.

**Brief Summary:** A recent research conducted by a well-known security company has concluded that almost 52 percent of people do not perform something as simple as password protecting their mobile device. In addition, researchers also discovered that approximately 22 percent people use software based anti-theft solutions on their mobile devices. According to the published article, most of the consumers to date rely on their mobile devices to perform rudimentary tasks such as storing and accessing sensitive digital data. Statistics show that approximately 35 percent of the people use their mobile devices to perform online banking and the lather 57 percent use their mobile devices just to do simple everyday tasks such as reading and writing emails. In addition, there are the 57 percent of people world wide who use their mobile devices to stay up to date on social media platforms such as Twitter, Instagram, Facebook and last but certainly not least, LinkedIn. As with anything digital, physical or otherwise, there is the potential for people to commit unlawful acts to gain their hands-on unauthorised information, committing crimes, etc. Having a lot of important information and precious data stored on your mobile device does not raise your awareness towards information security. Amidst all the statistics above, less than 48 percent of people of those whom were surveyed used a password to protect all the valuable content available on their mobile device, and only 14 percent of those people took steps to encrypt their files and folders to further prevent the possibility of unauthorised access. This could have devastating consequences on the consumer if their mobile device gets compromised or hacked into let alone, gets lost or stolen. Personal information such as photos, messages and not to mention financial details could be compromised. Moreover, even if the mobile devices are password protected, only 41 percent of them actually make backups of the important and personal information available on the mobile device.

**Information Asset:** Consumers personal information such as contacts, notes, photos, messages, account credentials and last but most certainly not least, financial details.

**Security Issue:**

1. **If it is a vulnerability:** The reason for a non-password protected mobile device being a vulnerability is that now, all the consumers personal information, as mentioned earlier, contacts, text messages, account credentials, photos and most important financial details are exposed to a hacker who commits either a virtual attack through the internet and the world wide web or a hacker who manages to get their hands on a physical unlocked mobile device be it through the care-lessness of the consumer or through the commission of a petty crime like theft or pickpocketing.

**Article 4**

Risk assessment (Limited to one example for each of the following four categories – use the template given and write concisely – try to keep to 1 page for each example).

Question 1d: A summary of a recent article identifying a physical threat to a mobile phone

* Lost, stolen and damaged phones are common, but there are others (you may remember 2017 reports of flaming Samsung phones).

Grading Criteria: Comprehensive summary that correctly identifies the threats, explains vulnerability, describes the incident and identifies the security goals that have been compromised.

**Article Title:** Galaxy S10 Users Continue to Report Overheating Issues.

**Author:** Value walk

**Reference Details (if online article, give the URL and date accessed):**  Jain, A. (2019). Galaxy S10 Users Continue to Report Overheating Issues. Retrieved 22 August 2019, from <https://www.valuewalk.com/2019/04/galaxy-s10-overheating-issues-continue/>.

**Brief Summary:** Sometime this year, Samsung released a few mobile phones to add to its already very popular line up (The Galaxy S10+, S10 and S10e). According to many users who did upgrade their mobile devices to the new Samsung Galaxy S10, there are still reports of excess heat being generated by the mobile phone. Some users have mentioned an unusual amount of heat is generated when the mobile device is connected to the wall outlet and left to charge. In addition, some posts on certain forums talking about this issue have said, it differs with the service provider that they are under too. People under Sprint (an American based telecommunications company) say that it could be due to the LTE signal/ data connection bug. In depth research further explains this phenomenon to be the mobile device’s inability lock on a proper cellular band. Moreover, some Exynos-based Galaxy S10 models were overheating because of a CPU-related bug that triggered after dialling or answering Voice-Over-IP based calls via platforms such as Viber or WhatsApp. For some users, the Samsung Galaxy S10 and its overheating issues could simply be due to the mobile device unlocking accidentally while it is in their purse/pocket. This could be further justified by a defect in the under-display proximity sensor and considering that the mobile device remains in an enclosed space, it causes the battery to drain rapidly thus resulting in the mobile device overheating.

**Information Asset:** None mentioned in the article

**Security Issue:**

1. **If it is a threat:** The overheating of a mobile device, as indicated in the case above, can be treated as a threat because in the more severe cases, it can lead to problems such as fires and even explosions. This can be as a result from the mobile device not being able to cut off the incoming power when it has completed its charging cycle.
2. **If it is a vulnerability:** Most users would associate an overheating mobile device with the mobile device running many background processes. This can be vulnerability, because many users don’t check the background processes that they are running. Some of these processes, could be extracting personal data or information from the mobile device as the user uses it throughout his/her day. When many background processes are running, one of the main signs is that the mobile device’s battery begins to drain rapidly and the mobile device begins to get warmer to touch.

Question 1e: A risk assessment conclusion relating to issues you have identified in this risk assessment to your personal information security.

