Project Assignment

EE 379K: Information Security and Privacy

Student Name: Abel Philips

1 Change History (ASSIGNMENT #2-4)

Date	Description of Change	Change made by:
2/10/2020	Creation of purpose and audience description, outline data inventory and description	Abel Philips
2/21/2020	Creation of information valuation and categorization, updated purpose, and added statistics on data inventory	Abel Philips
4/15/2020	Updated the vulnerability matrix and descriptions. Created access control design section.	Abel Philips
4/24/20	Added section to describe incident response plan and give information on events, incidents, and breaches.	Abel Philips
5/9/20	Added section describing trust frameworks, technology, and design principles. Added introduction paragraph to section 8.	Abel Philips

2 Purpose (ASSIGNMENT #1-4)

This document's goal is to describe an audience that will benefit from reading its contents and provide a data inventory for Longhorn Ride. The description of the document audience will allow for those interested in our company and its operations to understand the importance of security and privacy at the company and how they play a role in its maintenance. By being properly informed of their role, the audience can help Longhorn Ride keep the chance of an information breach low. If there is such an incident, then it will assist the company and other interested groups in remedying the situation and guiding parties on how to move forward. The data inventory will lay out what data the company will collect, where it is stored, and who has ownership over it. This information can be used to figure out the level of security certain data sets have been given, which department may utilize this data, and if any other individuals outside of the company have access to this data. In the case of an information breach, it will help to determine liability, how it may have occurred, and what steps to take in the future to prevent the incident from happening again. It will also assist regulators in determining legality of operations and how the company can adapt to changes in legislation. Longhorn Ride aims to be transparent in its operations and take necessary steps to ensure that its usage of collected information remain ultimately benevolent.

The data categorizations and valuations will allow readers of the document to understand how much data collected by Longhorn Ride is worth and what security measures are being taken to protect it. Readers will understand how data is viewed by the company and how specific datasets are being protected. The valuations will allow readers to see how negligence or malicious attacks in data security can cause financial repercussions to Longhorn Ride and its users. Hopefully, this will inspire them to understand how data is used and take necessary precautions to protect it.

The vulnerability matrix and diagram will allow interested parties to understand the possible ways that information could be compromised by different factors. By viewing this section, employees can become educated of ways their actions could jeopardize secure information and how they can prevent security breaches. Additionally, outside advisers can clearly see what issues Longhorn Ride is aware of currently and can suggest additions to the list if needed.

The trusted identity section outlines the access control methods employed by Longhorn Ride. This section will allow users, employees, and others to understand some of the measures Longhorn Ride has taken to ensure the protection of their private information. Advisers can also better understand current levels of assurance for different stakeholders and suggest improvements if needed.

The incident response section will show how Longhorn Ride views security incidents and who will be involved in their resolution. Readers can find examples of security events, incidents, and breaches to better understand what they are and their distinction. Additionally, they will also be able to see what members will make up an incident response plan and how they are notified of security problems.

The information security and privacy sections detail the design choices and technology that Longhorn Ride has taken to protect data. Readers can understand how data is protected and can

provide criticism or ensure that legal and ethical standards are being met. Additionally, readers can learn some of the attacks that Longhorn Ride has implemented countermeasures against.

3 Audience (ASSIGNMENT #1)

The main groups that should read this document include users, drivers, investors, vendors, employees, and government officials. By understanding who owns data at Longhorn Ride they can evaluate how liability for data is distributed about the company and what liability they may hold. Data ownership will be shared across several departments in the company. These departments are Human Resources, Information Technology, Financial, Marketing, and Legal. Relevant data that is collected by Longhorn Ride will be accessible to and owned by one or more of these departments. All employees will need to log into an account provided by Longhorn Ride to access data related to their department. Vendors will also be given accounts with restricted access to some data that is necessary for their successful operation. Vendors for equipment and other necessities will receive accounts with access to addresses, phone numbers, and some employee emails of Longhorn Ride so they can coordinate deliveries. Some of the data collected regarding driver applicants will be shared with vendors such as a firm that does background checks on drivers. Financial records will be accessible to accounting firms hired by Longhorn Ride via accounts provided to them.

Information access will also be granted to government officials given a reasonable cause such as an investigation into a data leak. They will also be allowed to view processes used to ensure security and privacy in the workplace. With approval by the Chief Security Officer of Longhorn Ride, investors in the company may be able to view some financial information of the company and security processes being utilized by the company. As Longhorn Ride is publicly traded, financial records will be released to the United States Security and Exchange Commission when requested.

Users of Longhorn Ride and its drivers will be allowed to request to see data that the company has collected about them. Furthermore, they can request to have information deleted from company records that will not impact financial records.

4 Data Inventory (ASSIGNMENT #1)

The data inventory located in Appendix A details all the data that Longhorn Ride collects and generates. With each data element, a location is specified as to where the information is stored. This can assist the company in finding out how an information leak or error with the usage of the data occurred and how to fix it. Each element also has a specified owner(s) that are responsible for the usage and collection of that data. This helps in assigning liability to different departments as well as understanding how data that is collected will be used. Legal responsibility, such as for misuse of data, can be more easily assigned and understood. By giving ownership of the data to different departments we also increase the privacy of users, drivers, and employees by keeping parts of their information separate and not completely accessible to every employee. Additionally, regulators from the government can look through the inventory to ensure that Longhorn Ride is not illegally collecting data it should not and is following relevant laws. It can also help security experts see where data is located and if Longhorn Ride is using secure methods to store data. The valuation will allow regulators, employees, and other interested parties to see the level of risk that data at the company may hold. Hopefully, the financial repercussions of a data breach for companies and users will promote responsibility when handling data. To ensure that higher valued data is given proper protection, Longhorn Ride has categorized the data into three categories to efficiently prioritize resources to provide necessary security for different data.

5 Information Valuation and Categorization (ASSIGNMENT #2)

At Longhorn Ride we realize that we collect a diverse set of data that may be sought after by different groups and require differing levels of security. We have decided to split our data into three categories: public, private, and restricted. We believe that by categorizing into these categories we can prioritize our time and resources to protect user information effectively.

The first category is public information. This category contains data that is already public information and carries very little risk. Data in the public category can be "freely released to the public" [1]. Since it is widely available to the public "the unauthorized disclosure, alteration or destruction of that data would result in little or no risk" [2] to Longhorn Ride. Some examples of data in this category include press releases, job postings, and business contact information [1]. The main security concerns in this data category are the unauthorized modification or destruction of the data [2]. Care must still be taken to ensure that outside parties do not have direct access to the information and the ability to change it. The private category includes data that "is not protected by law or industry regulations" [1]. What separates data in this category from the public category is that "unauthorized disclosure, alteration or destruction of that data could result in a moderate level of risk" [2] to Longhorn Ride. Data that is not subject to regulations and that is not considered public information will be put in the private category. This data may include strategic operations documents, emails, and financial information that do not have restricted information. Data in this category should be given moderate security measures to protect Longhorn Ride's interests and ensure that user information is not compromised. The restricted category is for data that "is protected by law, industry or government regulation, or confidentiality and contractual agreements from unauthorized access, use or destruction" [1]. Data in this category carries a large amount of risk for Longhorn Ride if it were modified, destroyed, or accessed by unauthorized entities. This data includes bank account information, payment information, and authentication data. Data in this category needs to be protected with the highest level of security possible.

By splitting the data into these three categories, Longhorn Ride is able to prioritize the protection of data in the private and restricted categories while still allowing for the necessary precautions on public data. As restricted data can cause the largest amount of damage to both Longhorn Ride and users, focus will be given first to ensuring that it is kept secure.

