

Airbnb

Business Continuity Plan

Version: 1.0

Developed on:

**Contents**

[**Introduction**](#_heading=h.gjdgxs) **3**

[COMPANY HISTORY](#_heading=h.30j0zll) 3

[Plan Scope & Applicability](#_heading=h.1fob9te) 4

[Plan Objectives](#_heading=h.2et92p0) 5

[Plan Assumptions](#_heading=h.tyjcwt) 6

[employee risk survey](#_heading=h.3dy6vkm) 6

[**Risk Assessment**](#_heading=h.1t3h5sf) **7**

[Hazard](#_heading=h.4d34og8) 7

[attack tools](#_heading=h.2s8eyo1) 10

[security breaches](#_heading=h.17dp8vu) 13

[malicious software](#_heading=h.3rdcrjn) 17

[Malicious attacks](#_heading=h.26in1rg) 20

[**Critical Business Functions**](#_heading=h.lnxbz9) **23**

[3.1 Critical Business Functions](#_heading=h.35nkun2) 23

[3.2 Recovery Goals and Requirements](#_heading=h.44sinio) 28

[**PLAN ACTIVATION and communication PROCEDURES**](#_heading=h.2jxsxqh) **31**

[Plan Activation during Normal Business Hours](#_heading=h.3j2qqm3) 31

[Plan Activation outside Normal Business Hours](#_heading=h.1y810tw) 31

[Internal communication procedures](#_heading=h.2xcytpi) 31

[**Resumption Strategies**](#_heading=h.1ci93xb) **32**

[Business Function Resumption](#_heading=h.2bn6wsx) 33

[**Employee Contact List**](#_heading=h.qsh70q) **36**

[**Vendor Contact List**](#_heading=h.3as4poj) **37**

[**Family Emergency Plan**](#_heading=h.1pxezwc) **38**

[**Insurance Considerations**](#_heading=h.49x2ik5) **38**

[**glossary**](#_heading=h.2p2csry) **38**

[**references**](#_heading=h.147n2zr) **39**

[**Appendix**](#_heading=h.3o7alnk) **44**

# Introduction

## COMPANY HISTORY

Airbnb has always aimed to “build an “end-to-end” travel app for the global travel community” (Rothaermel, 2019). Brian Chesky and Joe Gebbia, The first two founders of Airbnb whom both attended the college in Rhode Island together, and eventually both moved to California; They met up in San Fransisco quit their jobs, then rented out their extra space in their place for extra income letting guest sleep on an airbed; hence Airbnb’s name meaning Air bed and breakfast. Airbnb, just like any other business, had it’s trial and error stages but soon they realized that once marketing was up to par the business grew tremendously; this is when they brought on the third Co-Founder Nathan Blecharczy who implemented their website for the company.

Airbnb will always be determined to maintain that their company has removed the expense of investing in a hotel building in order to house many people for their travels, the company faces no such constraints because they don't own physical real estate or hotel buildings. According to Rothaemael, Airbnb was valued at 31 billion dollars in 2019. Arguments about Airbnb have been that Airbnb is the cause of higher rent and gentrification. “Research suggests that 0.10 percent increase leads to a 0.39 percent increase in rent, and a 0.64 percent increase in home prices.” (Rothaermel, 2019). Airbnb essentially allows most people to rent out their properties directly to consumers; As well as Airbnb will accommodate hosts with professional photos of their properties, marketing, in addition to helping with proper pricing which is tailored to the demands of the year.

Fundamentally, Airbnb is a digital based web application; they’ve created a platform that does all of the searching and booking process online. There is a headquarters that employs roles that must be carried out within a location. According to Rothaermel, Airbnb eliminated the pains of person to person transactions, the reservation and payment online only. This has been the reason why Airbnb had the potential for quick growth, The unlimited potential is combined with no or low costs for adding inventory to existing online offers (Rothaermel, 2019). Airbnb striked a great deal of attention, unfortunately this also means that there is a higher risk for vulnerabilities within the web application. There is potential for areas of the organization’s application that could improve security protocols. Hackers can potentially find the vulnerabilities within the company and single handley end the company's operations.

After analyzing Airbnb’s most important functions, they entail operating transactional bookings and collecting data as reviews for both the Airbnb guest and the host. “Airbnb strives for safety as there have been some past incidents; Airbnb now outlines its precautions to address safety concerns ranging from employing analytics in risk scoring, preparedness workshops for hosts, secure payments, profiles, secure messaging, and reviews. The platform promotes a global team on 24/7 standby in 11 different languages to support hosts and guests” (Rothaermel, 2019). This leads to possible vulnerabilities within the system that can be prevented. One of Airbnb’s motivations for assets and growth is that it’s a two sided platform, one the host providing properties, and the consumers are provided demand; this will need special monitoring knowing a data breach has occurred with the platform getting limited traffic than what it was supposed to.

## Plan Scope & Applicability

The scope of this plan entails Airbnb and all of the company's most important business operations. Airbnb’s company is internationally based. After analyzing the company’s Airbnb’s website and application platform, the plan is to prevent potential cyber attacks that could potentially harm consumers/guests, hosts and Airbnb’s employees. This plan will be applicable in the event that the platform or facility is inaccessible. When monitoring the vulnerabilities of the various types of data breaches the software and cybersecurity team should also respond to regional interruptions to the area. Airbnb is website and application based, which means that attack tools, security breaches, malicious attacks, and malicious software are potential risks for Airbnb. The company’s most important processes would entail a secure server for data to be stored, Internet connectivity, encryption of all information including data stored in the system, messages and transactions.

The following portions of the organization's platform will be assessed and covered by the BCP; Guests, Hosts, Communities, Shareholders, and the Employees; Including the Chief Executive Officer, Director, Chief Security Officer, Chief Financial Officer, Global Head of Hosting, Chief Legal Officer, Chief Technology Officer, Global Head of Operations and Global head of employee experience and other employees will be in the headquarters offices since other employees remain online. In this plan of prevention we will be protecting data, assets, and network infrastructure, Intellectual property, Finances and financial data, service availability and productivity and reputation. The necessary equipment needed to implement our prevention and protection techniques will include internet connection, computers, web servers, our team, and the headquarters building supporting the technology connections. A regulatory agreement to keep in mind will be that in certain states like New York where short term leasing is illegal, and in Paris where special registration is required, these must be acknowledged.

## Plan Objectives

This document holds the Business Continuity Plan (BCP) for Airbnb, Inc..

Contained within this document are predetermined objectives to increase the rate of positive outcomes from this BCP.

The primary objectives of the plan are to:

* Identify procedures that the organization should follow when responding to emergency events to ensure critical business functions resume in a timely manner
* Protect essential facilities, equipment, personnel, and other vital assets
* Determine the recovery goals and requirements
* Identify all threats and hazards that would be harmful to critical business functions
* Determine the severity of each threat and hazard that would be harmful to critical business functions
* Identify alternative courses of action to minimize the response time
* Minimize damages and losses
* create emergency contact lists of employees and vendors to be available for contact when an emergency occurs
* Provide a guide full emergency plan for any family members of employees to convey what can be done in the case of an emergency

## Plan Assumptions

The following assumptions were used while creating this plan:

* An emergency response team has been determined
* The IT department refers to this Business Continuity Plan if or when an emergency has occurred
* The Business Continuity Plan is being updated often to adapt to current external situations
* The organization has identified available space and resources to relocate business operations within two to five days of an emergency
* The IT Department performs a Data Recovery Plan in the case that an event causes significant data loss

## employee risk survey

Included in this BCP is an Employee Risk Survey. The survey contains questions that are intended to be answered by IT helpdesk representatives or any other employees that are involved with Airbnb host and guest support. The questions are designed as multiple choice answers to determine how often the event that is being referenced in the question happens. Some questions contain answers with numerical values to determine a quantitative response. The link provided below will redirect anyone to the survey. The survey is also included in the appendix of this document (see Appendix 12).

Survey link:

<https://calstatela.co1.qualtrics.com/jfe/form/SV_5sRBt8irHkcKeR8>

# Risk Assessment

## Hazard

| Hazard | Probability | Magnitude | Warning | Duration | Risk Priority |
| --- | --- | --- | --- | --- | --- |
| Earthquake | Highly Likely | Catastrophic | Minimal | < 3 hrs. | * High |
| Tsunami | Likely | Catastrophic | Minimal | < 3 hrs. | * High |
| Fire | Possible | Critical | Minimal | 3 – 6 hrs. | * Medium |
| Flooding | Highly Likely | Limited | Minimal | 3 – 6 hrs. | * Medium |

**Earthquakes:** An earthquake is the event in which 2 of the earth’s tectonic plates create sudden movement and release a large amount of elastic energy in the form of seismic waves. This causes the surface of the earth above the location of sudden movement to shake (“Our Hazards | Department of Emergency Management”). Because earthquakes are caused by natural causes, it is impossible to prevent them from happening. Instead, all personnel should routinely be trained on what to prepare and what to do in the event of an earthquake. In addition, the core business IT systems should perform a full backup every 24 hours. All backup systems should be stored and maintained in another facility at least 50 miles or more away from the main facility. Due to the location of Airbnb headquarters in San Francisco and the city being on the San Andreas fault, earthquakes are highly likely to occur. There is almost no knowing when an earthquake will occur, so a time frame for an earthquake warning is very minimal. Depending on the size of the earthquake, the facility, equipment, and personnel within could potentially sustain catastrophical damage. The duration of the earthquake and the aftershocks would last only several minutes. For these reasons, earthquakes have a high risk priority.

**Tsunamis:** A tsunami is a large oceanic wave that is caused by an earthquake in the ocean. Depending on the circumstances, tsunamis can move towards the shores and cause a lot of damage to the areas surrounding the shores. Because tsunamis are also caused by natural causes, it is impossible to prevent them from happening (“Our Hazards | Department of Emergency Management”). Instead, all personnel should routinely be trained on what to prepare and what to do in the event of a tsunami. In addition, the core business IT systems should perform a full backup every 24 hours. All backup systems should be stored and maintained in another facility at least 50 miles or more away from the main facility. Due to the location of Airbnb headquarters in San Francisco and the city being on the San Andreas fault, tsunamis are likely to occur but not as much as earthquakes. There is almost no knowing when a tsunami will occur, so a time frame for a tsunami warning is very minimal. Depending on the size of the tsunami the facility, equipment, and personnel within could potentially sustain catastrophical damage. The duration of the tsunami would last only several minutes. For these reasons, tsunamis have a high risk priority.

