Threat Asset Matrix

Name: Guizhi Xu
CWID: 20008770

Midterm Assignment:

- Identify and describe a fictitious enterprise network (you can draw or describe) and carefully list the valued assets for this network.
- (It would be recommended to keep the number of assets more than 10 but less than 25.)
- Then, create a threat-asset matrix for your fictitious example and estimate the security risk for each individual cell in the matrix.
- Write a 1-2 sentence justification for each risk estimate.
- You are welcome to draw the matrix by hand (scan and cut the image into your paper) or you can use a tool such as Excel or PowerPoint.
- Submit your assignment via the Course Site

Description:

We identify and describe a fictitious enterprise network called “OnlyArtists”, that runs a social media application like Pinterest, Tumblr, or Facebook for all the artists to post and share their works. In addition, this fictious application is hosted and deployed on Amazon Web services (AWS).

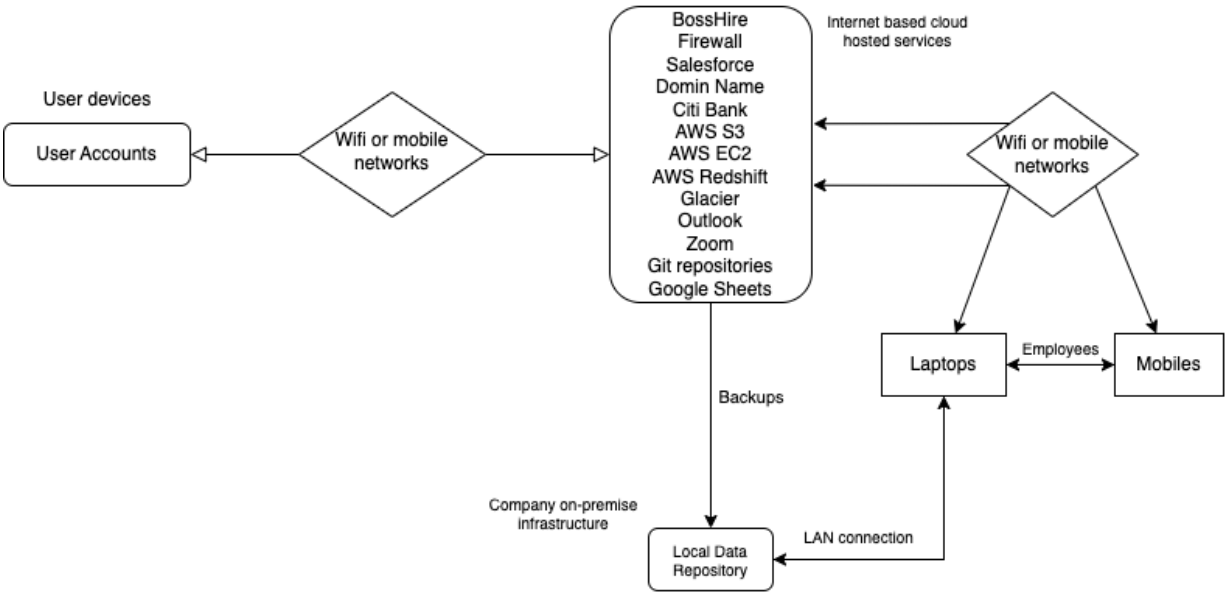
The assets for this website are listed and described as follows:

1. **Outlook**: The company's email domain for its employees, management, partners, and clients. Employees will have their own Microsoft account within the company's domain.
2. **Zoom**: Employees, like developers and artists, can collaborate in teams using Zoom meetings on their workplace or remotely.
3. **Domain Name**: The web domain name to access the application from the browser (onlyartist.com).
4. **BossHire**: BossHire is a recruiter management software. It is used for processing payrolls, keeping employee records (like leaves, designation, etc.), and processing employee applications for leaves, resignation, compensation, etc.
5. **Firewalls**: Firewall is used as a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.
6. **Salesforce**: Salesforce is a merchant software to manage client relationship data.
7. **Citi Bank**: Bank service for payroll and other financial transactional purposes and to store money securely.
8. **Git repositories**: Developers working in the company will use Git tools to coordinate their work before the software goes into production. It is stored locally as in most companies.
9. **User accounts**: The artists who post on "OnlyArtist" will create accounts to access the application from their devices, and these accounts will authenticate them before they can access it.
10. **Local Data storage**: A repository for the data stored on the cloud will also be stored locally on-premises data storage as a backup. Local data backups are taken from the cloud for both data security and experimentation purposes.