The valuation of data can be extremely difficult as one must consider the importance and usage of data from multiple perspectives, including but not limited to the company, user, third parties, and criminals. Longhorn Ride has decided to take an income-based approach to data valuation where data is valued based on monetary flow it can generate in the future [3]. To evaluate this amount, Longhorn Ride will take into account the cost to purchase similar data on the black market and the monetization value by criminals. By seeing how much the data is valued by criminal entities, we can determine their motivation and demand for certain kinds of data. We will also evaluate the loss to both the company and user. If data is compromised, the company may lose valuable information which can be used for its internal operations and may acquire lawsuits from users. This could cause major losses to Longhorn Ride which need to be taken into consideration. If competitors were to get processed data, it would undermine the company's work and cause a loss of resources [3]. Finally, the cost to replace data that is

lost will also be examined to see if it is extremely expensive to replace lost data and the repercussions of such a loss for the user and Longhorn Ride. We will assign data entries a rough estimate of their value according to one of the following magnitudes: $10, $100, $1K, $10K or $100K.

After assigning a category and value to each asset, Longhorn Ride was able to notice certain trends in this data. We found that 29% of data collected was classified as public, 51.5% as private, and 19.5% as restricted. It was found that financial information, such as bank account numbers, and personal information, like government documents, were usually valued at very high magnitudes and were often classified as restricted. A large amount of vehicle data was found to be valued at a low magnitude due to its classification as public information. Other similar groupings begin to show a correlation between high value magnitudes and having a restricted categorization and lower data valuations having a public categorization. Overall, Longhorn Ride collects a large amount of data that can be exploited by criminals and other malicious entities if it were compromised. This can cause devastating losses for the company and its users if the data is not secured properly.

References:

[1] G. Firican, “Get the scoop on data classification and GDPR before you're too late,” LightsOnData, 01-Oct-2019. [Online]. Available: https://www.lightsondata.com/data-classification-help-with-gdpr-compliance/. [Accessed: 21-Feb-2020].

[2] D. Markiewicz, L. Raderman, and M. A. Blair, “Guidelines for Data Classification - Information Security Office - Computing Services - Carnegie Mellon University,” *Guidelines for Data Classification*, 02-Jul-2008. [Online]. Available: https://www.cmu.edu/iso/governance/guidelines/data-classification.html. [Accessed: 21-Feb-2020].

[3] C. Mawer, "Valuing Data is Hard", Silicon Valley Data Science, 2015. [Online]. Available: https://www.svds.com/valuing-data-is-hard/. [Accessed: 21- Feb- 2020].

[4] J. Skowronski, “The Black Market Value Of Your Identity,” Bankrate, 27-Nov-2018. [Online]. Available: https://www.bankrate.com/finance/credit/what-your-identity-is-worth-on-black-market.aspx. [Accessed: 22-Feb-2020].

6 Vulnerabilities and Risks (ASSIGNMENT #3)

It is important to understand the different manners in which Longhorn Ride's security protocols may fail via exploitation of vulnerabilities. Once we realize ways in which data at Longhorn Ride may be compromised, we can better prepare to recover from these exploits and take steps to reduce the risk of them occurring. It will also allow us to understand which aspects of the company are the most vulnerable to being exploited by certain entities and how to identify their attacks in advance.

Another important practice is identifying risks at the company. When a vulnerability is exploited, it is useful to know how and why it has impacted Longhorn Ride and its users. By identifying the risks of a vulnerability, we will understand which vulnerabilities should be prioritized in remedying and putting resources towards their prevention. Risks also tell us the value of some data and how other entities may utilize it.

To that end, Longhorn Ride has created a matrix to lay out both vulnerabilities and risks to the company. By using this matrix, you will see specific ways in which Longhorn Ride's security may be compromised and their potential repercussions. It will be used to determine the best way to approach exploits and determine the severity of an attack. For example, if a hacker gains access to a company server, they could release extremely confidential information which could cost the company an extravagant amount.

Number	Type of Vulnerability	Description of specific vulnerability occurrence	Risk posed by vulnerability	Risk Level
1.	Lack of Employee Education	Hacker uses employee login information to gain access to company server after employee gives it to them accidentally or otherwise	Confidentiality – Hacker gains access to company data and can use or release it. May sell it to malicious groups online. Integrity – Hacker can modify the data in the servers. Depending on security clearance of stolen user credentials, this could result in them changing extremely important data. Availability – Hacker may decide to corrupt data or delete it. This may make the data	High risk to confidentiality, integrity, and availability. Large amounts of data which the company may have built up over time could potentially be lost or abused extremely quickly. Depending on the security clearance of the employee, this could essentially cripple the company for months or cause it to shut down.

			practically lost or unavailable for a long time.	
2.	Disposal Procedures and Maintenance	Hardware that has been disposed of still has important data accessible on it	Confidentiality – Entities may restore information on the hardware and use it in a malicious manner, such as selling it.	High risk to confidentiality. If the hardware contains an SSN or other important personal information, it could be disastrous. Risk Impact: The risk presented by this vulnerability is especially dangerous. Information such as SSNs, credit card number, and other personal information can cost thousands of dollars to replace according to estimates in the data valuations in Appendix A. Additionally, trying to research and discover a leak of this kind may be very difficult. Assuming labor is $100/hour, it may take employees around a week before they discover faulty disposal methods. This would cost the company a large amount. Additionally, reputation would suffer as a result, lowering business. Lawsuits may also emerge due to the data leak.
3.	Lack of Employee Education	Employee lets a malicious person into a secure area	Confidentiality – The entity may gain access to paper records or computers that hold important information. Availability – The entity may destroy physical records or	Medium risk to confidentiality and availability. While it is possible for the person to destroy important physical records and devices, it would be more difficult to do so without alerting on-site security and most information is stored digitally. However, it is still possible for them to do

			hardware with data.	a lot of damage if they find a way to gain digital access.
4.	Lack of Manpower	Company server is unexpectedly overwhelmed by requests and no staff are available to help resolve situation.	Availability – A malfunctioning server may prevent access to important information until someone is found who can fix it.	Low risk to availability. An overwhelmed server is very dangerous and can cause a loss of profits due to inability to conduct services. However, we can protect against these scenarios by hiring and training staff to handle crisis situations like these.
5.	Disposal Procedures and Maintenance	Server overheats or is damaged due to poor maintenance	Availability – Data might be lost due to damage to the server failing and service might be interrupted depending on what fails.	Low risk to availability. The biggest problem raised by this vulnerability is service being interrupted. Most likely the data will be recoverable from a backup and will not cause a large loss of data. Additionally, other servers will likely be able to make up for one server failing.
6.	Lack of Employee Education	Employee falls for phishing attack and downloads malware	Confidentiality – Malware may be able to access restricted information from the user's computer. Integrity – If employee has authorization to modify data, the malware may modify information via their terminal.	High risk to confidentiality and integrity. Malware on one computer can possibly compromise an entire network and cause large amounts of data to be leaked or changed in a malicious manner. This can cause major financial losses and possibly carries legal implications. Risk Impact: Removal of malware from a system may take a long time and more manpower. At $100/hour these costs can quickly add up to thousands of dollars. Additionally, the company would lose money due to