**Flooding**: Flooding is the overflow of water onto land that is dry normally. To mitigate or prevent the risk of flooding is by checking the weather forecast everyday before leaving home and paying attention to the flash flood watches and warnings. We will store all important belongings and equipment on higher grounds in the building so that in the event of a flood electrical and personal belongings will be stored safely. The proper drainage systems will be implemented surrounding the headquarters including inside the building according to Helmer (2020). Protective clothing will be stored along with an emergency kit, including (emergency bag, food, a gallon of water per person, gloves, towels, silicone rain boots per person, matches/lighters; Covid-19 needs like sanitizer, antibacterial wipes, masks, and thermometers; medications advil/tylenol. Also including important paperwork and files backed up on two seperate USBs, extra cash & emergency funds, and bandages, goss, hydrogen peroxide, and neosporin/ healing ointments, flotation device for each employee in the event that water rises too high. Stairways and exit routes will be mapped and discussed with all employees in the event of evacuation. The steps that will be taken in the event that there is a flood. Stairways and exit routes will be implemented for evacuation purposes.

If flooding were to happen in the building, backups should have already occurred considering it happens every 24 hours; it is best to unplug all computers and electrical equipment; and take hard drives and computers to higher grounds, instructions will be administered by the manager stating when to unplug and move equipment to higher grounds. The probability of a flash flood is highly likely in the San Francisco/Bay area according to (CBS San Francisco, 2021a). The magnitude of flash flooding is critical because San Francisco is known for severe flooding; Flash flooding warnings generally happen about 6 hours before the event takes place, the risk of this happening in this area is high.

**Fire:** Fire hazards entail high temperatures, strong winds, and low humidity which prompts fires to happen in nature and eventually spread to rural and suburban areas. To mitigate the risk of being caught in a fire we will need to check the weather forecast everyday before leaving home and pay attention to the fire warnings. We will keep fire extinguishers in every room including bathrooms and hallways, Stairways and exit routes will be mapped and discussed with all employees in the event of evacuation; We will put flammable items in a safe storage in a dry secure spot in a closet; Designated smoking area for employees to prevent fire hazards, Make sure smoke/fire alarms are all active and updated, Protective clothing will be stored along with an emergency kit, including (emergency bag, food, a gallon of water per person, gloves, towels, silicone rain boots per person, matches/lighters; Covid-19 needs like sanitizer, antibacterial wipes, masks, and thermometers; medications advil/tylenol analyzed from the research of (Helmer, 2020b). Also including important paperwork and files backed up on two seperate USBs, extra cash & emergency funds, and bandages, goss, hydrogen peroxide, and neosporin/ healing ointments, flotation device for each employee in the event that employees need to stay in secure zone. Training for every employee on the evacuation to which If a fire hazard were to occur All employees will take clearly marked exit routes in event of fire evacuation, as well as not using elevators in event of fire evacuation and Masks must be worn for respiratory protection these actions were researched by (Londo, 2018). Important equipment like harddrives will be placed in a bag to take out of the building safety, if there is time equipment must be unplugged to avoid electrical fires. To avoid any loss of data, data will be backed up in harddrive, so that it can be used for later while employees are safely exiting the building; if there is time to move computers into safe storage or out of the building that will be important while thinking about employees safety.

In the San Francisco/Bay area it is highly likely that the probability of a fire could possibly happen. The magnitude of fires can be catastrophic. The warning before knowing that a fire may happen is very minimal because fires happen so quickly and spread quickly. The risk of fires happening in the San Francisco/Bay area is high according to (Londo, 2018).

## attack tools

| Attack Tools | Probability | Magnitude | Warning | Duration | Risk Priority |
| --- | --- | --- | --- | --- | --- |
| Vulnerability Scanners | Likely | Critical | Minimal | < 3 hrs. | * High |
| Exploit Software | Likely | Catastrophic | Minimal | < 3 hrs. | * High |
| Password Crackers | Likely | Critical | Minimal | < 3 hrs. | * High |
| Keystroke Loggers | Likely | Critical | Minimal | < 3 hrs. | * High |
| Wardialers | Possible | Critical | Minimal | < 3 hrs. | * Medium |

**Vulnerability scanner:** Vulnerability scanners are attack tools that search for potential vulnerabilities in networks, systems, and web applications. Some examples of vulnerability scanners include nmap, nikto, legion, and burpsuite (Kingatua). To help mitigate the risk of a vulnerability being exploited to an unethical hacker’s advantage, a team of certified ethical hackers should be implemented to look for and report newly discovered vulnerabilities. Vulnerability scanners are likely to be used on our systems for attackers to find vulnerabilities and use them to their advantage. Vulnerability scanners are used by both black hat hackers and white hat hackers on a daily basis and is a very common tool for hackers to have in their arsenal, so an unauthorized vulnerability scan on our network is likely. Depending on the vulnerability detected, the magnitude of the vulnerability can become critical and can happen without warning. The average duration of a vulnerability scan would take 3 hours or less because attackers most likely do not want to linger too long and risk being detected and found (Kingatua). Therefore, we claim vulnerability scanners to be of high risk priority. If an unauthorized vulnerability scan is suspected, our cybersecurity specialists should deploy the ‘honeypot’ network to attract the attacker’s attention from the main network. In addition, an authorized vulnerability scan should be performed to identify and reinforce potential vulnerabilities.

**Exploit software**: Exploit software is an attack tool that is used to target known specific vulnerabilities in systems. Some examples of exploit software include Metasploit, searchsploit, and sqlmap. To help mitigate the risk of a vulnerability being exploited to an unethical hacker’s advantage, a team of certified ethical hackers should be implemented to look for and report newly discovered vulnerabilities. Exploit software is likely to be used by attackers to gain access to databases that contain vital information such as usernames, passwords, and credit card information. Similar to vulnerability scanners, Exploit software are other common tools that hackers obtain either by legal purchases or on the black market. Once a vulnerability is detected and exploit software is used against the vulnerability, the magnitude of the situation could be catastrophic. Because a prior vulnerability scan can go undetected, an exploit software attack can occur at any given time with minimal warning. On average, the attack would last 3 hours or less (Kingatua). Given the circumstances, we place exploit software as a high risk priority. Should an exploit software attack happen, all systems should be restored using backup images or system recovery points. Authorized vulnerability scans should then be performed and all identified vulnerabilities should be dealt with in a timely manner.

**Password crackers**: Password crackers are attack tools that are used to input passwords and gain unauthorized access to any systems, networks, or accounts. Some examples of password crackers include ncrack, medusa, cewl, and ophcrack. To help mitigate the risks from password crackers, Systems must implement a limited number of password attempts for users. When the limited number of login attempts are reached, users should be temporarily unable to login in case an attacker is attempting to use a password cracker. Attacks using password crackers are common and if successful can cause critical results. Password crackers are another common tool that are used on a daily basis by hackers. For that reason, it is likely that our network access points and or devices connected to the network are vulnerable to password crackers. The magnitude would be critical because the attacker may gain access to confidential emails, data, or personal information. The attacker may also begin to sniff packets that travel through the network. An attack with a password cracker may happen with minimal warning and last less than 3 hours (Frankie Wallace). Thus, we rate the risk priority of a password cracker as high. If a certain department has highly suspected a password crack attempt on their network or systems. All employees from within that department shall be required to enter a new password. IT Operations should also implement new passwords on routers, servers, and Administrative workstations that were affected.

**Keystroke loggers**: A keystroke logger is malicious software that is considered as spyware. Once a keystroke logger has infected a victim, the keystroke logger begins to record any input from the victim’s keyboard or mouse-clicks and send that info back to the attacker. To help mitigate the risks of attackers stealing information with keystroke loggers, the systems must constantly be updated with the latest versions of operating system security and anti-virus software.

The cybersecurity industry is constantly on the lookout to identify new viruses and add their virus signatures to anti-virus signature databases. Unintentionally downloading a keystroke logger is likely to happen and would be critical if the attacker obtains personal or confidential information. In addition, there would be minimal or no warning when a system is infected with a keystroke logger (Kingatua). Thus, the risk priority for keystroke loggers is high.

**War dialers:** A war dialer is an attack tool that is used to dial a large volume of telephone numbers. Their main objective is to collect information on whether the devices that answered are modems, fax machines, or any other devices of interest. To help with the risk against a war dialing attack, the number of devices connected to a phone line shall be limited to the least amount possible. In addition, call-back devices should also be implemented to automatically reject suspicious incoming phone calls. Unlike the previous attack tools mentioned, War dialers are less commonly used by hackers but would still result in critical magnitude. A war dialing attack could happen at any time with minimal warning and would last 3 hours or less because hackers want to reduce the risk of their attack being detected. Given these reasons, the risk priority for war dialers is set at medium (“WAR-DIALING :: Chapter 11: Probing a Target :: Part 3: Breaking and Entering Computers :: Steal this computer book 3 :: Misc”). In the event that a war dialer is suspected to be in use without authorization, all phone lines should be temporarily disconnected and all phones, fax machines, and modems connected to phone lines should have their numbers changed.

## security breaches

| Security Breach | Probability | Magnitude | Warning | Duration | Risk Priority |
| --- | --- | --- | --- | --- | --- |
| Distributed Denial of Service Attacks (DDoS) | Highly Likely | Catastrophic | Minimal | 3 – 6 hrs. | * High |
| Backdoors | Highly Likely | Catastrophic | Minimal | 12+ hrs. | * High |
| Data  Modification | Highly Likely | Catastrophic | Minimal | 12+ hrs. | * High |
| Hoaxes/Phishing/ Scams | Highly Likely | Catastrophic | Minimal | 3 – 6 hrs. | * High |
| Cookies | Highly Likely | Critical | Minimal | 12+ hrs. | * Medium |
| Unacceptable  Web Browsing | Likely | Critical | 4. Minimal | < 3 hrs. | * High |

**Distributed Denial of Service (DDoS)** **attack**: is a different type of a DoS attack that entails extremely large numbers of attacking computers to overwhelm the target with fake traffic. To prevent the risk of a DDoS attack it to create a DDoS response plan, the plan entails how to respond to a DDoS attack, when a DDoS attack happens the first step is upload data remaining data to the cloud server then the manager will upload data to external hard drive, then the second step will be to disconnect the network so that the flood will seize, we will also need to implement higher levels of network security, have server redundancy by using a contain delivery network (CDN) in research from (Osborne, 2020). This means we will use a virus scanner, if something is found we will implement the malware and virus cleaning/removal software, after that is done we will reboot or restart the computers. Once the computer is rebooted, we will virus scan again to check computers, then we will reconnect the network (Wi-Fi) and check if any data is missing and monitor it closely.