11. **Google Sheets**: Google Sheets are a handy tool for preparing and collaborating on spreadsheet-related work. It comes with the G Suite account for each user.
12. **Glacier**: Application data (artist posts) stored on S3 will routinely be transferred to glacier after a stipulated time period since their generation.
13. **Employee laptops**: As most IT companies, "OnlyArtist" will provide its employees with a company laptop (Mac in this case). Inevitably, important code, data, and email communication will be present on it.
14. **Employee mobile devices**: Employees will configure their emails on their personal/work mobile devices, as well as probably the Slack channel for faster communication.
15. **AWS S3**: The data of the application, including all the posts made by artists (text, media, video, etc.), are stored on the S3 buckets.
16. **AWS EC2**: The application is deployed using Elastic Compute Cloud (EC2) instances as the servers. Elasticity load balancing service of AWS automatically scales the number of instances as the need arises.
17. **AWS Redshift**: Redshift is used for analytics and warehousing of large petabyte-sized data that is generated dynamically on the system.

Diagrammatic Representation:

The diagrammatic representation of the above describes architecture is as follows:



Scale: 3 = High, 2 = Medium, 1 = Low

The threats faced by the assets of this system fall mainly in 4 categories:

Confidentiality: Access to sensitive information by attacker.

Integrity: maintaining the consistency, accuracy, and trustworthiness of data.

Availability: Ensuring Services and Data is available and working correctly.

Theft/Fraud: Acquiring Data or Services illegally.

Assets/Threats	Confidentiality	Integrity	Availability	Theft/Fraud	Total Risk
Glacier	P = 2 C =3 |R = 6	P = 2 C =2 |R = 4	P = 1 C =1 |R = 1	P = 2 C =2 |R = 4	15
Outlook	P = 2 C =3 |R = 6	P = 1 C =2 |R = 2	P = 1 C =1 |R = 1	P = 2 C =2 |R = 4	13
Zoom	P = 2 C =2 |R = 4	P = 2 C =1 |R = 2	P = 1 C =1 |R = 1	P = 2 C =1 |R = 2	9
Git repositories	P = 2 C =3 |R = 6	P = 1 C =1 |R = 1	P = 1 C =1 |R = 1	P = 2 C =3 |R = 6	14
Google Sheets	P = 2 C =2 |R = 4	P = 1 C =1 |R = 1	P = 1 C =1 |R = 1	P = 2 C =1 |R = 2	8
Domain Name	P = 1 C =2 |R = 2	P = 1 C =3 |R = 3	P = 1 C =3 |R = 3	P = 1 C =3 |R = 3	11
BossHire	P = 1 C =2 |R = 2	P = 1 C =2 |R = 2	P = 1 C =1 |R = 1	P = 1 C =2 |R = 2	7
Firewall	P = 2 C =3 |R = 6	P = 1 C =3 |R = 3	P = 1 C =3 |R = 3	P = 2 C =1 |R = 2	14
Salesforce	P = 1 C =2 |R = 2	P = 3 C =2 |R = 6	P = 2 C =2 |R = 4	P = 1 C =1 |R = 1	13
Citi Bank	P = 2 C =3 |R = 6	P = 2 C =2 |R = 4	P = 1 C =1 |R = 1	P = 2 C =2 |R = 4	15
Employee laptops	P = 2 C =3 |R = 6	P = 1 C =1 |R = 1	P = 1 C =2 |R = 2	P = 2 C =3 |R = 6	15
Employee mobiles	P = 2 C =2 |R = 4	P = 1 C =1 |R = 1	P = 1 C =1 |R = 1	P = 1 C =2 |R = 2	8
Local Data storage	P = 3 C =2 |R = 6	P = 2 C =2 |R = 4	P = 2 C =1 |R = 2	P = 3 C =3 |R = 9	21
User accounts	P = 2 C =3 |R = 6	P = 2 C =2 |R = 4	P = 1 C =1 |R = 1	P = 2 C =3 |R = 6	17
AWS S3	P = 1 C =3 |R = 3	P = 2 C =3 |R = 6	P = 1 C =2 |R = 2	P = 2 C =2 |R = 4	15
AWS EC2	P = 2 C =3 |R = 6	P = 2 C =2 |R = 4	P = 2 C =1 |R = 2	P = 1 C =1 |R = 1	13
AWS Redshift	P = 2 C =3 |R = 6	P = 2 C =2 |R = 4	P = 2 C =2 |R = 4	P = 2 C =2 |R = 4	18

Threat-Asset matrix:

The threat-Asset matric for the above describe system is as follow:

1. Glacier:

Confidentiality: AWS Glacier stores sensitive data that, if leaked, could damage the company's reputation.