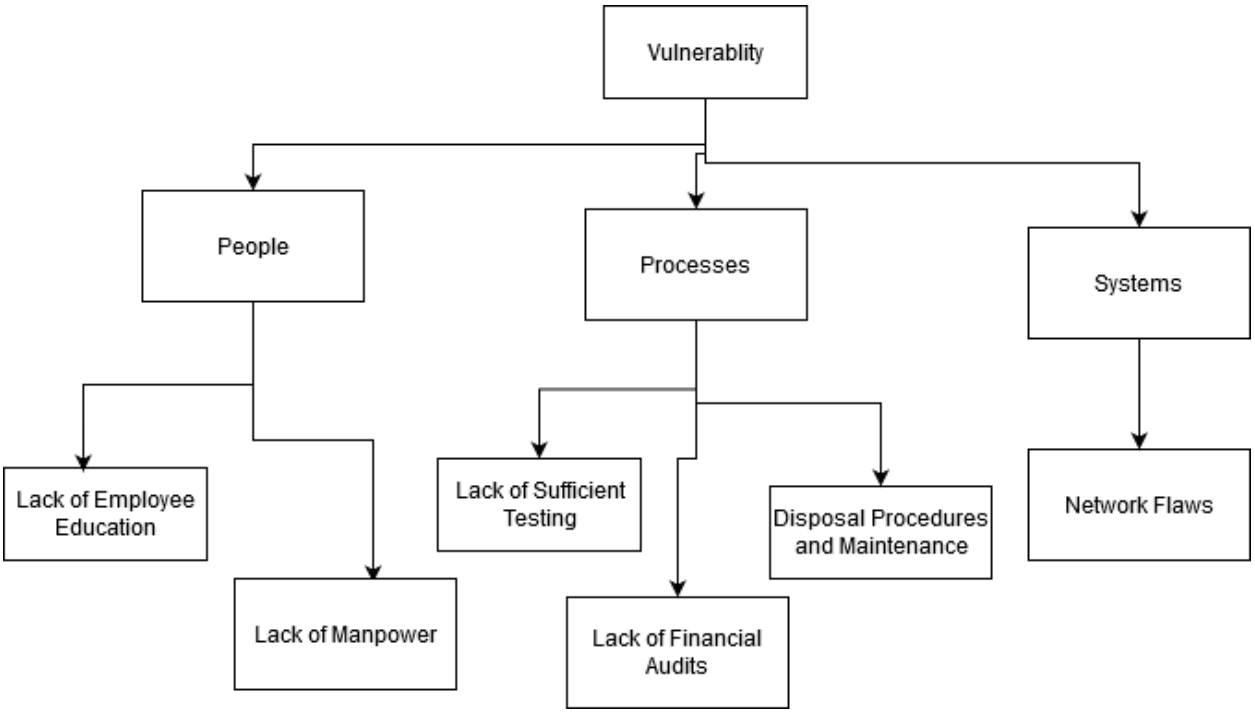
				settling potential law suits from compromised data. Business would also be impacted due to a lack of service from a system going offline for repair.
7.	Lack of Employee Education	Employee key card is lost or stolen and used to gain access to company because employee did not notify company.	Confidentiality – Depending on what information is displayed and stored on keycard, an entity may use it to impersonate them. They may also gain access to a digital system with this information. Integrity – Data may be modified if a key card provides verification to gain access to a digital system.	Medium risk to confidentiality and integrity. The key card can offer access to physical locations where data can be accessed, but there will be limited ways in which digital systems can be accessed using information on key cards. Additionally, there are methods to deactivate lost key cards once an employee reports it. Training employees to report such an event will be key.
8.	Lack of Sufficient Testing	Software has not been updated or tested on an old OS.	Confidentiality – A bug may allow users to see information they are not allowed to normally view. Availability – Due to incompatibility, user may not be able to use service or has problems doing so.	Low risk to confidentiality and availability. Bugs may allow the user to view some information which may threaten a user or employee's privacy. To prevent this, important personal information will not be stored in the cloud servers which the app will use. To counteract the availability issue, the app may be rendered unusable on certain OS versions and inform users that it is incompatible. That way even if testing is not done on an old OS, the app cannot be used on it in the first place.

9.	Network Flaws	Employees are unable to access emails or servers due to network connection being down.	Availability – Service will be unusable until connection is restored by the company.	Medium risk to availability. Without access to emails or servers, the company will be completely unable to do business and will lose considerable amounts of money. Additionally, the company may not immediately have a way to fix the network connection.
10.	Disposal Procedures and Maintenance	Technology used by the company becomes outdated or no longer supported	Integrity – If hardware or software no longer is supported by a company, exploits may be discovered that will not be patched. Entities may use these exploits to modify company data. Confidentiality – Exploits in outdated technology may allow for an entity to access information that they would not usually have access to normally.	Medium risk to confidentiality and integrity. Outdated technology presents a major problem to data security. However, by properly maintaining the technology that is used and updating it if necessary, this risk can be reduced considerably.
11.	Lack of Employee Education	Employee connects an unknown device like a USB drive into company computer and installs malware	Confidentiality – Malware might be installed onto company network via the terminal. The malware may then be used to view restricted information. Integrity – Malware may be used to modify important information on the system,	High risk to confidentiality and integrity. Malware may cause a system to be taken offline for a long time to repair it. It will also call into question the validity of data on the system and cause business to be interrupted.

12.	Disposal Procedures and Maintenance	Employee deletes a file, but it is not deleted from a backup server	Confidentiality – The data that is still available on the backup server might be accessed by an unauthorized entity in the future if it goes unnoticed.	High risk to confidentiality. If the issue goes unnoticed, it could cause legal issues for the company if the data that is still being stored is protected by a law such as GDPR. Additionally, someone may gain unauthorized access to it via the backup and exploit it.
13.	Disposal Procedures and Maintenance	Employee transfers data to an unauthorized device, such as a personal computer and it is not deleted	Confidentiality – Someone may gain access to the employee's copy of the data or the employee may use it after being fired.	High risk to confidentiality. Keeping track of copies of information can be very difficult. If the company is unaware that information has been leaked and how, it can be difficult to mitigate or detect the exploit.
14.	Network Flaws	Connection is not secure at workplace.	Confidentiality – Unauthorized entities can exploit connection and gain information of users and employees. Integrity – Entities may use the connection to modify information or requests for data.	High risk to confidentiality and integrity. Financial information or other valued data being leaked would cause the company to have to spend time and resources fixing the issue. It also makes the company liable for monetary losses and open to a lawsuit. If data is changed without the company knowing, then company operations might be compromised.
15.	Network Flaws	A server sends information to the wrong destination.	Confidentiality – Data sent may be sensitive in nature. If may end up in the hands of a malicious entity if server sends it to the wrong place.	Medium risk to confidentiality. The company would be liable for compromised data and would need to ensure the server operates properly. This would take time and resources, but it would not occur frequently.
16.	Lack of Sufficient	A driver's personal	Confidentiality – The entity should not be	High risk to confidentiality. The company will be held

	Testing	information is shown to unapproved entity	able to view the driver's information and might use it in a malicious manner.	responsible for the leak of this information. This could result in a lawsuit and having to pay reparations to the driver.
17.	Lack of Sufficient Testing	App is unusable by some users due to a programming error	Availability – The service is not able to operate as normal and inconveniences many people.	High risk to availability. If the business is not able to operate as normal the company will lose a large amount of money on lost time and efforts to fix the error. There will also be damage to the company's reputation.
18.	Network Flaws	Passwords are not encrypted when being sent over the network.	Confidentiality – Data that is highly restricted or important may be accessed by an outside entity using these passwords. Integrity – Data may be changed by an entity if they gain a high-level security clearance using the passwords.	High risk to confidentiality and integrity. The entity may view information, modify data, and release restricted data if they can gain a high-level security password like the CEO's.
19.	Network Flaws	Insecure network used to see all transactions for an employee computer	Confidentiality – Data may be accessed by a entity and used or sold. Integrity – Entity may modify data a computer receives in an unauthorized way.	High risk to confidentiality and integrity. Entity can cause a lot of damage to company using an employee terminal that has a high security clearance. It would also be difficult for the company to notice initially.
20.	Network Flaws	Company servers may not check that requests are coming from an approved source.	Confidentiality – Entity will be able to view information on the server that could be exploited to gain further access or sold. Integrity – Entity could	High risk to confidentiality and integrity. If an unapproved entity can send requests to the server it would be disastrous for the company and cause legal and financial damage. However, the chance of it

			modify the available information and change it in unknown ways.	occurring can be lowered via countermeasures such as requiring authorization tokens.



7 Trusted Identity for Information Access and Sharing Controls (ASSIGNMENT #4)

The method of access control chosen by Longhorn Ride is role-based access control (RBAC). This type of access control allows for the distribution of privileges in accessing and creating data for Longhorn Ride to be determined by a person's role in the company. At Longhorn Ride, these roles will be determined by a person's job title. For example, people working in the IT department will have privileges to assign roles and modify approved user privileges while those working in the financial department have no need to do so. Therefore, financial department employees are not given these privileges in their role.