We can look for the warning signs like poor connection, slow performing tasks, crashes, and unusual traffic coming from different IP addresses, and continuous monitoring of network traffic. If the security breach were to occur, these are the steps that will be taken if DDoS attack occurs. If one is able to manage the website, put it in maintenance mode so that no data will be lost. Call the ISP and tell them you are under DDoS attack, Capture as much information as possible. Report the time of day/night when it happens to keep record and when necessary engage with experts on services like cloudflare, DOS arrest, Incapsula, and more for help in research from (Osborne, 2020). A DDoS attack is highly likely to happen considering the fact that DDoS attacks occur every 60 seconds daily, the magnitude of DDos attacks can be catastrophic in the case that data can be erased, there are minimal warning time when a DDoS attack can happen since it can happen anytime, the duration of a DDoS attack could last up to 4 hours. The warning for a DDoS attack is minimal. The risk priority can be high considering the fact that Airbnb has been under attack in recent years in research of (Cucu, 2022).

**Backdoors**: A backdoor invokes any procedure by which authorized and unauthorized users are able to get around usual security measures and gain high level user access (aka root access) on a computer system, network, or software application. Once they're in, cybercriminals can use a backdoor to steal personal and financial data, install additional malware, and hijack devices according to (Osborne, 2020). If a backdoor were to show presence on a computer, the first thing to do will be upload all remaining data to the cloud server, then the manager will collect it and transfer it to an external hard drive; after the data is transferred the network will be disconnected, then a virus scanner will be utilized to scan for backdoors. If a backdoor, rootkit, or trojan is found we will use our rootkit removal software because it does different removal techniques than a normal virus/malware removal software. After the backdoor is removed the computer will be rebooted; ater system is rebooted we will scan with backdoor/rootkit scanning software again then reconnect the network (Wi-Fi). After Wi-Fi is connected we will make sure no data is missing, and monitor the systems closely.

Backdoor malware is generally classified as a Trojan. A Trojan is a malicious computer program pretending to be something it's not for the purposes of delivering malware, stealing data, or opening up a backdoor on your system. There’s also rootkits which gives the unauthorized user root access to security operations, there’s hardware backdoors and software back doors. The best way to prevent backdoors from happening would be to Use an antivirus to protect the computers, Be mindful of what is downloaded on the computers, Implement a firewall, Utilize a password manager, and Stay updated with security updates and patches. In this situation the best way to get rid of a backdoor would be to use a backdoor removal software since they are hard to remove manually in research of (Osborne, 2020).

Backdoors are highly likely to happen considering that Airbnb has had a data breach in 2020; The magnitude of backdoors can be catastrophic considering that all data can be modified or erased. The warning of time before knowing a backdoor attack can happen is minimal, it can happen with no warning signs. Backdoor attacks can last 12+ hours because backdoors can be installed and running without the user knowing, so it can run for hours at a time. The risk priority is high for backdoor attacks this is new research from (Kiguolis, 2021).

**Data modification:** Data modification: attacks where a hacker decides to not take the data, but instead make subtle,secretive changes to the data for some type of gain, can be just as immobilizing for companies compared to theft. There are various ways to mitigate the risk of a data modification attack. One way of mitigating data modification is integrity checking; many companies are beginning to use integrity or hashing checking software, this ensures that there are no errors during the process of restoring data. Another great way to mitigate the risk of data modification is File Integrity Monitoring (FMI) is a system that is installed and will send us alerts when data is modified and it can also determine what data is eliminated according to (Townsened, 2019). A good way to track the unauthorized user is having endpoint visibility; is a software that is implemented by the IT technician and it gives the analyst a tracing route when data has been modified. Another great way to counteract data modification attacks is implementing encryption; many companies do not use this but this ties into integrity checking. This is one of the best ways to prevent data modification attacks. We also need to create a periodic backup schedule, and utilize firewalls in research from (Townsened, 2019).

In the event that a data modification attack occurs, we need to disconnect the computer from the network then we will need to reinstall the operating system. We must turn on the network's firewall, and change the password. Install antivirus software, then we can reinstall apps in the operating system and refrain from downloading or visiting untrustworthy applications or websites. according to (Reinstalling Your Compromised Computer | Information Security Office, 2022).

The probability of data modification occurring is highly likely considering that most people doing a data modification attack are profit driven since they mainly target financial, healthcare and government data (Brooke, 2019). The magnitude could be catastrophic considering that data is one of the most important components in growing the company’s assets, so without important data it will make it a challenge for the company. The warning time for this risk to happen is minimal considering that a data attack happens within a few seconds. The duration of a data modification attack could be up to 12 hours, and the risk for a data modification attack is high.

**Hoaxes**: This is often a chain message telling users to forward the mail to all their contacts. The aim is simply to cause alarm and confusion among users. Mainly to manipulate the user. Examples of hoaxes are scams and phishing emails. To mitigate the risk of hoax, scam, and phishing emails, the following actions will be taken for prevention. Filtering the emails that are transported to and from people outside of the company, it will be used to screen headers and malicious content; using software to filter emails also includes examining URLs and the system will follow specific rules. We can also utilize a sandbox or denotation chamber to cautiously remove malicious links. Blocking emails that contain a size too large will be blocked from company operations. Implementing warning messages to users when the contents of the email including attachments are not included in the organization. In the event that the company often receives phishing emails we will implement phishing protection inside the place where we receive emails according to (Cisa 2022).

In the event that an employee clicks on a phishing email and the computer is under attack we will need to disconnect the device, it’d be good to turn the Wi-Fi off as well so that the malware will not spread. Backing up our files would be the next action to save all the data possible. We will then use a virus scanner to scan our software; then we will change our passwords and then we will set up a fraud alert so that the crime will be reported automatically. Hoax emails are a high probability of happening if it's not prevented; The magnitude could be catastrophic because the damage could be severe depending on the software that is downloaded. There’s not usually a warning before being able to check the email header for unusual senders from outside of the organization. The duration can be a few hours because the anti virus software will be removing the malicious attempt. The risk is high considering the emails for phishing have ramped up since 2020.

**Cookies**: The reason for the cookie is to help the website keep tabs of your visits and activity. Most internet retailers utilize cookies to keep tabs of the items in a user’s shopping cart as they explore the site.; without the use of cookies, our shopping carts would reset to zero each time you clicked a different link on the site. This would make it impossible to buy anything online. In the event that a harmful cookie has infiltrated the system the first thing we would need to do is upload all remaining data to the cloud server, management will then transfer the data to an external hard drive; we will then need to clear all cookies; management will instruct all employees on how to clear all cookies off the computer; the system will then be restarted, scanned with antivirus software, and then will be monitored closely.

A website may also utilize cookies to keep recordings of your most recent visits or recording your login information. A “zombie cookie” is a cookie that regenerates itself after being deleted, this makes zombie cookies more complex to manage. Third-party tracking cookies can also bring up security concerns, since they make it easier for users you can’t spot the cookies to watch where you are going and what your actions are online. Actions that can be taken to prevent harmful cookies from damaging the organization is requiring a secure connection; this means that only trusted protocols will be able to reach the host destination (AIRBNB); we will configure our browser to send cookies only using SSL connections because SSL is the most secure. We will monitor the network. Another action in order to prevent a harmful cookie from infiltrating is using the HTTPOnly flag which will let the browser know that it's not allowed, that does not allow hackers to be able to infiltrate the vulnerabilities in the system. The probability of the organization foreseeing a harmful cookie in the system is likely; the magnitude of this occurrence can be critical but not catastrophic in the fact that cookies themselves aren't harmful, it is the software that could be attached and most likely will be a tracking system for browsing history. There is not much of a warning in considering the fact that a cookie can be installed in one click. Cookies can stay on a browser indefinitely if it’s not removed. The risk for this occurrence is medium in the fact that cookies can easily be removed from research from (J. 2022).

**Unacceptable Web Browsing:** Visiting internet sites that contain obscene, hateful, pornographic or otherwise illegal material or utilizing the computer to perpetrate any form of fraud, or software, film or music piracy. To mitigate safe use of the internet within the organization, we will ensure that our policies are clear and concise, and we will filter the browsing options with an Internet management system; this will have a component that is able to track the data an employee is research and for which person may need a corrective action, as it will improve endpoint security within USB control access configurations according to (Strickland, 2021). In effort to prevent the risk if occurence the first step will be to install a software that manages bandwidth that each employee is using; when high bandwidth is used for applications like Youtube, Netflix, HBO etc, then the internet's performance is reduced drastically; this will monitor each employee's bandwidth usage. Recording the details of the incident will take place as well.

In the event that the computer has been infected from unacceptable web browsing, which will be filtered out by the filter thats been placed on the browser for the company; but if an instance where unacceptable web browsing occurs and a risk has been found, all employees in the department will upload all data to the cloud, the manager will transfer the data to an external hard drive; a virus scan will be implemented if a risk is found, the system will be disconnected from the network “Wi-Fi” the security breach will then be removed; the system will be restarted (rebooted) then another scan will take place; after nothing is found, the system will be closely monitored for unacceptable web browsing.

The probability of unacceptable web browsing is high considering that if there’s not a plan implemented for employees it’s highly likely to happen. The magnitude of unacceptable web browsing can be critical considering that untrustworthy software can accidentally get downloaded into companies operating systems. There’s not usually a warning when unacceptable web browsing happens; sometimes it's quick depending on what is requested of the user. The duration of unacceptable web browsing can be minimal or longer depending on the task of the user. This occurrence is high in research from (Strickland, 2021).