1. This should make connections between points you made in Section (2) and Section (3). Which of your assets are most at risk – What are the vulnerabilities and the threats that could exploit them. What is the impact if your assets are affected? Why is this important for you, as the device owner/user?
2. NOTE: You do not need to discuss risk treatment options – that is in part (3).

Being an International student, studying in Australia, there are some times when the Uber app does come in handy. This is because, some times I decide to venture out of the Brisbane Central Business District and into other suburbs whether it is to mingle with friends and have fun or to visit some family relatives who live further away from the Brisbane CBD. In article 1, a breach in the Uber app would compromise my personal details as much as it does the riders. As Uber riders, it is mandatory that we provide some personal information about ourselves to the service during registration. Some of the personal details provided are names, address, email address and mobile number, not to mention, credit card information. All this information gets sent to Uber and is verified and saved on their servers as well as the app itself. Having the Uber app hacked into and the identities of their drivers in and around the United States and around the world, not to mention the riders as well, compromised could have a dangerous outcome. Someone getting a hold of my personal details such as my name, email address and mobile number could commit something as serious as identity theft and use my information to make false purchases under my name. With regards to my credit card information being stolen, the data on the servers and the app can be encoded by hackers on the magnetic stripe present at the back of most credit cards these days. This then gives hackers the opportunity to use their credit cards to make purchases, but because someone else’s credentials are encoded on it, it’s the other persons card that gets charged for the transaction. The data from the credit card can also be encoded onto gift cards and loyalty cards making it easier to commit a crime with the information at hand as gift cards can be bought readily off the shelves at local supermarkets and even some convenience stores. Identity theft and even false transactions can lead to huge sums amounting on monthly credit card statements leading to card cancellations and in some extreme cases, even bankruptcy, If the crime is not caught early.

Furthermore, in article 2, it is mentioned that those who have downloaded the latest beta profile for Apple’s proprietary operating system, iOS 13, are in serious danger on getting locked out of their accounts and having their account credentials modified if their physical device gets in the hands of the wrong type of people. I save all my account credentials on my iPhone (which includes the usernames and passwords to all my accounts) for the ease of access. This allows me to have multiple accounts online but not having to remember any of my account credentials. If I need to visit one of these accounts, I simply open the webpage, and the Auto Fill feature automatically fills in my credentials into the appropriate places on that webpage and in some cases even logs me into the account automatically. This significantly reduces the possibility of someone looking over your shoulder and guessing your passwords as you try to remember them and type them in correctly. The problem with this breach for me is that, similar to the one before, if any of my account credentials are compromised, hackers can then get access into my accounts, modify information and even steal certain pieces of information from there and use that to make false purchases under my name, a form of identity theft. Unauthorised purchases can also be made to the credit card saved on the account and details of the payer can also be extracted for use in an unlawful way.

Finally, as a mobile device owner, it is important for me to know about the security of my information being ensured as long as I store it on my mobile phone. I use my mobile phone a lot especially in part time profession I have chosen to pick up, photography. If my mobile device gets lost, stolen or hacked into, it is not just my personal details that are compromised, but the work that I keep on the device for my clients. This could result in bigger problems, such as loss of profit and even loss of customers for a small business owner like myself.

References

1. Jain, A. (2019). Galaxy S10 Users Continue to Report Overheating Issues. Retrieved 22 August 2019, from <https://www.valuewalk.com/2019/04/galaxy-s10-overheating-issues-continue/>.
2. Bhatia, R. (2019). New iOS 13 vulnerability allows access to iPhone passwords. Retrieved 22 August 2019, from <https://www.securitynewspaper.com/2019/07/16/new-ios-13-vulnerability-allows-access-to-passwords-stored-on-your-iphone/>.
3. Uber fined $148m for failing to notify drivers they had been hacked. (2019). Retrieved 16 August 2019, from <https://www.theguardian.com/technology/2018/sep/26/uber-hack-fine-driver-data-breach>.
4. Fingas, R. (2019). iPhone XS A12 Bionic chip features 7nm design, next-gen Neural Engine. Retrieved 23 August 2019, from <https://appleinsider.com/articles/18/09/12/iphone-xs-a12-bionic-chip-features-7nm-design-next-gen-neural-engine>.
5. Welch, C. (2019). iPhone XS has slightly smaller battery and more RAM than iPhone X. Retrieved 23 August 2019, from <https://www.theverge.com/circuitbreaker/2018/9/19/17879438/iphone-xs-max-xr-battery-ram-specs>.
6. Nations, D. (2019). The True Tone Display on the iPad Is Way Cool. Retrieved 23 August 2019, from <https://www.lifewire.com/what-is-true-tone-display-4048131>.
7. iPhone XR - Technical Specifications. (2019). Retrieved 23 August 2019, from <https://www.apple.com/au/iphone-xr/specs/>.
8. (2019). Retrieved 24 August 2019, from <https://www.securitymagazine.com/articles/89220-half-of-consumers-dont-password-protect-their-mobile-devices>.