By doing this, Longhorn Ride is ensuring that only those who require access to data will get access to it, keeping different parts of the company separate to prevent unauthorized access if an employee account is compromised. Additionally, an attack from the inside by an employee would be hindered as they will not have access to all data available at the company. One issue with RBAC is that there may be edge cases where a specific user needs access to specific data that their role doesn't normally include. They may need to then apply for access which will take time. This system also gives a large amount of power to network administrators who assign roles and permissions. If one of them acted maliciously, it may be harder to counteract in RBAC. We can help prevent this by putting in safety measures that prevent one network administrator from having complete control of the system and implementing rules for when and how they modify roles. These rules are implemented to ensure rule-based access where other conditions such as the location will be used to verify the user is who they say they are.

Type of Stakeholder	**Description of the Stakeholder**
Customer, Passenger	Requests rides from the company. They will be providing location information, phone number, login information, passwords, credit/debit card information. Need access to ability to request rides, pay, and change their own information.
Employee, Driver	Provides rides to customers. They will provide location information, phone number, login information, and bank account information. Need access to accept passengers, receive money from company, and change their own information.
Employee, Network Administrator	Manages the network of the company. Provides and assigns roles to other employees and customers. Has ability to modify others' roles and what roles have access to.
Employee, Business Analyst	Analyzes financial information of the company. Needs access to company financial records and current performance of app from day-to-day. Will also need access to information about investments and legal records.
Employee, Human Resources	Manages employee issues, pays employees, and hires new employees. Needs access to employee personal information, employee records, and

	bank account information.

Level of Assurance:

Type of Stakeholder	Classification for Information Accessed	IAL	TAL	LOA	Justification for Assignment of Assurance Levels
Customer, Passenger	Public	Low	Low	Level 1	Customers are already assumed to have a large amount of information considered public accessible to the general public. The main private information that is being protected is their location and payment information, as these are valuable and can cause damage to the user if released. Increasing the level of assurance for public information would be a waste of resources due to the large amount of customers, but the company still provides adequate protection for payment information with a level 2 classification.
Customer, Passenger	Private, Restricted	Medium	Medium	Level 2	
Employee, Driver	Public	Low	Low	Level 1	Driver information such as names or age is publicly available, so Longhorn Ride has decided that it is better to keep this information at level 1. Instead, resources are shifted to ensuring that private and restricted information for drivers is kept at level 2. This ensures that information such as their bank account is not compromised by only having one access token. This also prevents any dangers that might come from imposters pretending to be an employee of Longhorn Ride.
Employee, Driver	Private, Restricted	Medium	Medium	Level 2	

Employee, Network Administrator	Private, Restricted	High	High	Level 4	The network administrators at Longhorn Ride have the very important role of assigning roles to users and defining what different roles have access to. To ensure that the company's access control methods are not compromised, a level 4 level of assurance needs to be implemented. This ensures that the chances of an unauthorized entity gaining access to role management are greatly reduced. Due to the large effort to maintain these tokens and prevent massive damage to the company, these employees are expected to keep tokens secure and provide multiple methods of verification. Login information and some credentials are enough to ensure level 2 protection for their public information.
Employee, Network Administrator	Public	Medium	Medium	Level 2	
Employee, Business Analyst	Private, Restricted	High	High	Level 3	Business analysts have access to very important financial information and legal documents that the company highly values. Additionally, government regulations concerning some of this data need to be observed. If this data is compromised, the company will suffer dire consequences, so a level 3 assurance level is necessary to ensure that malicious entities do not leak company secrets or regulated data due to the higher financial and reputation cost. Public information has a lower priority and can be protected with employee IDs to lower costs.

Employee, Business Analyst	Public	Medium	Medium	Level 2	
Employee, Human Resources	Private, Restricted	High	High	Level 3	Employees in human resources have the responsibility to hire employees, pay workers, and manage employee issues. Due to this they need access to other employee information such as employee records and bank information. Due to the nature of their job, they have access to some important information for all other employees. This means that effort is taken to ensure that employees from other divisions of the company and outside entities cannot access or modify this information. HR employees are provided multiple tokens to ensure a level 3 level of assurance to prevent such a leak of information from happening. Login information and some credentials are enough to ensure level 2 protection for their public information.
Employee, Human Resources	Public	Low	Low	Level 2	

Stakeholder Access Control:

Type of Stakeholder	Access Control Specification	Access Control Specification applies to what part of the Information Inventory
Passenger	IF{(Role==Passenger) AND (Email==Valid email) AND (Password==Correct password)}	Public Passenger Data
	IF{(Role==Passenger) AND (Email==Valid email) AND (Password==Correct password) AND (Phone #==Valid #) AND (Credential==Code texted to phone #)}	Private, Restricted Passenger Data
Driver	IF{(Role==Driver) AND (Email==Valid email) AND (Password==Correct password) AND	Public Driver Data

	(Phone #==Valid #)}	
	IF{(Role==Driver) AND (Email==Valid email) AND (Password==Correct password) AND (Phone #==Valid #) AND (Credential==Code texted to phone #)}	Private, Restricted Driver Data
Business Analyst	IF{(Role==Business Analyst) AND (Email==Valid email) AND (Password==Correct password) AND (Credential 1==One-time code) AND (Credential 2==Employee ID #)}	Private, Restricted Business Analyst Data
	IF{(Role==Business Analyst) AND (Email==Valid email) AND (Password==Correct password) AND (Credential 1==Employee ID #)}	Public Business Analyst Data
Human Resources	IF{(Role==Human Resources) AND (Email==Valid email) AND (Password==Correct password) AND (Credential 1==One-time code) AND (Credential 2==Employee ID #)}	Public Human Resources Data
	IF{(Role==Human Resources) AND (Email==Valid email) AND (Password==Correct password) AND (Credential 1==One-time code) AND (Credential 2==Employee ID #) AND (Location==Approved IP address)}	Private, Restricted Human Resources Data
Network Administrator	IF{(Role==Network Administrator) AND (Email==Valid email) AND (Password==Correct password) AND (Credential 1==One-time code) AND (Credential 2==Employee ID #)}	Public
	IF{(Role==Network Administrator) AND (Email==Valid email) AND (Password==Correct password) AND (Credential 1==One-time code) AND (Credential 2==Employee ID #) AND (Location==Approved IP address) AND (Device==Recognized device) AND (Automated Phone Call/Text==Received and correct code input)}	Private, Restricted Network Administrator Data

8 Incident Response Plan (ASSIGNMENT #5)

This section will allow for stakeholders to understand how to identify security events, incidents, and breaches. Understanding the differences in severity and actions needed to handle these different security issues will allow for them to understand if their data is at risk and what is being done by Longhorn Ride to remedy the situation. Examples are given below to aid in identifying similar issues and how they will affect the company. Additionally, the roles of those involved in responding to an incident and details on how to contact them in the event of an incident are included.

Incident Identification:
Examples of Events:

Name of Events	Description of Event	Possible Loss	Concern for Business Continuity
Spam Emails	Spam emails are received by employees. Employees report these emails as suspicious to the IT department.	IT department may have to spend significant amount of time to look through some of the emails. Department will also use time, money, and other resources to set up filters to prevent future spam messages. Low risk of data being lost.	This event may take up time for employees in the IT department. Unfortunately, this will limit the number of employees that can work on other functions and development. Progress would become slow for some time.
Unauthorized Software	An employee downloads and installs an unauthorized software onto a company computer or device.	IT department will need to investigate and see what the software was to determine if the software is a threat. If the software is malicious, the IT department will need to take time to wipe it from the computer or any servers. HR will also take some time to deal with the employee. Since this is an event, we are assuming the software was unable to access sensitive data and instead did another undesirable behavior (adware).	The unauthorized software could damage the device irreparably and cause it to be disposed of. Additionally, some servers may need to go offline briefly so IT can determine whether the software is on them and to remove it if so. This can cause a lapse in service for customers or different departments.
Security Service	A server that is meant to	IT will need to take up	This event can cause a

Failure	handle filtering requests and provide security to other servers goes down due to a network flaw or issue at the physical location.	time to repair the connection to the server. This can also cost more money than labor costs if the physical device was damaged, such as a power surge overloading it. Due to the lack of security to other servers they might be left vulnerable, so IT may take them offline to protect them. This interruption of service can cost the company business as well as reputation.	loss of service in any department or in sending out information to customers if servers are taken down to protect them due to fear that they might be attacked while security servers are repaired. In this scenario, customers will be unable to request rides or internal processes will be interrupted.
Faulty Firewall	A firewall fails to allow through approved communications with the company or allows a connection with an unapproved source.	IT department will need to spend time to determine what is wrong with the firewall and repair it. This can mean shutting down a server for some time or needing to purchase new equipment. Departments will have difficulty doing needed work in such a scenario.	Any of the departments could be affected if they are unable to access a server due to a firewall rejecting their requests. They might be unable to do their work or access needed information until the firewall grants them access. This can halt IT, HR, financial, and legal services temporarily.
Unauthorized Device on Network	An unauthorized device connects to the company network after being given access by someone.	IT department will need to detect and find the device. This can eat up their time and take time away from other important job functions.	This event will most likely not cause any major failures in service. It is possible that it will cause IT employees to have less time to do other functions which may cause internal functions in the department to slow down.