## malicious software

| Malicious Software | Probability | Magnitude | Warning | Duration | Risk Priority |
| --- | --- | --- | --- | --- | --- |
| Spyware | Likely | Catastrophic | Minimal | 12+ hrs. | * High |
| Worms | Highly Likely | Catastrophic | Minimal | 12+ hrs. | * High |
| Virus | Highly Likely | Catastrophic | Minimal | 12+ hrs. | * High |
| Trojan Horse | Highly Likely | Catastrophic | Minimal | 12+ hrs. | * High |
| Rootkits | Possible | Catastrophic | Minimal | 12+ hrs. | * Medium |

**Spyware**: Spyware is a certain type of malicious software created to go into the user's computer device, collect data about the user, and send it to a third-party without your consent. Spyware can also refer to legitimate software that monitors your data for marketing purposes like advertisement. On the other hand, malicious spyware is used exactly to profit from data that is stolen. A good example of spyware would be a keystroke logger, or “keystroke capture parasites”. To mitigate the risk of spyware infiltrating the system we can run at least two spyware cleaners at all times, this ensures that the companies systems are protected. Another action we will take in order to prevent spyware from being able to infiltrate is closing the desktops communication holes; this ensures that when automatic updates happen nothing untrustworthy can disguise itself as “new features”.

In the event that spyware has been found in the companies operating systems to mitigate the risk we will begin by disconnecting the internet router, then we will uninstall the program that our scanning software found. After we delete the program, we will scan the computer once more to ensure all spyware is removed. The probability of spyware being found in the system is highly likely considering there are no filters on the organization's internet browser. The warning is minimal considering it only takes 18 seconds for malware to infiltrate a system. Spyware can stay on the computer until it is removed; the risk of spyware can be high if it's not prevented properly according to (How to remove spyware from your computer, n.d.).

**Worms**: A computer worm is a certain classification of malware that can spread copies of itself from computer to computer. A worm can replicate itself without any human interaction, and it does not need to attach itself to a software program to cause damage. Worms can enter the system through the internet, Emails, platforms that are able to share files, instant messages, mobile phones, IoT devices, removable drives and more. The actions that should be taken in order to prevent worms from being able to infiltrate the system would be to be attentive when downloading files; best idea would be to not open files from unknown senders. Another way to prevent worms in the company's systems is to not click on pop up ads when browsing the internet; worms can inject adware in legitimate websites. When mitigating the risk of worms we must also update our software regularly as well as employee passwords. We will also perform frequent backups of data.

If a worm was found by our security protection softwares we will need to quarantine the device; meaning we will need to disconnect it from the internet and remove it from the LAN network since worms can spread through the LAN network so it will potentially reach multiple devices. We will then scan the other devices to see if any others have been infected with worms as well. If we do find worms we will use a software to remove specifically worms. The probability of worms infiltrating the system is highly likely considering that worms are one of the most frequently used types of malware. Worms magnitude of damage can be catastrophic because of the fact on how worms can spread device to device and cause irreplaceable damage. There is minimal warning time with a worm infecting a computer because it can all happen in the matter of a few seconds. If not handled properly a worm can have a system down for several hours; the risk of a worm is high and should be handled with proper preventative measures.

**Virus:** A computer virus is a malicious piece of computer code designed to spread from device to device. A subset of malware, these self-copying threats are usually designed to damage a device or steal data. The first action that we will take to ensure virus protection is by downloading anti-virus software. We will educate all employees on internet safety like noticing untrustworthy email attachments, and not open emails from unknown senders and avoid untrustworthy websites. We will also make continual backups. We will also patch our operating system by regularly updating our software whenever a patch is available. If a virus were to infiltrate the companies system the following action will need to be taken; we first must download and install a virus scanner, after we must disconnect from the internet. The following action will reboot the computer into safe mode, then delete all temporary files. We will then run a virus scan again then delete or quarantine the virus. We will now reboot the computers, update passwords, and software, our browser and the operating system.

The probability of getting a virus on the company's operating system is high without the right preventative measures. The duration of a virus varies, it can last several hours and the magnitude can be catastrophic considering that sometimes data can be irreplaceable. When not properly mitigating the risks, the risk is high for getting a computer virus according to (What Is a Computer Worm and How Does It Work?, 2022).

**Trojan Horses:** A Trojan horse, or Trojan, is a classification of malicious code or software that looks authorized but can take control of your computer. A Trojan is engineered to harm, disrupt, steal, or in general inflict some other destructive action on your data or network. It can download a keylogger to monitor keystrokes. In effort to prevent trojans from infiltrating the companies system we will need to have anti-virus software installed and a Trojan Remover. This software will alert the user if the device has possibly been infected with a trojan. Another great way to prevent trojans is by implementing our browsing filter so that warnings will pop up when going to an untrustworthy website and practicing internet safety by not downloading files from unknown users and not visiting websites containing harmful trojan software. In the event that a trojan horse has infiltrated the system, the first action is to restart our devices and put it into safe mode; we will add or eliminate programs that have been affected by the Trojan Horse. We will also remove extensions, and in order to do that we have to remove the files from the system folder.

The probability of a trojan horse infecting the companies system is high for the fact that they disguise themselves as email attachments, spoofed messages (pretending to come from someone you may trust), infected websites and more. The magnitude of trojan horses can be catastrophic because they are meant to cause harm to the network, like steal data. A trojan horse can infect one's computer in the matter of seconds; a trojan horse can last up to 200 days if undetected collecting passwords and other data. The risk for a trojan horse is considerably high for the fact that they can be disguised in emails, pop up ads, and more according to (Kaspersky, 2021b).

**Rootkits**: A rootkit is a malicious software computer program created to supply continuous privileged access to a computer while actively disguising its presence. Rootkits are most widely used with Unix/Linux programs. They are powerful because they can disable anti-malware and anti-virus software. Rootkits are advanced and this risk can be properly mitigated by the following actions. We must scan our systems, specifically with rootkit scanners. Another way to prevent a rootkit attack is to avoid phishing attempts; this is when one can receive an email or message to swindle users into clicking a malicious link and or infected attachment. We will also need to update the company's software. Another effective action to detect a rootkit would be to use next-gen antivirus; this will tell the user where the rootkit originated, and essentially block it from the company's system.

In the event that a rootkit attack has infiltrated the company's system we will implement rootkit removal software. We will next enact a boot time scan, the reason is because rootkits can outsmart automatic antivirus scans; next if the last step didn't work we will need to backup your data, (considering we have already done this) we will need to delete everything the system and reinstall it from a clean start. This will be the last option to remove a rootkit. The probability of a rootkit attack is possible but it's not as common as other types of malwares, rootkits are responsible for less than 1% of the cumulative malware discovered. The magnitude of rootkits damage can be catastrophic in the sense that they can launch DDoS attacks, heightened privileges and embezzle sensitive data. The warning is minimal considering that software can be downloaded within a few seconds, but a rootkit can remain in place for years if not detected. The risk is medium considering rootkits are harder to install according to (Norton, 2021b).

## Malicious attacks

| Malicious Attack | Probability | Magnitude | Warning | Duration | Risk Priority |
| --- | --- | --- | --- | --- | --- |
| Brute Force Password Attack | Highly Likely | Critical | Minimal | 3 – 6 hrs. | * High |
| Dictionary Password Attacks | Highly Likely | Critical | Minimal | 3 – 6 hrs. | * High |
| Session Hijacking | Likely | Critical | Minimal | 3 – 6 hrs. | * High |
| Man-in-the-Middle Attacks | Likely | Critical | Minimal | 3 – 6 hrs. | * High |
| Social Engineering | Highly Likely | Critical | Minimal | 12+ hrs. | * High |

**Brute force password attack:** A brute force password attack is an attempt to crack a password by inputting all possible combinations of characters. By implementing a password length of 8 characters or longer, requiring password changes every 60 - 90 days, and having a limited number of login attempts, we can diminish the rate of successful brute force password attacks. Should a brute force password attack be detected, all personnel should be required to do a password change and login attempts should be temporarily unavailable.

Bruteforce password attacks are common and depending on the length and complexity of passwords, attacks can have a duration of 3 hours or more. A successful attack would cause critical results and can happen at any time without warning. Thus, the risk priority for a brute force password attack is high.

**Dictionary password attack:** A dictionary password attack is very similar to a brute force password attack. It is an attack that attempts to crack a password. However, the key difference is that a dictionary password attack uses a large list of commonly used words to provide as input for the algorithm. In addition to requiring users to use special characters in their passwords, the same regulations to mitigate a brute force attack should apply. Implement a password length of 8 characters or longer, require password changes every 60 - 90 days, and have a limited number of login attempts. Should a dictionary password attack be detected, all personnel should be required to do a password change and login attempts should be temporarily unavailable.

Dictionary password attacks are common and depending on the length and complexity of passwords, attacks can have a duration of 3 hours or more. A successful attack would cause critical results and can happen at any time without warning. Thus, the risk priority for a brute force password attack is high.

**Session hijacking:** A session hijacking attack occurs when an attacker takes control of a user’s internet session by obtaining info of the user’s session ID with a web application. By doing so, an attacker can fool the server into thinking that the attacker’s computer is the victim’s computer and will be authorized to perform what the victim can do. An example would be if the victim logged into their bank account on the web and the attacker hijacked his session. Then the attacker would be able to steal money, take out a loan, and or commit identity theft. Some of the practices that should be done to reduce the chances of session hijacking are to require users to use Virtual Private Networks (VPNs) to encrypt network traffic and force HTTPS protocols when accessing the web (Poremba). Because of the amount of session IDs transmitted through networks, session hijacking is likely to happen and would cause critical data breaches or financial losses to any company. A session hijack could last up to 3 hours or more. For these reasons, session hijacking is considered a risk of high priority. If a user is experiencing a session hijack, the cybersecurity teams should be notified and force the servers to terminate all connections. This would require all previous connections to be restarted and use different cookies and session IDs. The teams should also check again if https protocols are being enforced. (Poremba)

**Man-in-the-Middle attacks:** A Man-in-the-Middle attack occurs when an attacker intercepts a connection between a victim and a web application. As a Man-in-the-Middle, the attacker can eventually be able to determine the information that is being exchanged between the victim and the web application such as session IDs, usernames, passwords, and other personal information. The practices that should be done for session hijacking should also be done to prevent Man-in-the-Middle attacks. Users should be required to use VPNs and HTTPS protocols should be forced when accessing the web. Man-in-the-Middle attacks are likely to happen and would cause critical data breaches or financial losses to any company. A Man-in-the-Middle could last up to 3 hours or more. For these reasons, session hijacking is considered a risk of high priority. If a Man-in-the-Middle attack is suspected, the cybersecurity teams should be notified and force the servers to terminate all connections. This would require all previous connections to be restarted and use different cookies and session IDs. The teams should also check again if https protocols are being enforced and that VPNs are being utilized.