Integrity: While data in Glacier is encrypted, a security breach could still occur. However, since the data is not frequently accessed, the system has more time to detect and respond to breaches.

Availability: Since Glacier is used for archival purposes, it is less vulnerable to DDoS attacks.

Theft/Fraud: There is a significant risk of theft due to the presence of valuable user data.

2. Outlook:

Confidentiality: Email data in Outlook is highly valuable and must be protected from competitors and hackers. Security protocols include general email account authentication and the company's firewall.

Integrity: Authentication protocols and firewalls make it difficult for hackers to gain unauthorized access to Outlook data. Any attempt at manipulating the data can be remedied easily.

Availability: Denial-of-service attacks on Outlook could cause inconvenience but are not critical.

Theft/Fraud: While there may not be much valuable data on Outlook, certain confidential business plans could be targeted by hackers.

3. Zoom:

Confidentiality: Zoom's security protocols may not be strong enough to fully protect company data, leading to the potential for eavesdropping and data leaks.

Integrity: While the communication on Zoom may not be critical, a breach could still have consequences.

Availability: Since Zoom is used internally for communication, other forms of communication can be employed while the system is being remedied.

Theft/Fraud: While confidential information may occasionally be shared on Zoom, the risks are covered in the preceding threats.

4. **Git repositories:**

Confidentiality: Git repositories contain critical intellectual property for the company and must be secured to prevent unauthorized access.

Integrity: Changes to the code are easily detected and remedied due to rigorous testing and backup procedures.

Availability: Since Git is used for development before the production phase, it is not susceptible to DDoS attacks.

Theft/Fraud: A breach of authentication and firewall security could lead to serious loss for the company.

5. **Google Sheets:**

Confidentiality: Google Sheets may contain sensitive data used in internal and external meetings.

Integrity: The scope for an integrity attack on internal documents is low.

Availability: Google Sheets are backed up and any DDoS attack will be remedied by Google. Alternatives to Google Sheets exist if necessary.

Theft/Fraud: Google Sheets are not a consumer-facing service and there is not much scope for selling information stolen from them.

6. **Domain Name:**

Confidentiality: Domain name hijackers can gain control of email accounts, leading to major confidentiality consequences. Careful use of 2-factor authentication and reputable domain registrar companies can mitigate this risk.

Integrity: Once a domain name is hijacked, attackers can install malware or use social engineering attacks, but the probability of success is low.

Availability: Popular domain name hijackings can lead to significant denial of service consequences for legitimate users.

Theft/Fraud: Hijackers can steal personal information from unsuspecting users who enter their data on hijacked websites.

7. **BossHire:**

Confidentiality: BossHire contains confidential information of the company's employees that could be sold on the dark web. It is password protected and uses AES 256-bit encryption and TLS 1.2 protocol.

Integrity: Attempts to alter transactions and records are unlikely due to the system's strong security.

Availability: BossHire is considered low risk and does not directly affect the company's system.

Theft/Fraud: There is a small risk of theft or fraud, possibly by an employee.

8. **Firewall:**

Confidentiality: Firewalls are usually the first line of defense against cyberattacks, making them a prime target for attackers. If a firewall is compromised, it can leave the network assets vulnerable to attack.

Integrity: Attackers can bypass firewalls by disguising data packets as legitimate packets. These malicious packets can corrupt the system or modify data.

Availability: Backup firewalls are often used to ensure availability in case of damage to the primary firewall.

Theft/fraud: Firewall logs and configurations contain sensitive information that could be valuable to attackers attempting to exploit vulnerabilities or gain unauthorized access.

9. **Salesforce:**

Confidentiality: Customer Relationship Management (CRM) data typically includes user data and is often targeted by attackers.

Integrity: Attackers who gain access to the CRM can manipulate website trends and compromise confidential user data.

Availability: As long as there is a contract with Salesforce, CRM data will remain available.

Theft/fraud: Cybercriminals may attempt to steal customer data or use fraudulent methods to gain access to Salesforce accounts, potentially leading to financial losses and damage to the company's reputation.

10. Citi Bank:

Confidentiality: Banking systems process and store highly confidential information, making them a prime target for attackers.

Integrity: If attackers gain access to bank records, they can alter the information stored there.