Examples of Incidents:

Name of Incidents	Description of Incidents	Possible Loss	Concern for Business Continuity
Loss of Equipment	A piece of equipment that belongs to the company is lost by an	The IT department will need to determine the best way to recover the	The department spending time on this will mean less time to

	employee. The equipment has sensitive data stored on it.	lost device or stop anyone from accessing the data inside. This will cost time and resources to locate the device or determine a way to prevent access to the data. Also, if the general public finds out about this incident, the company's reputation will suffer. If the IT department fails to stop access to the data or get the device, it will take time to prepare for a possible information breach and find ways to mitigate it if it happens. It will also cost money to replace the device.	be put towards other processes and maintenance. If they fail, it will mean other lower priority support tickets will need to be put on hold to prepare for any information lost or to neutralize the loss.
Phishing	Employee responds to a suspicious email and provides personal information.	IT department will need to implement better security filters and determine what can be accessed with the stolen information. They may need to heighten security on other services due to this. This will have more labor and monetary cost associated with. The reputation of the company should not suffer from this incident.	If it implements higher security protocols then employees will need to adjust to the new environment, which may cause some department processes to slow. However, most services should be unaffected. HR will occasionally need to take some time to educate employees on avoiding phishing.
Employee Misusage	An employee downloads sensitive information in an unauthorized manner and takes it elsewhere.	The nature of the stolen data may cost the company a large amount to replace. It will also cost the IT department time to determine what information was taken and find a way to mitigate the loss. The HR department will also	The IT department will have less time to spend on other support and maintenance as they will need to deal with the ramifications of the lost data. This will cause maintenance and support processes to be hindered.

		need to take time to fire the offending employee. This is only an incident as we assume data was not lost that is classified as Restricted or otherwise extremely important.	
Malware Infection	Employee accidentally installs malware onto company computer. The malware may spread to a server.	The IT department will take time to remedy the malware and detect where it has gone. They will need to see what data it has accessed and prevent it from doing so. The labor cost for this is rather large. Additionally, servers may go down to clean them of malware. This will cost other departments time and may cause loss of profit if customers cannot use the service. If customers cannot access the service, then reputation will suffer.	The servers going down can prevent employees from doing important services for the company in any department. Additionally, the rideshare service may go down temporarily while the servers are cleaned.
DDOS Attack	An entity overwhelms company servers with requests, and they become unavailable.	IT department will need to respond to the incident to reestablish service. This will have labor costs. Unfortunately, this will also prevent employees from accessing important data. This will cost time to the company and money if employees cannot work. Customers will also not be able to request rides while servers are down which will mean that company reputation and profits will be affected.	The rideshare service may be taken down by a DDOS attack as servers will not be able to handle the amount of requests from customers. Additionally, internal processes at different departments will also cease temporarily if the employees are unable to access needed data.

Examples of Data Breaches:

Name of Breaches	Description of Breach	Possible Loss	Concern for Business Continuity
Theft of Equipment	A piece of equipment that belongs to the company is stolen by someone. The equipment has restricted data stored on it. This entity gains access to the data while in possession of the device and leaks it.	IT department will need to see if it is possible to stop the data from being accessed in any way which will take time. Once it is leaked, it can cost the company large sums of money if the data is restricted or private. The cost to replace it and payments required by lawsuits would be extremely high. The data on the device could also have legal restrictions.	The company would lose a large amount of money to costs associated with this data. This may cause layoffs which in turn would slow down internal processes in the departments. However, the rideshare service itself should remain available.
Employee Passwords Obtained	An employee's authorization tokens, such as passwords, are gained by a malicious entity. The entity uses the passwords to gain access to restricted data.	The labor cost to replace the authorization tokens is minimal. However, the legal costs and replacement costs of the leaked information could be extremely high. For example, if the entity gained access to an SSN the costs would be very high. Time would be taken up for the IT and legal departments to address the issue. Additionally, company reputation would suffer extremely due to perceived failure to protect data. However, impact can be reduced slightly depending on level of access that the employee has.	The damage to reputation could cause decline of use of the app over time. The time taken to respond to this issue will eat up time from multiple departments and not allow them to work on any other processes for some time or slow them considerably.
Security Protocol Flaw	The security programs and processes used by the company have an unknown flaw which	The data lost to the entity can be restricted and have legal matters associated with it. The	The rideshare service will have to temporarily go down so the IT department can

	allows unauthorized entities access.	IT and legal departments will need to spend time and resources to address the issue. Replacement and legal costs will be very high if restricted information has been leaked. Unlike in the case of employee passwords being used, if the security program itself has a flaw it will take more time to repair and the amount of information accessed will be much higher than using passwords. Company reputation will be very hard to repair once this occurs.	address the issue. Additionally, anything the IT department is doing that is of lower priority will need to be put on hold to address this breach. The legal department will also be preoccupied with lawsuits for some time, which will impact any other services they provide.
Insider Breach	Employee releases restricted data to the public.	The information revealed will be limited to what the employee had access to. If they had a high security access level, the information revealed will have a high cost. The legal department will need time and resources to handle any associated lawsuits. The IT department will also need to handle replacing data lost and determining scale of the breach. Company reputation will suffer greatly due to this breach.	Legal department will be very busy for some time due to the legal cases that can be brought up. IT will be occupied with determining the scale of the breach and replacing data so they will be unable to do other functions until the breach is resolved. The rideshare service will most likely be unaffected so customers can still use it.
Data Corruption	Restricted data on servers becomes corrupted due to an attack.	The data becomes effectively unusable in this scenario. Due to that the data would need to be recollected, replaced, or be lost forever. The costs of	The rideshare service may become unusable until the issue is resolved depending on what data is corrupted. The legal and IT departments will be

		this for restricted data will be extremely high. Additionally, there may be some lawsuits for losing important information if there are laws concerning its usage. The legal team will need to spend time and money to resolve this. The IT department will use up a lot resources and time to recover lost data. Company reputation would be hurt as well.	unable to do other functions for some time as the repair of this breach would take precedence over almost any other issue.

Incident Prioritization:

Incident Priority Level	Criteria	Justification	Example
Level 1	(Functional Impact = Low) AND (Information Impact = None) AND (Recoverability Impact = Regular)	This level of an incident will most likely not require many people to handle the issue and is not a huge threat. If an incident is Level 1 it might be inconveniencing or cause minimal harm. However, the company is still able to do regular duties, and no data is compromised. We will be able to recover from a level 1 incident quickly and with less cost.	Adware is installed on a company computer. The adware does not collect or access any data but annoys employees. The IT department can clean the computer of the adware within a short amount of time.
Level 2	(Functional Impact = Low) AND (Information Impact = Integrity Loss) AND (Recoverability Impact = Supplemented)	A Level 2 incident means that some sensitive data has been changed or lost. In this level the nature of the compromised data is not so important that it has impacted the functioning of Longhorn Ride. This incident may take some more effort to resolve as data lost or changed may be harder to detect and difficult to recover. With some more time and resources the	Company records of costs for one event have been deleted. The company can still operate normally and may be able to recover the costs from another source, possibly by working with the bank. Operations in the financial department are slightly impacted as they are unable to accurately account for costs for the event, but all other functions still operate fine.