**Social Engineering:** Social engineering in information security is defined as the act of deceiving a victim to manipulate them and compromise confidential and personal information for fraudulent use. One of the most common forms of social engineering is through phishing emails. As a way of reducing the number of successful social engineering attacks, users should constantly be reminded to look for red flags. Things such as, emails asking for confidential information, receiving calls from a person of an unidentified vendor or organization, and links directing to suspicious websites (Frankie Wallace). A social engineering attack is very likely to happen against the business as attackers are constantly attempting social engineering attacks to a mass number of potential victims. If an attacker were to have a successful attack, substantial amounts of data would be compromised and financial losses are very likely. Therefore, the risk priority for social engineering attacks are high. To help mitigate the risks of social engineering, employees should be required to complete training sessions every several months throughout the year to remind employees of what social engineering is and what are the red flags to look out for. Any information on recently discovered methods of social engineering should also be available for employees to learn. If a social engineering attack has occurred, the employee or the department the employee works in shall notify the cybersecurity team. After careful investigation of the situation, the cybersecurity should notify all departments of the social engineering attempt and provide the details to help prevent future successful social engineering attempts.

# Critical Business Functions

## 3.1 Critical Business Functions

1. **Engineering -** The department of engineering provides functionality to the business needs by creating the necessary web applications, website design, and software applications for other departments to do their jobs effectively and efficiently. They also research, design, and or buy technical equipment for business purposes. The department of engineering is part of the foundation that creates our guest and host user interfaces and assists other parts of the business.
2. **Marketing -** The marketing department of our company focuses on providing advertisements, maintaining international and domestic business relationships, and managing the usage of social media to comunicate with the public about business activities. In addition, the art development and market strategy teams also lie within the marketing department. Airbnb as a company understands the importance of having the marketing department to provide assistance in market strategy and seeking opportunities to bring more guests and hosts to the business.
3. **Financial operations -** Financial Operations is in charge of any of business activities that involves financial planning, financial analysis, accounting measures, and management of the payment systems with the assistance of the department of engineering. Financial operations provide a lot of functionality to the business in regards to financial activities and needs.
4. **Information Technology -** The information department is responsible for governance meaning implementing functional guidelines for computer system units, independent usage of IT systems. The IT department is also responsible for infrastructure meaning the hardware malfunctions that pose a risk to computer systems; and the IT department is also responsible for functionality, this means generating and sustaining viable applications, securing, development, saving and retaining data to all of the main functional departments of our company. (Evans).
5. **Design operations -** The design operations department would be responsible for maintaining different approaches to design content for the application / website; design operations works closely with product managers to understand and produce solutions to determine how to make products better. The design team is responsible for all content shown on a screen; and ensuring that communication between hosts and guests are working properly; this includes the interface, getting the email of confirmation, marketing page, instructions that are provided in the help center. A good example is when a customer purchases a trip in a home, the design operations team sends out an email providing more information on the property along with confirmation. (Phillips, 2022)
6. **Product and Home Operations -** The product and home operations department conducts organizing, planning, and conducting the company's procedures to balance various costs, revenues, to gain the most operating profit possible. They are also responsible for product design, forecasting which is using data to predict the trends in the future. (Operations management 2022).

Critical Business Functions are the responsibilities and tasks that need to be completed in order to consider your business as operational.

| # | Function | Criticality | Maximum Downtime | Role/Team | Required Resources | Brief Process to Complete Function |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | Engineering | High | 6 hrs | Website/ software development, Research and Development | # Employees: 120  Equipment: 100 Workstations, Hardware repair tools, 20 Printers, LANs  Supplies: Paper, System development documents and diagrams  Technology: Website development software, Communications software,  Interdependencies: Information Technology and Design operations, Airbnb platform. | * Create and develop user web applications and websites. * Research and buy or develop software to provide for other departments. * Research and buy or develop technical equipment for business purposes. |
| 2 | Marketing | High | 6 hrs | Advertise, maintain business relations, social media management | # Employees: 145  Equipment: 100 workstations, LANs, 20 printers.  Supplies: Paper  Technology: Microsoft office software, Communications software, Airbnb platform.  Interdependencies: none | * Produce advertisements. * Maintain international and domestic business relations with business partners. * Manage business social media accounts. * Create and develop art to promote business. |
| 3 | Financial Operations | High | 4 hrs | Financial analysis and Accounting | # Employees: 60  Equipment: 40 workstations, 10 printers, 40 telephones, LANs  Supplies: Paper  Technology: Microsoft office software, Communications software,  Interdependencies: Engineering | * Conduct financial analysis and assessments on business activities on a daily basis. * Perform accounting activities for business purposes. * Collaborate with the engineering department in managing payment systems and assess the revenues and total profits of the business. |
| 4 | Information Technology | High | 6 hrs | Oversees all computer systems, hardware/ software, managing data. | # Employees: 20  Equipment: 20 workstations and 5 printers, 20 telephones.  Supplies: External drives.  Technology: Microsoft Office, VoIP communications, guest support ticketing system, malware & virus scanning software, Airbnb platform; server to client communication network. | This function involves the process implementing functional guidelines for computer system units, independent usage of IT systems.  Responsible for hardware malfunctions that pose a risk to computer systems.  The IT department is also responsible for functionality, this means generating and sustaining viable applications, securing, developing, saving and retaining data to all of the main functional departments of our company. |
| 5 | Design Operations | High | 2 hrs | Maintaining the interface for all people using the platform as well as communication, assisting with confirmation email. | # Employees: 50  Equipment: 50 workstations and 50 telephones.  Supplies: External Hard Drives, papers, pens.  Technology: Airbnb platform, Microsoft office, VoIP communications, Host support ticketing system, Adobe Suite. | Maintaining different approaches to design content for the application / website; design operations works closely with product managers to understand and produce solutions to determine how to make products better.  The design team is responsible for all content shown on a screen; and ensuring that communication between hosts and guests are working properly; this includes the interface, getting the email of confirmation, marketing page, instructions that are provided in the help center. |

| 6 | Product and Home Operations | High | 6 hrs | Analysis of planning and conducting company procedures like maintaining costs and revenue. | # Employees: 50  Equipment: 50 workstations, 10 printers, 10 telephones.  Supplies: External drives, papers, pens.  Technology: Airbnb platform , server to client communication network, data analysis software.  Interdependencies: none | This function involves The product and home operations department conducts organizing, planning, and conducting the company's procedures to balance various costs, revenues, to gain the most operating profit possible.  Responsible for product design, forecasting which is using data to predict the trends in the future. |
| --- | --- | --- | --- | --- | --- | --- |

## 3.2 Recovery Goals and Requirements

**RECOVERY POINT OBJECTIVE (RPO)**

**Engineering** is a vital function that can equate to 6 hours of downtime. The best way for

The engineering department to recover as quickly as possible is to create backups of all necessary documents, information, and files used for web development, software development, and equipment diagrams. All backups should be stored securely on a cloud platform and backups should be conducted daily or at the minimum 4 times a week. Creating standard system recovery points is also a valid option as using recovery points would allow for the systems to be returned to an operable state it was in the past (Fielding, J. 2021). The system recoveries should begin as soon as a threat has been identified and all affected employees shall be notified as soon as possible.

**Marketing** is a function in the business that can equate to 6 hours of downtime. The reason being that the marketing department is one of the main driving forces in advertisements, marketing strategies, and creating conceptual art to promote business. All of the vital data that is needed for this function to run shall be backed up on a daily basis or at the minimum 4 times a week. All backups should be managed and stored securely on a designated cloud platform. When a threat is detected, the IT cybersecurity team should begin analyzing the event and complete the recovery of all affected systems within the 6 hour time frame. The system recoveries should begin as soon as a threat has been identified and all affected employees shall be notified as soon as possible.

**Financial Operations** is a function within the business that can equate up to 4 hours of downtime. This function involves the activities of conducting business financial assessments, accounting tasks, and managing the payment systems that include personal information and credit card numbers. Therefore, it is very crucial for this function to be recovered in the shortest time possible. All of the vital data that is needed for this function to run shall be backed up on a daily basis or at the minimum 4 times a week. When a threat is detected, the IT cybersecurity team should begin analyzing the event and complete the recovery of all affected systems within the 4 hour time frame. An analysis would also be done to determine the financial losses that occurred because of the downtime. All affected employees, guests, and hosts shall be notified as soon as possible.

**Information Technology:** The maximum downtime is the amount of time a business can endure with the lack of this business function. Airbnb is mainly dependent on their websites being able to deliver rental homes to guests and customers to hosts classifying this function as a critically high area of the company. The maximum downtime will be at least 6 hours. This will enable the IT analysts to be able to scan for viruses, and make sure the whole network is safe and protected. The IT department will backup all critical data using USBs and external hard drives; as well as making sure replicas of programs are available for reinstallation (IT disaster recovery plan 2021). When documenting the issues and ticketing they will be logged onto a special binder with paper and pen if this potential risk were to occur.

**Design Operations:** The maximum downtime for the design operations business function can endure about 2 hours; The reasoning behind this is the fact that design operations manages the interface of the system meaning this is the first page that anyone logging into the airbnb website will interact with; also the design operations department deals with the help instructions page, the communication between guests and hosts, and sending email confirmations after a guest has rented a home (Phillips 2022). This function of the company must be restored immediately therefore in the backend, systems will be scanned, fixed and restored in 2 hours or less.

**Product and Home Operations:** The maximum downtime for the product and home operations business function can endure about 6 hours; The reasoning why product and home operations can endure about 6 hours of downtime because they handle organizing and planning the company's procedures and the trends between the data and how it can affect costs and revenue (Operations management 2022). When given 6 hours for maximum downtime for recording costs and revenue and plans, a binder with paper and tracking templates will be available to continue while the product and home operations are being restored.

BUSINESS RECOVERY REQUIREMENTS

If a crisis regarding a security threat were to occur, each and every department of the business will follow these procedures as following the recovery sequence; The information technology business function has maximum downtime of 6 hours and must be restored first so that any other business function that is at risk will be handled swiftly. The engineering function has a maximum downtime of 6 hours so that IT can help restore the systems next considering that they handle the access to the application / website. The design operations would be the next with knowing their maximum downtime of 6 hours but one of most important functions that must be restored considering that this function handles the interface that is first shown by anyone using the Airbnb site, communication between hosts and guests, and sending confirmation emails to guests who have purchased a rental. The following function that must be restored is the financial operations function; allowing 6 hours of downtime for IT to do the restoration of the systems; The next function that must be restored is product and home operations because the downtime is 6 hours meaning that data can be recorded with templates while IT is restoring the department; the last most important function that will be restored is the marketing team; data will be backed up from all departments onto the cloud server, then will be transferred into a external hardrive for later access.

