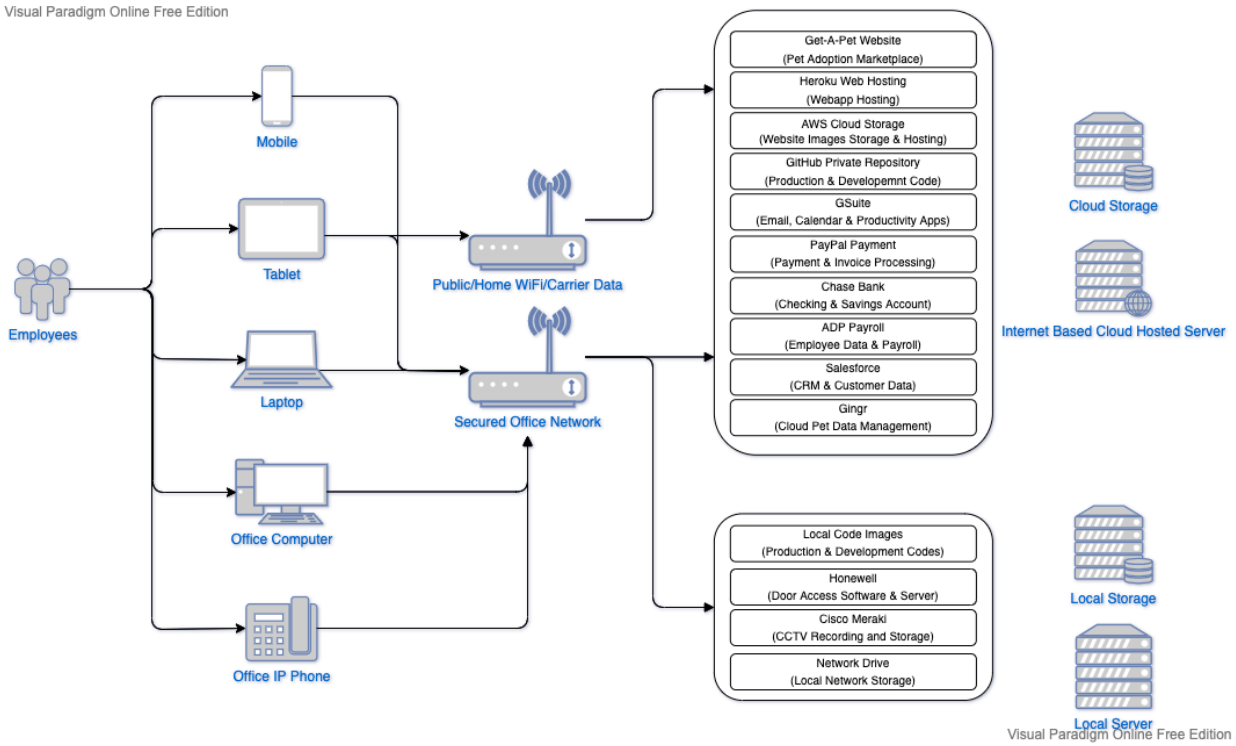
Threat Asset Matrix

Get-A-Pet: It is an organization that helps people adopt pets from their online website. Following is the company's network diagram:



R = Risk C = Consequence P = Probability
Risk is Probability (P) of Threat times Consequence (C) of Threat

	Confidentiality	Integrity	Availability	Theft/Fraud
Employee Mobile (Email, Chats, etc.)	P=1 C=2 R=2 People keep their phones close by, and usually, it requires a password to unlock. Company Email and Chats might contain confidential information.	P=1 C=2 R=2 As it might contain confidential information, someone might get access to credentials or keys which can enable them to make modifications to the system.	P=1 C=2 R=2 Similar to Integrity, someone with access to confidential data might be able to limit or stop complete access to the product.	P=1 C=2 R=2 Might result in downtime as discussed in availability which can lead to financial loss as well.
Employee Tablet (Website Demo, Photos, PDFs, etc.)	P=1 C=1 R=1 Mostly password protected and physically close. Only contains a Demo of the product, information on the device is already available to the public.	P=1 C=1 R=1 Has no access to the server, codes, confidential information, etc. Cannot harm the integrity of the system.	P=1 C=1 R=1 Has no access to the server, codes, confidential information, etc. Cannot harm the availability of the system.	P=1 C=1 R=1 Has no access to the server, codes, confidential information, etc. Won't affect the company so much.
Employee Laptop (Development Code, Software, etc.)	P=2 C=3 R=6 Asset to competitors as it contains very confidential information, source code and software.	P=2 C=3 R=6 Anyone with access to this can easily make modifications to the system, hampering the system's integrity.	P=2 C=3 R=6 Has complete access to limit or stop access to web servers making the website unavailable to users.	P=2 C=3 R=6 This can result in source code and other confidential data being stolen.
Employee Office Computer (Development Code, Software, Local Server Files, etc.)	P=2 C=3 R=6 Although many steps are taken to keep the office computer very secure, it is an asset to competitors and hackers. Contains very confidential data and has access to data on the local onsite server.	P=2 C=3 R=6 Anyone with access to this can easily make modifications to the system, hampering the system's integrity and make further modification to the local onsite server.	P=2 C=3 R=6 Has complete access to limit or completely stop access to the web and local servers making the website unavailable to users.	P=2 C=3 R=6 This can result in source code and other confidential data being stolen.