		team may be able to replace the compromised data, but since the functional impact is low this is not a high priority issue.	
Level 3	(Functional Impact = Medium) AND ((Information Impact = Integrity Loss) OR (Information Impact = Proprietary Breach)) AND (Recoverability Impact = Supplemented)	At this level, the incident has caused Longhorn Ride to be unable to service some users due to the integrity of the data being compromised. The company will need time to recover and provide services to the users again. During this time, the company will be losing business from being unable to provide rides but can still make money as other users can still use the service. It is crucial to recover any data that is lost at this level. Additionally, if a proprietary breach has occurred, then legal issues can be involved.	Location data was modified so that it breaks the app when it is launched in some areas. The company will need to take time to resolve the matter and reestablish service in those areas.
Level 4	(Functional Impact = None, Low, or Medium) AND (Information Impact = Privacy Breach) AND (Recoverability Impact = Supplemented, Extended, or Not Recoverable)	At Level 4, data has been leaked to another entity that contains restricted data of employees, customers, or another group. This information has legal matters associated with it and could cause lawsuits. Additionally, the cost to replace the data and damage to company reputation would be enormous. At this level, the incident response team will need to deal with the incident as quickly as possible to avoid further legal issues and reputation damage.	An entity gains access to company servers and leaks employee SSNs to criminals.
Level 5	(Functional Impact = High) AND (Information Impact = Any) AND (Recoverability Impact =	At Level 5, services are not available to any user. This essentially means that the company will make little or	Flaw in the security protocols for the servers leave them vulnerable to an attack. An entity breaks the

	Extended or Not Recoverable)	no money while the issue persists. All employees who can help solve the issue will be needed immediately to resolve it as quickly as possible. Additionally, the data involved in the incident is much more difficult to recover or it may be lost forever. At this level, investigations into what occurred will need to be launched as well. Legal costs and costs to recover from the incident will be very large. If the issue persists for too long, the company's reputation may never recover from this incident.	servers with malware making them unusable. The app becomes unusable for all users for the time being.

Incident Response Team:

Incident Response Team Member Role	Incident Response Team Member Responsibility
Incident Lead	The incident lead will regularly call for meetings of the incident response team to update and develop response plans. They are also responsible for selecting members and calling the team together when needed. During an incident, they will manage the team's efforts and keep track of progress in dealing with the incident. They will contact outside help and other groups if needed. Additionally, they ensure that all other members of the team can contribute to solving the incident effectively.
Head Forensic Technician	In charge of leading the IT department and any other technical teams involved in handling the incident. They will handle the technical side of recovering from the incident by guiding the teams and providing necessary input. They are also responsible for determining why an incident occurred and who may be responsible.
Public Relations Lead	They are responsible for communicating with the public about what the incident is and what is being done. They will need to determine what should be revealed to the public and how the company will handle complaints. Their goal will be to reduce damage to the company's reputation.
Legal Counsel	They provide legal advice on how to handle the incident. They will be responsible for talking with authorities when necessary and informing the team about laws that relate to the incident. If necessary, they will handle the formation of a legal team to address any lawsuits or court cases that are brought against Longhorn Ride.

Financial Lead	They advise the team on how much money can be allocated to address the incident and how to distribute it. They will handle the distribution of resources to different teams and keep a budget for the incident. If more people are hired or outside help is brought to handle the incident, the financial lead will be responsible to ensure they are paid for their services.

Incident Response Playbook – Notification Plan:

Incident	Notify Who?	Notification Method	Notification Timing
Level 1	Incident Lead, Head Forensic Technician	Email, in-person at office	Within 10 hours
Level 2	Incident Lead, Head Forensic Technician, Financial Lead	Email, in-person at office	Within 5 hours
Level 3	Incident Lead, Head Forensic Technician, Financial Lead, Public Relations Lead	Email, text, in-person	Within 1 hour
Level 4	Incident Lead, Head Forensic Technician, Financial Lead, Public Relations Lead, Legal Counsel	Email, call, text	Within 30 minutes
Level 5	Incident Lead, Head Forensic Technician, Financial Lead, Public Relations Lead, Legal Counsel	Email, call, text, call home phone	Within 10 minutes

9 Information Security and Privacy: Trust Frameworks, Technology and Design Principles (ASSIGNMENT #6)

This section will outline the framework and technologies used by Longhorn Ride to protect against potential security incidents. Understanding these countermeasures will allow for stakeholders to understand the level of security and actions being taken by Longhorn Ride to ensure the security of data. It will also allow for criticism and improvement of the system.

Trust Framework:

The best trust framework for Longhorn Ride's purposes is federated identity management. Federated identity management allows for several useful features that Longhorn Ride has implemented in its systems. Federated identity management has "one profile with one authentication method" [1]. Due to this, for Longhorn Ride all "authentication is performed in one place, and separate processes and systems determine" [1] if a user is authenticated. Due to this, Longhorn Ride can determine whether a user has already been authenticated when they attempt logging onto the different company systems. This increases the efficiency and convenience for users and employees. The system will also be easier to maintain due to the system being in one location, however initial implementation of the technology will be difficult. The system will be somewhat complex, as it will need to assure a user has been authenticated across different systems. Keeping track of the user's activities and authentication is not trivial, so the system will be programmed with authenticity and integrity in mind. In terms of security, the convenience of federated identity management could become dangerous if a malicious entity gains access to credentials and gains access to multiple systems. To protect against this, data that is marked as higher priority will still require further authentication to access via additional tokens. This should prevent a large leak of information with only some stolen credentials.

References:

[1] C. P. Pfleeger, S. L. Pfleeger, and J. Margulies, Security in Computing, 5th ed. Upper Saddle River, NJ: Prentice Hall, 2015.

Technology Solutions:

	Data Classification	Technology or Design Principle	CIA Protection	Rationale for Selection
Data at Rest	Public, Private	Symmetric Encryption	Confidentiality	Symmetric encryption can encrypt bulk amounts of data quickly and efficiently. Data in a cloud or on a server is stored in large amounts, so it is important to encrypt it at a quick

				speed. If another entity gains access to the data, it will essentially be useless due to being encrypted. Symmetric encryption is not very secure when being transmitted, but data at rest will remain on the server until it is requested for and will be staying in one location. Therefore, symmetric encryption can be used confidently.
	Public, Private	Integrity Checksum	Integrity	Integrity checksums can determine when data has been modified on a system. They store a copy of the data in a secure location and can compare these copies to what is on the server. If it does not match, then it is likely that data on the server has been modified. This will allow for Longhorn Ride to determine when integrity of its data has been compromised. This does have some issues, especially for data that might change regularly, such as hours that someone has driven, as it may flag it falsely. However, this can be worked around by making copies regularly and manual reviews in addition to the program.
	Restricted	Intrusion Detection Device	Confidentiality, Integrity	This device protects the network by looking for

				suspicious activity. It will build a model of acceptable behavior for the network and flag suspicious behavior. This will allow for Longhorn Ride to determine when a threat forms against restricted data on the network. This can show when someone is accessing restricted data or modifying it in an unapproved manner. This technology depends on a device, which could possibly fail. To mitigate this risk, we can install multiple devices or shut down the network temporarily in case of failure.
Data in Transit	Public, Private	Firewall	Availability, Confidentiality	Firewalls will allow for access to data held by Longhorn Ride to be restricted to only trusted addresses and prevent traffic which is seen as harmful or suspicious. This will protect the confidentiality of the data as traffic that is seen as suspicious will be blocked, which will not allow them to access sensitive data. Additionally, this can help to prevent a server from being overwhelmed with requests in a DDoS attack, which preserves availability of the data.
	Restricted	Asymmetric	Confidentiality	This method of encryption

		Encryption		keeps restricted data safe from unauthorized viewing. Due to the use of a public and private key for encryption of restricted data in transit, a malicious entity would need the private key to decrypt the data. This will keep the data safe from being viewed. However, if another person gains access to the key, the data would be threatened. The chances of this occurring are low. Additionally, the cost of implementing this will be slightly higher than other methods.
Access to Data	All	Principle of Least Privilege	Confidentiality, Integrity	The role-based access control system at Longhorn Ride prevents those without a role that grants them access to data from having read or write access. This follows the design principle of least privilege, as roles are only given access to data that is necessary for them to do their work. This prevents accessing or modifying data that they are not given privilege to do so, which limits damage that a malicious entity can do with one role's credentials.

