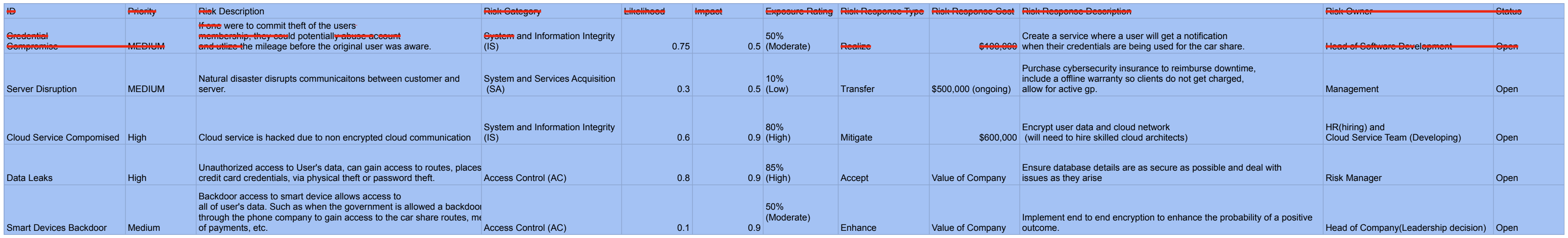
Paul Garewal
V00803658

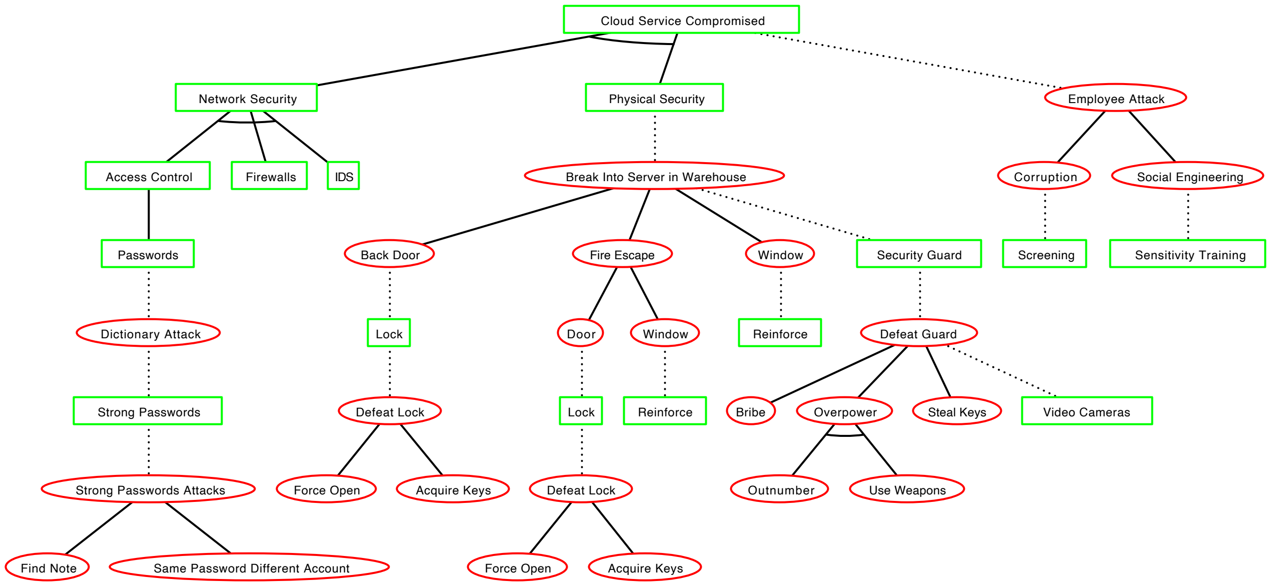
Section 1



~~ID~~	~~Priority~~	~~Ri~~sk Description	~~Risk Category~~	~~Likelihood~~	~~Impact~~	~~Exposure Rating~~	~~Risk Response Type~~	~~Risk Response Cost~~	~~Risk Response Description~~	~~Risk Owner~~	~~Status~~
~~Credential Compromise~~	~~MEDIUM~~	~~If one~~ were to commit theft of the users ~~membership, they cou~~ld potentially ~~abuse account and utlize~~ the mileage before the original user was aware.	~~System~~ and Information Integrity (IS)	0.75	0.5	50% (Moderate)	~~Realize~~	~~$100,000~~	Create a service where a user will get a notification when their credentials are being used for the car share.	~~Head of Software Development~~	~~Open~~
Server Disruption	MEDIUM	Natural disaster disrupts communicaitons between customer and server.	System and Services Acquisition (SA)	0.3	0.5	10% (Low)	Transfer	$500,000 (ongoing)	Purchase cybersecurity insurance to reimburse downtime, include a offline warranty so clients do not get charged, allow for active gp.	Management	Open
Cloud Service Compomised	High	Cloud service is hacked due to non encrypted cloud communication	System and Information Integrity (IS)	0.6	0.9	80% (High)	Mitigate	$600,000	Encrypt user data and cloud network (will need to hire skilled cloud architects)	HR(hiring) and Cloud Service Team (Developing)	Open
Data Leaks	High	Unauthorized access to User's data, can gain access to routes, places credit card credentials, via physical theft or password theft.	Access Control (AC)	0.8	0.9	85% (High)	Accept	Value of Company	Ensure database details are as secure as possible and deal with issues as they arise	Risk Manager	Open
Smart Devices Backdoor	Medium	Backdoor access to smart device allows access to all of user's data. Such as when the government is allowed a backdoor through the phone company to gain access to the car share routes, me of payments, etc.	Access Control (AC)	0.1	0.9	50% (Moderate)	Enhance	Value of Company	Implement end to end encryption to enhance the probability of a positive outcome.	Head of Company(Leadership decision)	Open