TECHNICAL RECOVERY REQUIREMENTS

The IT infrastructure components that must be in place supporting the recovery of restoring critical business functions would be needed in general and just in case the company is notified of a cyberthreat; the business functions that will be focused on primarily is IT department, engineering, design operations, product and home applications, financial operations, and marketing. The components must include the cloud based server where data is stored, critical applications and back up files of those applications, an external hard drive for each of the companies business functions. LANS supplies will be provided for network connections, software components like anti malware/virus removing software as well as malware/virus scanning software, Microsoft office, Adobe Suite, financial software, development/engineering, communications software and hardware repair equipment will be components needed for these business functions. A workstation, a phone, paper templates for manually handwritten logs for data if the business function is at risk, it would be necessary in the event that internet connection is down and email communication is not possible; communication in a timely manner is something that will be critical in a cyber emergency.

# PLAN ACTIVATION and communication PROCEDURES

## Plan Activation during Normal Business Hours

If a crisis regarding a security threat were to occur during work hours the company will react by having each and every department of the business that has a security breach will follow these procedures; a security threat as taken place, IT will be called; then next step will be to warn all employees in the department of a security threat; employees will upload remaining data onto the cloud based server; management will collect all data from the cloud with the file containing departments data and transfer it onto an external hard drive; all of the affected departments will stop it’s activities then IT will eliminate the suspicious activities. The system will then be restored, and monitored closely.

## Plan Activation outside Normal Business Hours

If the crisis happens outside of business hours the company will react by having management must notify employees through a message to everyone in the department notifying them of a possible security threat that could affect personal data. The message will instruct employees on calling credit card companies, banks notifying of possible breach of sensitive data so that personals can be monitored closely. An IT personnel will login to the cloud and look for the file’s who’s department is at risk and back up the remaining data onto an external hard-drive from home; and the systems activities will be stopped, the suspicious activity will be eliminated, then the system will be reinstated, and closely monitored. (How to inform your staff of a data breach, n.d)

## Internal communication procedures

Best methods for distributing communications to staff.

| Employee Communication Methods | |
| --- | --- |
| 1 | Phone |
| 2 | Face-to-Face |
| 3 | E-mail |

# Resumption Strategies

(Area that needs to be restored first/ which department functions need of concern primarily)

* Resume business functions in priority sequence based upon the classification and criticality of the function.
* Purchase and acquire equipment, supplies and travel arrangements needed for the resumption effort.
* Temporarily eliminate non-critical functions, as necessary, to support the resumption efforts.
* As applicable, utilize personnel from other sites to support the resumption efforts.

## Business Function Resumption (see notes)

| # | Function | Required Resources | Resumption Procedures |
| --- | --- | --- | --- |
| 1 | Engineering | # Employees: 120  Equipment: 100 Workstations, Hardware repair tools, 20 Printers, LANs  Supplies: Paper, System development documents and diagrams  Technology: Website development software, Communications software,  Interdependencies: Information Technology and Design operations | Resumption would occur at either the main site or the alternate site depending on the circumstances. Backups of necessary data and files will be used as needed. System recovery points will also be utilized as needed. All workstations and devices that are affected by an event will be examined to relieve some of the damages and inspect for vulnerabilities. |
| 2 | Marketing | # Employees: 145  Equipment: 115 workstations, LANs, 20 printers.  Supplies: Paper  Technology: Microsoft office, Communications software,  Interdependencies: none | Resumption would occur at either the main site or the alternate site depending on the circumstances. Backups of necessary data and files will be used as needed. System recovery points will also be utilized as needed. All workstations and devices that are affected by an event will be examined to relieve some of the damages and inspect for vulnerabilities. In addition, employee relocation would also be considered if needed. |
| 3 | Financial Operations | # Employees: 60  Equipment: 40 workstations, 10 printers, 40 telephones, LANs  Supplies: Paper  Technology: Microsoft office software, Communications software,  Interdependencies: Engineering | Resumption would occur at either the main site or the alternate site depending on the circumstances. Backups of necessary data and files will be used as needed. System recovery points will also be utilized as needed. All workstations and devices that are affected by an event will be examined to relieve some of the damages and inspect for vulnerabilities. In addition, transactional data that is available as backups will be used as needed to recover transactional data from the payment systems. Employee relocation would also be considered if needed. |
| 4 | Information Technology | # Employees: 20  Equipment: 20 workstations and 5 printers, 20 telephones.  Supplies: External drives.  Technology: Microsoft Office, VoIP communications, guest support ticketing system, malware & virus scanning software, Airbnb platform; server to client communication network. | Resumption would occur at either the main site or the alternate site depending on the circumstances. Templates that are prepared for the ticketing system and other IT data will be logged back in digitally once restored, Backed up data will be retransmitted into the cloud based server, as well as all critical applications be reinstalled as well as restoring the systems and will be monitored closely. |
| 5 | Design Operations | # Employees: 50  Equipment: 50 workstations and 50 telephones.  Supplies: External Hard Drives, papers, pens.  Technology: Airbnb platform, Microsoft office, VoIP communications, Host support ticketing system, Adobe Suite. | Resumption would occur at either the main site or the alternate site depending on the circumstances. Workstations and external hard drives, paper templates for logging design operations will be provided and reentered when operations resume this will help reduce downtime. Employees would relocate as needed. |
| 6 | Product and Home Operations | # Employees: 50  Equipment: 50 workstations, 10 printers, 10 telephones.  Supplies: External drives, papers, pens.  Technology: Airbnb platform , server to client communication network, data analysis software.  Interdependencies: none | Resumption would occur at either the main site or the alternate site depending on the circumstances. external hard drives, template for handwritten data logs shall be available at both the main site and alternate site beforehand to help reduce downtime. Employees would relocate as needed. |

# Employee Contact List

| Employee Name | Title / Responsibility (Inc. Succession) | Home / Cell Number | Personal Email Address |
| --- | --- | --- | --- |
| Brian Chesky | CEO | 415-310-3223 | brian.chesky@airbnb.com |
| Michael Curtis | VP of Engineering | 415-323-3445 | michael.curtis@airbnb.com |
| Jason Bosinoff | Director of Engineering | 415-350-9870 | jason.bosinoff@airbnb.com |
| Maxim Charkov | Director of Engineering | 415-760-5445 | maxim.charkov@airbnb.com |
| Paul Youn | Director of Security | 415-310-7667 | paul.youn@airbnb.com |
| Kevin Rice | Engineering Manager | 415-650-8778 | kevin.rice@airbnb.com |
| Daniel Loreto | Engineering Manager | 415-850-6776 | daniel.loreto@airbnb.com |
| Ari Stemberg | Engineering Manager | 415-760-8778 | ari.stemberg@airbnb.com |
| Mike Jennings | IT Director | 415-666-8877 | mike.jennings@airbnb.com |
| Alex Shleifer | VP of Design | 415-877-9955 | alex.shleifer@airbnb.com |
| Judd Antin | Director of Research | 415-987-6543 | judd.antin@airbnb.com |
| Adrian Cleave | Director of Design Ops | 415-910-7630 | adrian.cleave@airbnb.com |
| Fabio Resende | Design Manager, Trips | 415-920-7630 | fabio.resende@airbnb.com |
| Amber Cartwrite | Design Manager for Guests | 415-930-7640 | amber.cartwright@airbnb.com |
| Marissa Phillips | Product Lead Content | 415-530-7650 | marissa.phillips@airbnb.com |
| Jenny Arden | Design Manager | 415-705-3110 | jenny.arden@airbnb.com |
| Vlad Loktev | VP of Product & Home Operations | 415-805-3220 | anthony.carinhas@airbnb.com |
| Dan Hill | Director of Guest Experiences | 415-987-6009 | dan.hill@airbnb.com |
| Donna Boyer | Director of Product Host & Home | 415-908-9898 | donna.boyer@airbnb.com |
| Laurence Tosi | Chief Accounting Officer & Controller | 415-760-5005 | laurence.tosi@airbnb.com |
| David Bernstein | Chief Accounting and Controller | 415-920-3100 | david.bernstein@airbnb.com |
| Krishna Rao | Co-Head of Corporate Development | 415-710-3230 | krishna.rao@airbnb.com |
| Sara Adler | Co-Head of Corporate Development | 415-760-8580 | sara.adler@airbnb.com |
| Aisling Hassell | Head of Global Customer Experience | 415-780-8530 | aisling.hassell@airbnb.com |
| Jonathan Mildenhall | CMO | 415-960-7500 | jonathan.mildenhall@airbnb.com |
| Alexandra Dimiziani | Director of Global Brand Marketing | 415-660-8601 | alexandra.dimiziani@airbnb.com |
| Ayni Raimondi | Director of Global Brand Marketing | 415-770-0701 | ayni.raimondi@airbnb.com |
| Nancy King | Global Consumer Insights | 415-889-0903 | nancy.king@airbnb.com |
| James Goode | Director, Art Department | 415-359-0782 | james.goode@airbnb.com |
| Matt Ghering | Director, Strategies & Operations | 415-429-0332 | matt.ghering@airbnb.com |
| Sarah Goodnow | Global Lead of Airbnb Open | 415-488-0762 | sarah.goodnow@airbnb.com |

# Vendor Contact List

| Vendor | Resource/Service | Contact Information |
| --- | --- | --- |
| Microsoft | Software/Operating System provider | Nearest location: 555 California, Suite 200  San Francisco, CA, USA  94104  Phone number: +1 (800)-642-7676  Live chat URL: [Contact Us - Microsoft Support](https://support.microsoft.com/contactus) |
| Google Inc. | Advertisement services | Nearest location: 345 Spear Street  San Francisco, CA 94105  United States  Phone number: +1 (415)-736-0000 |
| Cisco | Network hardware provider | Nearest location: 1 Bush St #1300,  San Francisco, CA 94104  Phone number: +1 (800)-553-6387 |
| Dell | Workstation/ Server hardware provider | Nearest location: 301 Howard St Suite 1700, San Francisco, CA 94105  Phone: +1 (800)-624-9897 |
| Adobe | Software provider | Nearest location: 345 Park Ave,  San Jose, CA 95110  Phone number: +1 (800)-833-6687 |
| RingCentral | VoIP provider | Nearest location: 20 Davis Dr,  Belmont, CA 94002  Phone number: +1 (888)-528-7464 |

# Family Emergency Plan

(figure out what steps need to be taken when instructing employees on how to handle a cyber attack exposed information, like calling credit card company, cancel cards…. etc)

In the case of a security breach, the family members of our employees should be informed of the incident by the employee related to the family upon learning the news. Family members of company employees should be advised to change contact information if possible for reasons being that emergency contact information could potentially be compromised. Family members should also be on high alert for suspicious activities such as phishing emails, scam calls, social engineering phone calls, or suspicious activity around the home addresses included in the emergency contact information.