Solution Set for Network and Web Security:

Solution	Solution Description	Reduces risks with what threat?	Improves?
1. Train employees to prevent incidents from emails.	Train employees at Longhorn Ride to understand threats associated with clicking links in suspicious emails or responding to them. The company can also inform them of proper actions to take when receiving these emails.	Phishing, Spam Emails, Fake Email Messages	Authenticity, Confidentiality
2. Intrusion Detection Device	Detects when unauthorized activity occurs on the network. Can build a model to determine what traffic is suspicious and will flag it for review.	Server-side include	Confidentiality
3. Virus Detectors	Virus scanners look for malicious code in files. Can detect if a file has become infected and prevent it from running harmful code.	Keystroke Logger, Download Substitution	Confidentiality, Integrity
4. Security Event Manager	Security event managers protect the network by flagging suspicious IP addresses and behavior. They can block addresses which are flagged from contacting the network.	Distributed Denial of Service attack	Availability
5. Principle of Separation of Privilege	This design principle states that a system should not grant permission based on a single condition. The company should ensure	Man-in-the-browser attack	Confidentiality, Integrity

	that multiple credentials are required to access any data.		
6. Pretty Good Privacy (PGP)	PGP allows for messages to be encrypted and transmitted to a recipient. The recipient of the message can then validate the message's contents by reversing the steps used to encrypt it.	Message Interception, Unsecure Network	Confidentiality, Authenticity
7. SSL Certificate	An SSL certificate assures that transactions between a web server and browser are secure. Using this, users can identify whether a website they are viewing is legitimate or potentially malicious.	Page-in-the-middle attack	Authenticity, Confidentiality

Appendix A: Enterprise Information

NOTE to students: ***Your list should include at least 200 data elements.***

	Assignment #1				
Number	**Data Element**	**Location**	**Owner**	**Valuation**	**Classification**
1.	User Name	On-premise server	Information Technology (IT)	$10	Public
2.	User Date of Birth	On-premise server	IT	$100	Private
3.	User Phone OS	Off-premise server	IT	$10	Private
4.	User Email	On-premise server	IT	$100	Private
5.	User Phone #	On-premise server	IT	$100	Private
6.	User Password	On-premise server	IT	$1K	Restricted
7.	Driver Name	On-premise server	IT	$10	Public
8.	Driver Date of Birth	On-premise server	IT	$100	Private
9.	Driver Phone OS	Off-premise server	IT	$10	Private
10.	Driver Email	On-premise server	IT	$100	Private
11.	Driver Phone #	On-premise server	IT	$100	Restricted
12.	Driver Password	On-premise server	IT	$1K	Restricted
13.	Driver Car Model	Off-premise cloud	IT	$10	Public
14.	Driver Car Color	Off-premise cloud	IT	$10	Public
15.	Driver License Plate	Off-premise cloud	IT	$10	Public
16.	Driver License Number	On-premise server	IT	$1k	Restricted
17.	Driver Location	Off-premise cloud	IT	$100	Private
18.	User Location	Off-premise cloud	IT	$100	Private
19.	User's History of Drivers	Off-premise server	IT	$100	Private
20.	Driver's History of Passengers	Off-premise server	IT	$100	Private
21.	User Card Number	On-premise server	Financial	$10K	Restricted

22.	User Card Expiration Date	On-premise server	Financial	$10K	Restricted
23.	User Card CVV	On-premise server	Financial	$10K	Restricted
24.	User Card Company	On-premise server	Financial	$100	Restricted
25.	User Overall Rating	Off-premise server	IT	$10	Public
26.	History of User Ratings	Off-premise server	IT	$10	Private
27.	Driver Overall Rating	Off-premise server	IT	$10	Public
28.	History of Driver Ratings	Off-premise server	IT	$10	Private
29.	Driver Bank Name	On-premise server	Human Resources (HR)	$1K	Restricted
30.	Driver Bank Routing Number	On-premise server	HR	$100K	Restricted
31.	Driver Hours Worked Currently	Off-premise server	HR	$100	Private
32.	Driver Hours Worked Overall	Off-premise server	HR	$100	Private
33.	Driver Pay Rate	On-premise server	HR	$1K	Private
34.	Driver Miles Driven	Off-premise server	IT	$100	Private
35.	Driver Car Mileage	Off-premise server	IT	$10	Private
36.	Driver Status	Off-premise server	IT	$10	Private
37.	Drivers near user	Off-premise cloud	IT	$10	Public
38.	Users near driver	Off-premise cloud	IT	$10	Public
39.	Driver's current passengers	Off-premise cloud	IT	$10	Private
40.	User Destination	Off-premise cloud	IT	$100	Private
41.	Dropoff Order of Passengers	Off-premise cloud	IT	$10	Public
42.	Driver Path	Off-premise cloud	IT	$10	Public
43.	Maps of Areas	Off-premise server	IT	$10	Public
44.	User charge	Off-premise cloud	Financial	$10	Private
45.	User Discounts	Off-premise server	Marketing	$10	Private
46.	User Address	On-premise server	IT	$1K	Restricted
47.	Driver Address	On-premise server	HR	$1K	Restricted

48.	Driver SSN	On-premise server	HR	$100K	Restricted
49.	Driver Currency	Off-premise server	HR	$10	Public
50.	Amount to Pay Driver	On-premise server	HR	$10	Private
51.	User Disability Needs	On-premise server	IT	$100	Private
52.	Employee Name	On-premise server	HR	$100	Private
53.	Employee Address	On-premise server	HR	$1K	Restricted
54.	Employee Date of Birth	On-premise server	HR	$10K	Restricted
55.	Employee Email	On-premise server	IT	$1K	Restricted
56.	Employee SSN	On-premise server	HR	$100K	Restricted
57.	Employee Phone #	On-premise server	HR	$1K	Restricted
58.	Employee Username	On-premise server	IT	$10	Public
59.	Employee Password	On-premise server	IT	$10K	Restricted
60.	Employee Job Title	On-premise server	HR	$10	Public
61.	Employee History	On-premise server	HR	$1K	Private
62.	Employee Bank Name	On-premise server	HR	$1K	Restricted
63.	Employee Routing #	On-premise server	HR	$100K	Restricted
64.	Driver Background Check	On-premise server	HR	$100	Private
65.	Employee Salary	On-premise server	HR	$1K	Private
66.	Employee Direct Deposit Status	On-premise server	HR	$1K	Private
67.	Employee Emergency Contact Name	On-premise server	HR	$10	Private
68.	Employee Emergency Contact Number	On-premise server	HR	$1K	Restricted
69.	Employee Security Clearance	On-premise server	IT	$10	Private
70.	Employee Medical Insurance	On-premise server	HR	$1K	Restricted
71.	App Ad Campaigns	Off-premise server	Marketing	$10K	Private
72.	Employee Files	On-premise server	IT	$10K	Private