Paul Garewal
V00803658

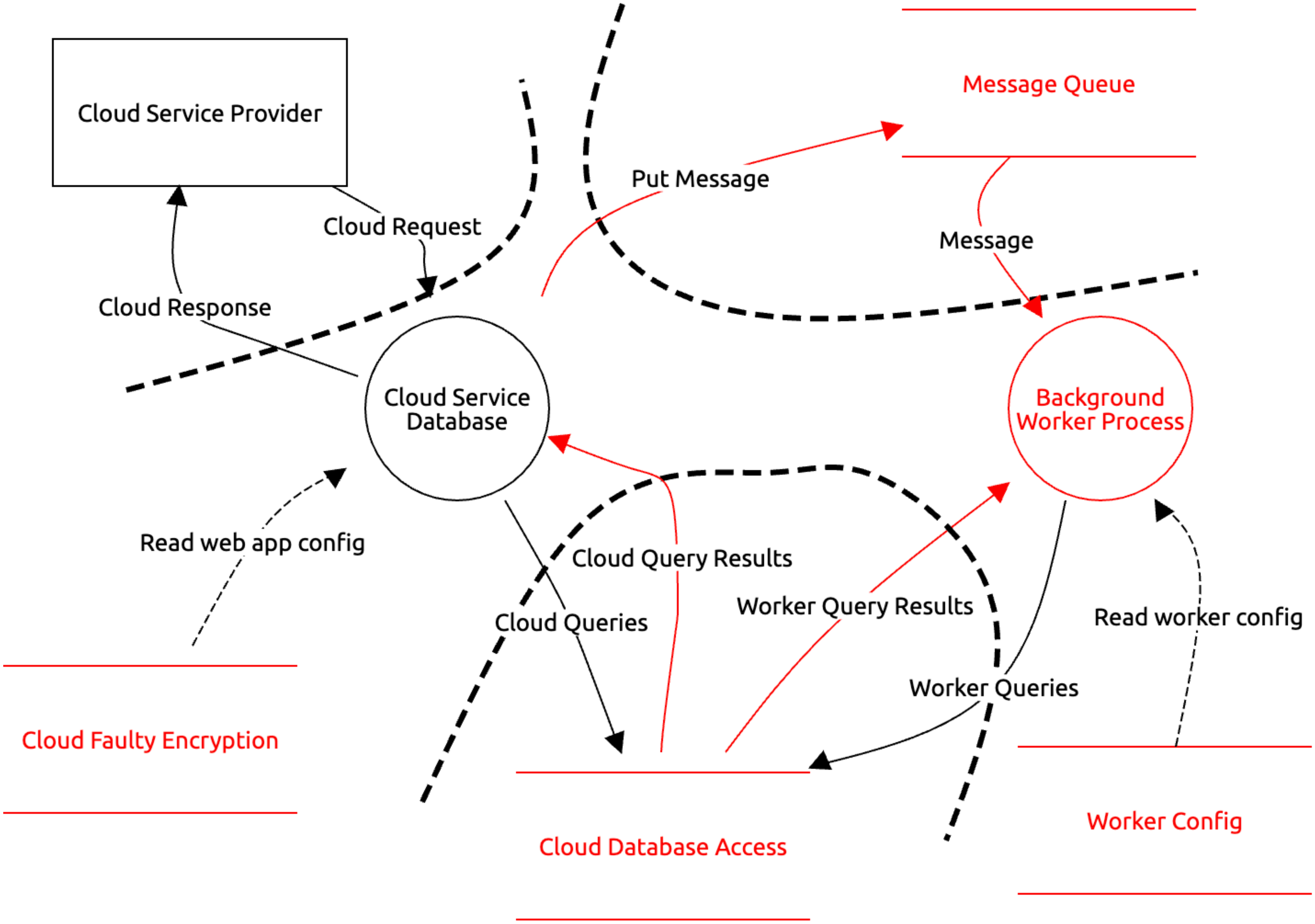
Section 2



Cloud Services attack tree. Signifies some threats from secure actions, such as network security leading to access attacks from passwords. What's interesting is that the physical security gave a lot of AND and OR branches, which went against my initial presumptions. Physical security may pose a lot of threats and counter measures, where one can never really be 100% secure. Furthermore it seems as though a lock can always be picked or a firewall can be breached and a password can be stolen from the mind of a human by means of deception rather than brute force.

Paul Garewal
V00803658

Section 3


Cloud Service Provider
Cloud Request
Cloud Response
Put Message
Message Queue
Message
Cloud Service Database
Background Worker Process
Read web app config
Cloud Query Results
Worker Query Results
Cloud Queries
Read worker config
Worker Queries
Cloud Faulty Encryption
Cloud Database Access
Worker Config