In the case of a hazardous emergency, family members will be notified via automated text message and email. Family members can contact their relative employee to know if their relative is ok. Family members may also contact the following below:

* Airbnb HQ HR office

Phone: 415-987-1735

email: [AirbnbHRSanFran@gmail.com](mailto:AirbnbHRSanFran@gmail.com)

* Emergency Response Team

Phone: 415-312-8348

email: [AirbnbERTSanFran@gmail.com](mailto:AirbnbERTSanFran@gmail.com)

Family members are more than welcome to provide any type of support to our employees in a security breach or emergencies.

# Insurance Considerations

The type of insurance coverage that is available if there is a cybersecurity risk can be provided by a few companies like Nationwide, AXA, Liberty Mutual, and a few others; it is needed in order to provide protection by alerting customers when there’s been a security breach, reinstating individual identities affected, and it can restore damaged computer systems. Many companies prefer AXA, and it can be accessed in the business through their website (Grones, 2019).

# glossary

**Business continuity plan (BCP)** is a document that outlines how a business will continue operating during an unplanned disruption in service.

**Security Risk Assessment** identifies, assesses, and implements key security controls in applications. It also focuses on preventing application security defects and vulnerabilities.

**Vulnerability scanner:** Vulnerability scanners are attack tools that search for potential vulnerabilities in networks, systems, and web applications.

**Exploit software**: Exploit software is an attack tool that is used to target known specific vulnerabilities in systems.

**Password crackers**: Password crackers are attack tools that are used to input passwords and gain unauthorized access to any systems, networks, or accounts.

**Keystroke loggers**: A keystroke logger is malicious software that is considered as spyware. Once a keystroke logger has infected a victim, the keystroke logger begins to record any input from the victim’s keyboard or mouse-clicks and send that info back to the attacker.

**War dialers:** A war dialer is an attack tool that is used to dial a large volume of telephone numbers.

**Distributed Denial of Service (DDoS)** **attack**: is a different type of a DoS attack that entails extremely large numbers of attacking computers to overwhelm the target with fake traffic.

**Backdoors**: A backdoor invokes any procedure by which authorized and unauthorized users are able to get around usual security measures and gain high level user access (aka root access) on a computer system, network, or software application.

**Data modification:** Data modification: attacks where a hacker decides to not take the data, but instead make subtle,secretive changes to the data for some type of gain, can be just as immobilizing for companies compared to theft. There are various ways to mitigate the risk of a data modification attack.

**Hoaxes**: This is often a chain message telling users to forward the mail to all their contacts. The aim is simply to cause alarm and confusion among users

**Cookies**: The reason for the cookie is to help the website keep tabs of your visits and activity. Most internet retailers utilize cookies to keep tabs of the items in a user’s shopping cart as they explore the site.; without the use of cookies, our shopping carts would reset to zero each time you clicked a different link on the site.

**Unacceptable Web Browsing:** Visiting internet sites that contain obscene, hateful, pornographic or otherwise illegal material or utilizing the computer to perpetrate any form of fraud, or software, film or music piracy.

**Spyware**: Spyware is a certain type of malicious software created to go into the user's computer device, collect data about the user, and send it to a third-party without your consent.

**Worms**: A computer worm is a certain classification of malware that can spread copies of itself from computer to computer.

**Virus:** A computer virus is a malicious piece of computer code designed to spread from device to device. A subset of malware, these self-copying threats are usually designed to damage a device or steal data.

**Trojan Horses:** A Trojan horse, or Trojan, is a classification of malicious code or software that looks authorized but can take control of your computer.

**Rootkits**: A rootkit is a malicious software computer program created to supply continuous privileged access to a computer while actively disguising its presence.

**Brute force password attack:** A brute force password attack is an attempt to crack a password by inputting all possible combinations of characters.

**Dictionary password attack:** A dictionary password attack is very similar to a brute force password attack. It is an attack that attempts to crack a password.

**Session hijacking:** A session hijacking attack occurs when an attacker takes control of a user’s internet session by obtaining info of the user’s session ID with a web application.

**Man-in-the-Middle attacks:** A Man-in-the-Middle attack occurs when an attacker intercepts a connection between a victim and a web application.

**Social Engineering:** Social engineering in information security is defined as the act of deceiving a victim to manipulate them and compromise confidential and personal information for fraudulent use.

**Engineering business function -** The department of engineering provides functionality to the business needs by creating the necessary web applications, website design, and software applications for other departments to do their jobs effectively and efficiently.

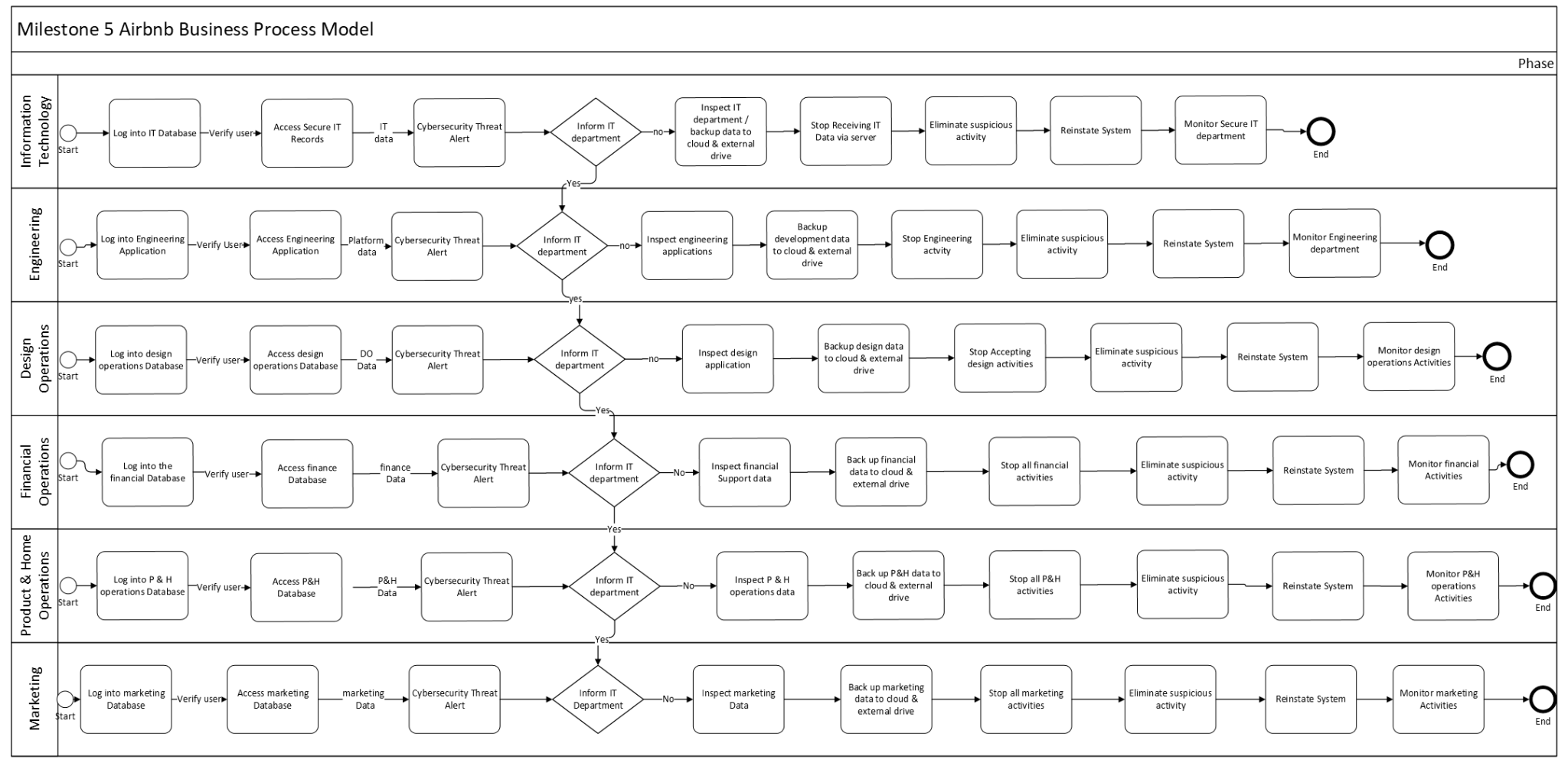
**Marketing business function -** The marketing department of our company focuses on providing advertisements, maintaining international and domestic business relationships, and managing the usage of social media to comunicate with the public about business activities.

**Financial operations business function -** Financial Operations is in charge of any of business activities that involves financial planning, financial analysis, accounting measures, and management of the payment systems with the assistance of the department of engineering.

**Information Technology business function -** The information department is responsible for governance meaning implementing functional guidelines for computer system units, independent usage of IT systems. The IT department is also responsible for infrastructure meaning the hardware malfunctions that pose a risk to computer systems; and the IT department is also responsible for functionality, this means generating and sustaining viable applications, securing, development, saving and retaining data to all of the main functional departments of our company.

**Design operations business function -** The design operations department would be responsible for maintaining different approaches to design content for the application / website; design operations works closely with product managers to understand and produce solutions to determine how to make products better; as well as in charge of all content shown on the side.

**Product and Home Operations business function** - The product and home operations department conducts organizing, planning, and conducting the company's procedures to balance various costs, revenues, to gain the most operating profit possible. They are also responsible for product design, forecasting which is using data to predict the trends in the future.



The business process model for restorations of the major business functions explains how management and employees will react and how the cybersecurity risk will be solved.

# references

Frankie Wallace. *Airbnb Cybersecurity Concerns*. 7 March 2022. *US Cybersecurity*, cybersecurity magazine, https://www.uscybersecurity.net/airbnb/.