Employee Office IP Phone (Office Call Logs and Contact List)	P=1 C=2 R=2 The chances are very low, but it contains contact information and logs which might be useful for competitors or hackers to sell data.	P=1 C=1 R=1 Cannot harm the integrity of the system in any way.	P=1 C=1 R=1 Cannot harm the availability of the system in any way	P=1 C=2 R=2 Contact information can be stolen, which can result in fraud with customers or vendors.
Get-A-Pet Website (Photos, Contact Information, Pet Data, Reviews, etc.)	P=2 C=3 R=6 Everything on website is for end users to access but part of it is after authentication. A loophole might leverage attackers to access private user data and steal information.	P=1 C=3 R=3 Although website is well administered and multiple steps are taken to filter bad user data/malicious attempts, if a hacker can do something like XSS attack successfully, they can dampen the integrity.	P=2 C=3 R=6 The website is an easy target to attack and prevent others from accessing. Something like a DDOS attack will heavily affect traffic and reduce the availability of our product to users.	P=3 C=3 R=9 Websites are very easy to copy/replicate. A phishing site of our website can steal user payment details and result in financial fraud.
Heroku Web Hosting (Release Code, API Keys as Secret)	P=2 C=3 R=6 Only few employees have access to hosting platform and are mostly covered with security methods like 2FA. Although gaining access to it is hard, if someone does then they steal all the code, data and API keys.	P=2 C=3 R=6 Hackers can try to gain access to this, and if they are successful, the integrity can be severely affected.	P2= C=3 R=6 Can completely take down the website.	P=2 C=3 R=6 Access to hosting platform can result in stealing of all the codes, data and API keys – in short, the entire product can be stolen.
AWS Cloud Storage (Website Media and data)	P=2 C=2 R=4 Hard to get access to due to multiple layers of security. Unauthorized access to lead to media being stolen, including user profile pictures.	P=2 C=3 R=6 With unauthorized access, media can be modified which can result in wrong data being displayed on the website.	P=2 C=3 R=6 Can delete/modify photos and other media. As an adoption website, photos and media play a major role. This can hamper the availability.	P=1 C=2 R=2 It is unlikely that photo and media will be stolen and cause any major harm.

GitHub Private Repository (ALL development codes, API Keys as Secret)	P=3 C=3 R=9 All developers have access to this, leaks can happen from any end device of developers. Entire Code Repo (Past versions, present version, future features, and versions) along with API Keys can be stolen.	P=1 C=2 R=2 Any changes made to code can easily be noticed and tracked. Usually more than one developer approval is required to modify code in critical branches. Any changed code can easily be reverted as well.	P=2 C=2 R=4 Although any changed code can be reverted and fixed, it may delay the availability of new versions and features to the product.	P=3 C=3 R=9 Will severely affect the company as the repositories hold one of the most valuable assets – product code.
GSuite (Email, Calendars, Google Cloud Documents and Files)	P=2 C=3 R=6 Even with security in place, accounts do get hacked. Confidential documents and data in emails valuable to others.	P=2 C=3 R=6 There is possibility that data leaked can result in unauthorized access to codebase, and modifications can be made.	P=1 C=2 R=2 Cannot directly harm the availability of the system.	P=1 C=1 R=1 Cannot directly result in theft of product and services being offered.
PayPal Payment (Payment processing data and invoices)	P=2 C=3 R=6 Payments are generally very secure, although a leak can result in confidential buyer and seller data stolen.	P=1 C=3 R=3 Low possibility, but if payment gateway is maliciously modified, it will severely impact the system.	P=2 C=3 R=6 Without payment, users cannot process their orders and thus will limit the product availability.	P=2 C=3 R=6 Can result in direct theft from company.
Chase Bank (Checking and Savings Account)	P=1 C=2 R=2 Limited users have access to this information. All security and guarantees are monitored by bank.	P=1 C=1 R=1 Cannot impact the integrity of the product.	P=1 C=2 R=2 Very less likely, but a hit to company funds can slow things down.	P=1 C=2 R=2 Unlikely, but can result in monetary loss.
ADP Payroll (Employee and Finance Data)	P=1 C=2 R=2 Confidential payroll and tax data can leak which is valuable.	P=1 C=1 R=1 Payroll cannot affect the product integrity directly.	P=1 C=2 R=2 A payroll delay might result in employee loss, but less likely.	P=1 C=1 R=1 Can result in financial data theft, which can result in company fraud.