Availability: Banking services need to be available around the clock, so there is usually no motive for attackers to target them with a denial-of-service attack.

Theft/fraud: Credit and debit card fraud can occur in banking systems.

11. **Employee laptops:**

Confidentiality: Developer laptops often contain valuable code and email information that could be of interest to competitors. However, Macs are generally well protected against malware.

Integrity: Companies typically have strong policies for backing up code, making integrity attacks less of a concern.

Availability: If an employee's laptop is out of service, companies can provide ad-hoc solutions like using another laptop or logging in from a colleague's device.

Theft/fraud: Since source code is of significant value to competitors, attempts at theft may be made on employee laptops.

12. **Employee mobile devices:**

Confidentiality: Employee mobile devices often contain email information and Slack channels, but generally not more critical information. Most phones, like iPhones, have biometric protection, but this is not always a guarantee since phones are personal and not provided by the company.

Integrity: Employee phones usually do not provide critical services to the company, so integrity attacks are less of a concern.

Availability: If an employee's mobile device is out of service, they can switch to using a laptop.

Theft/fraud: While email information and contacts have some value to competitors, they are not typically critical and are generally secured by biometric or two-factor authentication.

13. **Local data backup:**

Confidentiality: Data backups are connected to the company's Wi-Fi network to transfer data and are vulnerable to attacks on the internet. They are also connected to developer systems, making them an entry point for malware attacks.

Integrity: Backups are not part of the deployed system and are therefore not obvious targets for integrity attacks. However, they can be used as a route for malware attacks.

Availability: Since backups are not a service provided by the company, they are not usually targets for denial-of-service attacks.

Theft/fraud: Stolen backup data can be sold for profit.

14. **User accounts:**

Confidentiality: User accounts are vulnerable to hacking, which can result in the loss of personal data. While passwords are generally secure, phishing, and social engineering attacks can be used to obtain passwords from users. Additionally, server systems may be hacked to reveal passwords for multiple users. Social engineering on employees or hacking their systems can also lead to password disclosure.

Integrity: Malicious actors may attempt to take control of user accounts by obtaining passwords. Password authentication, which is common in social media applications, is a weak link. Personal data can be disclosed and sold on the dark web.

Availability: Directing DDoS attacks at users is not a viable attack vector since they are consumers of the service.

Theft/Fraud: User data is valuable, and on a large scale, data of many users is valuable to competitors for data analysis and consumer profiling. On a small scale, a single user may be targeted to disclose confidential information that is of interest to someone.

15. AWS S3:

Confidentiality: Since AWS is a major cloud provider, the probability of attempted attacks is significant. While S3 has encryption options, given its storage of vast amounts of user data (including private posts and other sensitive information), the consequences of a successful hack can be severe.

Integrity: S3 has a strong backup and recovery system, which reduces the probability of attacks succeeding. However, the consequences of data corruption will be serious since undermining user data integrity will amount to a breach of trust on the part of the company.

Availability: Since S3 stores only flat files, DDoS attacks are not very likely. However, the consequences of a denial of service will be somewhat inconvenient, despite not being critical.

Theft/Fraud: Stealing user data will be useful for malicious actors for data mining and even in cases of doxing on a large scale, which will have serious consequences for the company's reputation.

16. AWS EC2:

Confidentiality: EC2 deploys the application software using an executable (.exe) file. While being a public cloud, it is often attacked by malicious actors, reverse-engineering the code is extremely hard, hence there is not a very high confidentiality threat.

Integrity: An attack compromising integrity seeks to alter the application software in production. While motivations for such an attack exist, EC2 is generally secure and in the worst case, is backed up by replication and can be scaled to exclude hacked instances.

Availability: The possibility of a DDoS attack originating from hacked user accounts, employee accounts, or corrupted software is present but not likely to work due to the elastic load balancing feature of AWS, which expands the compute's capacity.

Theft/Fraud: Stealing compute will not have any impact due to the elasticity of EC2, and in any case, will be a liability of the cloud vendor rather than the company.

17. AWS Redshift:

Confidentiality: While Redshift has encryption options like S3, the consequences of a successful hack can be serious due to the warehoused user data.

Integrity: Corruption of the data warehouse hosted on Redshift will constitute an integrity attack. Redshift is backed up and thus relatively secure.

Availability: Since Redshift is dynamic, its availability can be compromised by attacks, although it has safety mechanisms.

Theft/Fraud: Like S3, the possibility of stolen data being sold to unauthorized parties is a serious threat.