Kim, D., & Solomon, M. G. (2016). Fundamentals of information systems security. Jones & Bartlett Publishers.

Kingatua, Amos. “6 HTTP MITM Attack Tools for Security Researchers.” *Geekflare*, 7 July 2021, https://geekflare.com/mitm-attack-tools/. Accessed 9 March 2022.

“Our Hazards | Department of Emergency Management.” *San Francisco Department of Emergency Management*, https://sfdem.org/our-hazards. Accessed 9 March 2022.

Poremba, Sue. “Session Hijacking Attacks: How to Prevent Them.” *Verizon*, https://www.verizon.com/business/resources/articles/s/how-to-prevent-session-hijacking-attacks/. Accessed 10 March 2022.

“WAR-DIALING :: Chapter 11: Probing a Target :: Part 3: Breaking and Entering Computers :: Steal this computer book 3 :: Misc.” *eTutorials.org*, http://etutorials.org/Misc/computer+book/Part+3+Breaking+and+Entering+Computers/Chapter+11+Probing+a+Target/WAR-DIALING/. Accessed 10 March 2022.

Helmer, B. J. (2020, September 18). *The New Go Bag: What You Need in Your*

*Emergency Escape Kit*. AARP. <https://www.aarp.org/home-family/friends-family/info-2020/emergency-go-bag.html?cmp=KNC-DSO-COR-DisasterPreparedness-15204-Bing-EmergencyGoBag-Phrase-NonBrand&&msclkid=8b26aefbf9661f6f1f14ccd56390581b&utm_source=bing&utm_medium=cpc&utm_campaign=Core-DisasterPreparedness-NonBrand-Phrase&utm_term=emergency%20preparedness%20kit&utm_content=Emergency%20Go%20Bag&gclid=8b26aefbf9661f6f1f14ccd56390581b&gclsrc=3p.ds>

Martens, B. (2021b, November 17). What Is a Backdoor & How to Prevent Backdoor Attacks (2022). SafetyDetectives. <https://www.safetydetectives.com/blog/what-is-a-backdoor-and-how-to-protect-against-it/>

CBS San Francisco. (2021a, October 25). UPDATE: Atmospheric River Drenches Northern California With Historic Rainfall. ..Cbslocal. <https://sanfrancisco.cbslocal.com/2021/10/24/atmospheric-river-flooding-san-francisco-mudslides-santa-cruz-mountains-russian-river/>

Osborne, C. (2020, February 18). *16 DDoS attacks take place every 60 seconds, rates reach 622 Gbps*. ZDNet. <https://www.zdnet.com/article/16-ddos-attacks-take-place-every-60-seconds-rates-reach-622-gbps/#:%7E:text=With%20over%2023%2C000%20recorded%20attacks%20per%20day%2C%20customer-facing,which%208.4%20million%20were%20recorded%20in%202019%20alone>

Kiguolis, L. (2021, June 3). *What are backdoors and how to remove them*. 2 Spyware. <https://www.2-spyware.com/backdoors-removal>

Londo, G. (2018, December 5). 10 Ways to Prevent Fire in the Workplace. Frontier Fire Protection. <https://www.frontierfireprotection.com/10-ways-prevent-fire/>

Osborne, C. (2020, February 18). *16 DDoS attacks take place every 60 seconds, rates reach 622 Gbps*. ZDNet. [https://www.zdnet.com/article/16-ddos-attacks-take-place-every-60-seconds-rates-reach-622-gbps/#:%7E:text=With%20over%2023%2C000%20recorded%20attacks%20per%20day%2C%20customer-facing,which%208.4%20million%20were%20recorded%20in%202019%20alon](https://www.zdnet.com/article/16-ddos-attacks-take-place-every-60-seconds-rates-reach-622-gbps/#:%7E:text=With%20over%2023%2C000%20recorded%20attacks%20per%20day%2C%20customer-facing,which%208.4%20million%20were%20recorded%20in%202019%20alone)

Cucu, P. (2022, February 22). How to DDoS Like an Ethical Hacker. Heimdal Security Blog. <https://heimdalsecurity.com/blog/how-to-ddos/>

Townsened, C. (2019, December 10). Data Manipulation Attacks And How To Counter Them. United States Cybersecurity Magazine. <https://www.uscybersecurity.net/data-manipulation-attacks/>

Reinstalling Your Compromised Computer | Information Security Office. (2022). UC Berkeley. <https://security.berkeley.edu/education-awareness/reinstalling-your-compromised-computer>

J. (2021, July 27). 5 Security Issues with Cookies That You Should Know. Quadrant Information Security. <https://quadrantsec.com/security-issues-cookies/>

Strickland, D. (2021, December 2). 5 Ways to Enforce Your Acceptable Use Policy (AUP). CurrentWare. <https://www.currentware.com/blog/5-ways-to-enforce-your-acceptable-use-policy/>

Gaskin, J. E. (2005, March 28). 10 ways to stop spyware. Network World. <https://www.networkworld.com/article/2319505/10-ways-to-stop-spyware.html>

How to remove spyware from your computer. (n.d.). Www.bullguard.com. https://www.bullguard.com/blog/2018/01/how-to-remove-spyware-from-your-computer

‌

Kaspersky. (2021, December 1). Avoiding a Trojan Virus: Keeping the Gates Closed. Usa.Kaspersky.Com. <https://usa.kaspersky.com/resource-center/preemptive-safety/avoiding-a-trojan-virus>

Kaspersky. (2021b, December 1). Avoiding a Trojan Virus: Keeping the Gates Closed. Usa.Kaspersky.Com. <https://usa.kaspersky.com/resource-center/preemptive-safety/avoiding-a-trojan-virus>

M. (2021b, September 7). Understanding Trojan Viruses and How to Get Rid of Them. McAfee Blog. <https://www.mcafee.com/blogs/internet-security/understanding-trojan-viruses-and-how-to-get-rid-of-them/>

Fielding, J. (2021, November 14). Backing up data – whose job is it anyway? TechRadar. Retrieved April 2, 2022, from <https://www.techradar.com/features/backing-up-data-whose-job-is-it-anyway>

Airbnb executive team | comparably. (n.d.). Retrieved April 20, 2022, from <https://www.comparably.com/companies/airbnb/executive-team>

What is Cyber Insurance? Nationwide. (n.d.). Retrieved April 19, 2022, from <https://www.nationwide.com/lc/resources/small-business/articles/what-is-cyber-insurance#:~:text=Cyber%20insurance%20generally%20covers%20your,license%20numbers%20and%20health%20records>

Grones, G. (2019, December 20). Top 10 cyber insurance companies in the US. Insurance Business America. Retrieved April 19, 2022, from <https://www.insurancebusinessmag.com/us/news/cyber/top-10-cyber-insurance-companies-in-the-us-195463.aspx>

&nbsp;, L. B., &amp; Brooke, L. (2019, December 10). Data manipulation attacks and how to counter them. United States Cybersecurity Magazine. Retrieved May 1, 2022, from <https://www.uscybersecurity.net/data-manipulation-attacks/>

Evans, K. (n.d.). The IT department: What they do vs. what everyone thinks they do. Retrieved May 4, 2022, from <https://www.jobs.net/article/cb-214-talent-network-it-the-it-department-what-they-do-vs-what-everyone-thinks-they-do/#:~:text=The%20IT%20department%20oversees%20the,that%20the%20network%20runs%20smoothly>

Phillips, M. (2022). Content strategy at airbnb. Airbnb.Design. Retrieved May 4, 2022, from <https://airbnb.design/content-strategy-at-airbnb/>

Operations management. Corporate Finance Institute. (2022, April 23). Retrieved May 4, 2022, from <https://corporatefinanceinstitute.com/resources/knowledge/strategy/operations-management/>

It disaster recovery plan. IT Disaster Recovery Plan | Ready.gov. (2021, February 21). Retrieved May 5, 2022, from <https://www.ready.gov/it-disaster-recovery-plan>

# Appendix

**Risk assessment survey**

Survey link: <https://calstatela.co1.qualtrics.com/jfe/form/SV_5sRBt8irHkcKeR8>

Airbnb cybersecurity risk assessment survey



Let's help to keep our systems and information secure and safe.

Thank you for taking some time to look at and complete this risk assessment survey. The purpose of this risk assessment survey is to assess, prioritize, and rank the many physical and cyber threats that our business must respond to at any time. The security of our customers' and employees' personal information is just as important as the security of our IT infrastructure. We do appreciate you taking the risk assessment survey and answering honestly to better assess the threats.

**How often are users filing complaints about not being able to log into their accounts.**

* Very often
* somewhat often
* not often
* not at all

#### How many characters are you using in your passwords?

* 2-4
* 5-8
* 8 or more

**Are special characters required to be used in the passwords?**

* yes
* no

#### How often are users filing complaints about bugs when using airbnb's services?

* Very often
* somewhat often
* not often
* not at all

#### How often do customers complain about not being to access Airbnb on the web or using the application

* Very often
* somewhat often
* not often
* not at all

#### How often do hosts or customers complain about the price of a listing increasing or decreasing unexpectedly?

* Very often
* somewhat often
* not often
* not at all

**Do customers complain about unusual activity on their Airbnb account?**

* Very often
* somewhat often
* not often
* not at all

#### Do hosts or customers complain about pop-ups that redirect them to another site?

* Very often
* somewhat often
* not often
* not at all

**How often are users filing complaints that their usernames and passwords have been compromised?**

* Very often
* somewhat often
* not often
* not at all

#### How often are users filing complaints that an unauthorized transaction has occurred from their Airbnb account?

* Very often
* somewhat often
* not often
* not at all

#### How often are users filing complaints that their sessions on the website or application terminate unexpectedly?

* Very often
* somewhat often
* not often
* not at all

#### What is the limited amount of attempts that a user has to provide the correct username and password when logging in their account?

* 3
* 4
* 5
* there is no limit

#### How often are customers filing complaints about receiving fake emails from people pretending to be representatives of Airbnb?

* Very often
* sometimes
* not often
* not at all

#### Have you ever received an email containing a booking from Airbnb but after clicking the link your computer shuts down?

* Very often
* sometimes
* not often
* not at all

#### Is there a system in place where hosts and guests are informed on the dangers of connecting to any network?

* Yes
* Maybe
* No

#### How often have you opened an email stating that they are from Airbnb but when you click on the link it redirects you to another site?

* Very often
* sometimes
* not often
* not at all