Salesforce (CRM, Customer Data, etc.)	P=2 C=3 R=6 Customer data is very confidential and valuable to competitors.	P=1 C=2 R=2 Customer data play an important role in designing the product, can impact integrity.	P=1 C=1 R=1 Cannot harm the availability of the product.	P=1 C=2 R=2 Can result in theft from customer or customer fraud.
Gingr (Pet Data, Medical Records, Vet Information, etc.)	P=1 C=1 R=1 Pet Data and Medical Records are not that valuable outside organization.	P=1 C=2 R=2 If a hacker can modify this data, it can damage the integrity of website as this is false data.	P=1 C=2 R=2 Accurate data is necessary for the customers. Can affect the availability.	P=1 C=1 R=1 Cannot result in fraud or theft.
Local Code Images (Local Backup Copy of Development Code)	P=3 C=3 R=9 Very confidential and valuable data to the competitors.	P=3 C=1 R=3 As this is backup code, it cannot affect the integrity of the system.	P=3 C=2 R=6 Backups are important in unforeseen cases. Can limit the availability in such cases.	P=2 C=3 R=6 Theft of code is very harmful for the organization and can result in product loss.
Honewell (Local Server for Door Access Processing and Access Logs)	P=1 C=2 R=2 Which employee has access to which area is somewhat confidential data.	P=1 C=2 R=2 Unauthorized access can result in access to the server area, where someone can play around with the systems.	P=1 C=1 R=1 Will not directly impact the availability of the product to users.	P=2 C=2 R=4 Can result in theft of company data and equipment.
Cisco Meraki (CCTV Local Recordings and Logs)	P=1 C=1 R=1 Not that useful outside the organization and not that confidential.	P=1 C=1 R=1 Cannot affect the integrity of the product in any way.	P=1 C=1 R=1 Cannot affect the availability of the product in any way.	P=1 C=1 R=1 Cannot result in theft or fraud.
Network Drive (Shared Local Files and Sharing)	P=2 C=3 R=6 Network Drive has confidential information, which can be asset to competitors.	P=1 C=1 R=2 Very unlikely to break the integrity of the product.	P=1 C=1 R=1 This should not affect the availability of the product to the end user.	P=1 C=2 R=2 Can result in document and data theft

Business Asset	Estimated Risk
Local Code Images (Local Backup Copy of Development Code)	Total Risk = 24
Employee Laptop (Development Code, Software, etc.)	Total Risk = 24
Employee Office Computer (Development Code, Software, Local Server Files, etc.)	Total Risk = 24
Get-A-Pet Website (Photos, Contact Information, Pet Data, Reviews, etc.)	Total Risk = 24
Heroku Web Hosting (Release Code, API Keys as Secret)	Total Risk = 24
GitHub Private Repository (ALL development codes, API Keys as Secret)	Total Risk = 24
PayPal Payment (Payment processing data and invoices)	Total Risk = 21
AWS Cloud Storage (Website Media and data)	Total Risk = 18
GSuite (Email, Calendars, Google Cloud Documents and Files)	Total Risk = 15
Salesforce (CRM, Customer Data, etc.)	Total Risk = 11
Network Drive (Shared Local Files and Sharing)	Total Risk = 11
Honewell (Local Server for Door Access Processing and Access Logs)	Total Risk = 9
Employee Mobile (Email, Chats, etc.)	Total Risk = 8
Chase Bank (Checking and Savings Account)	Total Risk = 7
Employee Office IP Phone (Office Call Logs and Contact List)	Total Risk = 6
ADP Payroll (Employee and Finance Data)	Total Risk = 6
Gingr (Pet Data, Medical Records, Vet Information, etc.)	Total Risk = 6
Employee Tablet (Website Demo, Photos, PDFs, etc.)	Total Risk = 4
Cisco Meraki (CCTV Local Recordings and Logs)	Total Risk = 4