73.	User Billing History	On-premise server	Financial	$1K	Private
74.	Company Operating Expenses	On-premise server	Financial	$1K	Private
75.	Company Purchase History	On-premise server	Financial	$10K	Private
76.	Company Financial Records	On-premise server	Financial	$100K	Private
77.	Vendor List	On-premise server	Financial	$100	Private
78.	Vendor Bills	On-premise server	Financial	$1K	Private
79.	Vendor Account Username	On-premise server	IT	$100	Private
80.	Vendor Account Password	On-premise server	IT	$1K	Restricted
81.	Vendor Bank Name	On-premise server	Financial	$1K	Restricted
82.	Vendor Routing #	On-premise server	Financial	$100K	Restricted
83.	Vendor Products	On-premise server	Financial	$10	Public
84.	Vendor Services	On-premise server	Financial	$10	Public
85.	Building Locations	Off-premise server	HR	$10	Public
86.	Building Phone #	Off-premise server	HR	$10	Public
87.	Department Phone #	Off-premise server	HR	$10	Public
88.	Driver Bank Account #	On-premise server	HR	$10K	Restricted
89.	Employee Bank Account #	On-premise server	HR	$10K	Restricted
90.	Vendor Bank Account #	On-premise server	Financial	$10K	Restricted
91.	User Country	On-premise server	IT	$10	Public
92.	Driver Country	On-premise server	IT	$10	Public
93.	Vendor Country	On-premise server	Financial	$10	Public
94.	User Currency	On-premise server	Financial	$10	Public
95.	Vendor Currency	On-premise server	Financial	$10	Public
96.	Vendor Work History	On-premise server	Financial	$100	Private
97.	Gas Prices in Areas	Off-premise server	IT	$10	Public
98.	Marketing Bills	On-premise	Financial	$1K	Private

		server			
99.	Advertising Partners	Off-premise server	Marketing	$10	Public
100.	Vendor Contracts	On-premise server	Legal	$1K	Restricted
101.	User Growth	Off-premise server	IT	$1K	Private
102.	Driver Growth	Off-premise server	IT	$1K	Private
103.	Company Growth	On-premise server	Financial	$1K	Private
104.	App Bugs	Off-premise server	IT	$1K	Private
105.	User Reports	Off-premise server	IT	$1K	Private
106.	User Reviews	Off-premise server	Marketing	$10	Public
107.	Competitor Reviews	Off-premise server	Marketing	$10	Public
108.	Competitor Advertisements	Off-premise server	Marketing	$10	Public
109.	Driver Efficiency	On-premise server	IT	$10K	Private
110.	Employee Contracts	On-premise server	Legal	$1K	Restricted
111.	Driver Contracts	On-premise server	Legal	$1K	Restricted
112.	User Agreements	Off-premise server	Legal	$10	Public
113.	Trademark Information	On-premise server	Legal	$100	Public
114.	Active Patents	Off-premise server	Legal	$10	Public
115.	Ongoing Patent Filings	On-premise server	Legal	$100	Private
116.	Ongoing Court Case Files	On-premise server	Legal	$100K	Restricted
117.	Resolved Court Case Files	On-premise server	Legal	$1K	Private
118.	Laws in Countries of Operation	Off-premise server	Legal	$10	Public
119.	Employee Applicant Resumes	Off-premise server	HR	$1K	Private
120.	Employee Applicant Email	Off-premise server	HR	$1K	Private
121.	Employee Applicant Phone #	Off-premise server	HR	$1K	Private
122.	Employee Background Check	On-premise server	HR	$1K	Private
123.	Driver Applicant Resume	Off-premise server	HR	$1K	Private

124.	Driver Applicant Email	Off-premise server	HR	$100	Private
125.	Driver Applicant Phone #	Off-premise server	HR	$1K	Private
126.	Driver Applicant Background Check	On-premise server	HR	$1K	Private
127.	Driver Applicant Car Model	Off-premise server	HR	$10	Public
128.	Driver Applicant License Number	On-premise server	HR	$10K	Restricted
129.	Driver Applicant License Plate	Off-premise server	HR	$10	Public
130.	Driver Applicant Password	On-premise server	IT	$1K	Restricted
131.	Company Products	Off-premise server	Marketing	$10	Public
132.	Company Hardware Information	On-premise server	IT	$10	Public
133.	Company Hardware Sales Information	On-premise server	Financial	$1K	Private
134.	Stock Price History	Off-premise server	Financial	$10	Public
135.	Investor List	On-premise server	Financial	$1K	Private
136.	# of Shares Held	On-premise server	Financial	$1K	Private
137.	Product Troubleshooting Information	On-premise server	IT	$1K	Private
138.	Planned Features	On-premise server	IT	$10K	Restricted
139.	Employee Medical Disabilities	On-premise server	HR	$100K	Restricted
140.	Employee Performance Review	On-premise server	HR	$100	Private
141.	Employee Satisfaction	On-premise server	HR	$100	Private
142.	Employee Resignations	On-premise server	HR	$100	Private
143.	Employee Severance Packages	On-premise server	Financial	$1K	Private
144.	Internal Audits	On-premise server	Financial	$1K	Private
145.	Employee Spouse	On-premise server	HR	$10	Public
146.	Employee Family Members	On-premise server	HR	$10	Public
147.	Employee	On-premise	HR	$10	Public

	Citizenship Status	server			
148.	Employee Green Card Information	On-premise server	HR	$1K	Private
149.	Employee Work Visa Information	On-premise server	HR	$1K	Private
150.	Employee Office Location	On-premise server	HR	$10	Private
151.	Company Assets	On-premise server	Financial	$1K	Private
152.	User Device Model	On-premise server	IT	$10	Public
153.	User IP Address	On-premise server	IT	$100	Private
154.	Driver Device Model	On-premise server	IT	$10	Public
155.	Driver IP Address	On-premise server	IT	$100	Private
156.	User Third Party App Connect Data	On-premise server	IT	$10	Private
157.	Driver Third Party App Connect Data	On-premise server	IT	$10	Private
158.	User Current Time	Off-premise cloud	IT	$10	Public
159.	User Current Date	Off-premise cloud	IT	$10	Public
160.	User Time Zone	Off-premise cloud	IT	$10	Public
161.	Driver Current Time	Off-premise cloud	IT	$10	Public
162.	Driver Current Date	Off-premise cloud	IT	$10	Public
163.	Driver Time Zone	Off-premise cloud	IT	$10	Public
164.	Driver Safety Rating	On-premise server	HR	$100	Private
165.	Driver Active Status	Off-premise cloud	IT	$10	Private
166.	Employee Activity	Off-premise server	HR	$10	Private
167.	Marketing Strategies	On-premise server	Marketing	$1K	Private
168.	Employee Social Media	Off-premise server	HR	$10	Public
169.	Driver Social Media	Off-premise server	HR	$10	Public
170.	User Previous Destinations	Off-premise server	IT	$100	Private
171.	User Requests for Driver	Off-premise cloud	IT	$100	Private
172.	Notifications Sent	Off-premise cloud	IT	$10	Public
173.	Driver Breaks	Off-premise	IT	$10	Private

		cloud			
174.	Driver Satisfaction	On-premise server	Marketing	$100	Private
175.	Employee 401K Service	On-premise server	HR	$1K	Private
176.	Employee 401K Status	On-premise server	HR	$1K	Private
177.	Subsidiary Companies	On-premise server	Legal	$10	Public
178.	Subsidiary Company Revenue	On-premise server	Financial	$1K	Private
179.	Subsidiary Company Employees	On-premise server	HR	$1K	Private
180.	Subsidiary Company Costs	On-premise server	Financial	$1K	Private
181.	Ongoing Contracts with Other Institutions	On-premise server	Legal	$10K	Restricted
182.	Research Costs	On-premise server	Financial	$1K	Private
183.	Self-driving Sensor Data	On-premise server	IT	$1K	Private
184.	Settlement Payments	On-premise server	Financial	$1K	Restricted
185.	Travel Costs	On-premise server	Financial	$1K	Private
186.	Backup Server Information	Off-premise cloud	IT	$10K	Private
187.	User Battery Life	Off-premise cloud	IT	$10	Public
188.	User Service Tickets	Off-premise server	IT	$100	Private
189.	Driver Service Tickets	Off-premise server	IT	$100	Private
190.	App Heatmap	Off-premise server	IT	$100	Private
191.	Marketing Analytics	On-premise server	Marketing	$100	Private
192.	Third-part promotions	Off-premise server	Marketing	$100	Public
193.	Loyalty Program Memberships	On-premise server	Financial	$10	Public
194.	User Phone Service Provider	Off-premise server	IT	$100	Private
195.	Driver Phone Service Provider	Off-premise server	IT	$100	Private
196.	User Recommendations	Off-premise server	Marketing	$100	Private
197.	Driver Discovery Method	Off-premise server	Marketing	$100	Private
198.	User Discovery	Off-premise	Marketing	$100	Private

	Method	server			
199.	Product Returns	On-premise server	Marketing	$100	Private
200.	Profile Picture	On-premise server	IT	$10	Public