Asset Identification and Risk Assessment - Starbucks

Student name: **D.James Chrishan**

Student ID: **AS0509**

Step 1: Defining the Organization

Organization: Starbucks Corporation
Industry: Retail (Food and Beverage)

Overview:
Starbucks is one of the largest coffeehouse chains in the world, with over 34,000 locations across 80 countries. It operates in the food and beverage retail industry, primarily selling coffee, tea, and snacks. However, its operations extend far beyond just physical stores, as it has embraced a digitally-driven business model.

Starbucks relies heavily on digital platforms to connect with its customers, including a robust mobile app, online ordering, and a widely used loyalty program called Starbucks Rewards. The app allows customers to make orders, pay online, and collect rewards, making it a critical component of Starbucks' customer engagement strategy. Additionally, the company is involved in e-commerce, selling merchandise, coffee beans, and other products directly to consumers.

The organization also emphasizes ethical sourcing and sustainability, reflecting its commitment to environmental and social responsibility. Starbucks operates in multiple sectors, from retail to corporate offices, supply chain logistics, and production facilities that handle the sourcing and manufacturing of its products.

Key Objectives:

1. **Customer Experience and Engagement**: Starbucks is dedicated to offering a seamless customer experience through personalized digital services and rewards systems, both online and in-store.
2. **Data Privacy and Security**: Given the large volume of transactions and personal data handled, including payment information and customer preferences, securing this data is essential to the company’s operations.
3. **Operational Efficiency**: Starbucks seeks to optimize its supply chain and streamline processes to maintain business continuity across its global network.
4. **Innovation and Technology**: Leveraging technology for innovation in customer engagement, mobile ordering, and digital payments is a central focus.

5. **Sustainability and Ethical Sourcing**: Starbucks aims to create a sustainable, ethically-sourced product supply chain, reducing its environmental footprint while promoting social responsibility.

Digital Infrastructure:
Starbucks has invested heavily in its digital ecosystem. It operates various digital platforms, including its mobile app, which integrates mobile payments, loyalty rewards, and ordering. These platforms generate a significant portion of Starbucks' revenue and are heavily reliant on secure IT infrastructure and data management systems.

The company's customer-facing technology is supported by a complex back-end system, which includes cloud-based solutions for handling data, managing transactions, inventory, and logistics. They also use in-store technologies, such as point-of-sale (POS) systems, in-store Wi-Fi, and connected devices that facilitate operations.

Operations:

- **Retail Operations**: Serving millions of customers daily through stores and digital platforms.
- **Supply Chain**: Starbucks manages a global supply chain, sourcing coffee beans and other materials from multiple countries. Its operations depend on reliable third-party vendors and logistics providers.
- **Technology and Data Management**: Includes the Starbucks mobile app, online ordering systems, databases, and cloud computing services that store and process sensitive customer and business data.
- **Corporate and Administrative**: Includes HR, finance, and legal departments, each handling sensitive employee and business information.

Starbucks' reliance on digital technologies, its global operations, and the vast amounts of personal and financial data it handles make cybersecurity a top priority. Protecting this data, ensuring compliance with global data privacy laws, and mitigating potential risks from cyber threats are critical to the organization's success and customer trust.

Step 2: Identifying key assets and resources

In a cybersecurity risk assessment, understanding and categorizing the assets of an organization is crucial. For Starbucks, these assets include data, systems, personnel, and physical facilities, all of which are vital for daily operations and long-term success.

1. Data Assets

Starbucks collects and processes a significant amount of data, much of which is sensitive and requires strong protection mechanisms.

- **Customer Data**:
    - **Personal information**: Names, addresses, phone numbers, email addresses, and other identifying details provided by customers through online orders, app registrations, and loyalty programs.
    - **Payment data**: Credit card information and transaction history from both in-store and online purchases. As Starbucks processes millions of transactions daily, the integrity and security of this payment data are paramount.
    - **Loyalty program information**: Starbucks Rewards, one of the most popular loyalty programs globally, stores customers' purchase histories, preferences, and accrued points, which are tied to personal profiles.
    - **Behavioral data**: Information on customer preferences, order histories, and interactions with Starbucks' app, helping the company personalize marketing and promotions.
- **Corporate Data**:
    - **Business financials**: Financial reports, sales records, forecasts, and other sensitive financial documents.
    - **Intellectual property**: Proprietary recipes, product development data, and market strategies.
    - **Partner/vendor data**: Information about the third-party vendors and suppliers involved in Starbucks' global supply chain, including contracts and payment records.
- **Employee Data**:
    - **Personal information**: Human Resources (HR) records, payroll information, health benefits data, and other confidential details of Starbucks' employees across stores, corporate offices, and supply chain partners.

2. System Assets

Starbucks operates a vast network of digital systems that support its global operations. The integrity, availability, and security of these systems are crucial to daily business functions.

- **POS (Point-of-Sale) Systems**:
  The in-store POS systems handle all transactions and connect to Starbucks' central data systems for real-time updates. These systems are often interconnected across locations, making them essential for business continuity and financial management.
- **Mobile Applications and E-commerce Platform**:
    - **Starbucks Mobile App**: One of the most critical customer-facing systems, the app is used for placing orders, managing loyalty points, and processing payments. It's integrated with personal customer data and financial transactions, making it a high-value target for cyber attackers.

    - **E-commerce website**: Used for online purchases of Starbucks merchandise and coffee, connecting to the same back-end systems as the mobile app.
- **Cloud Infrastructure**:
  Starbucks relies on cloud services to store vast amounts of data, including customer profiles, financial transactions, and business analytics. This infrastructure must be protected from breaches, unauthorized access, and outages.
- **Corporate Systems**:
    - **Databases**: Secure databases store sensitive business, customer, and employee information.
    - **Email and communication systems**: Used internally for corporate operations, including confidential communications between corporate offices, store management, and supply chain partners.
    - **Networks**: Secure, global network infrastructure supports both corporate offices and retail stores. Ensuring these networks are protected from breaches or downtime is critical to business operations.

3. Personnel Assets

Starbucks' workforce is a critical part of its operation, from baristas to corporate executives. Ensuring that employees are equipped with the tools and knowledge to maintain cybersecurity is essential.

- **Retail Employees**:
  Starbucks store workers (baristas, shift supervisors, store managers) are responsible for operating POS systems and interacting with customer data daily. These employees need training on secure transaction practices and protocols for handling digital payments and customer interactions.
- **Corporate Employees**:
    - **IT and cybersecurity personnel**: These teams manage and monitor Starbucks' digital infrastructure, responding to security threats and ensuring the protection of systems and data.
    - **HR and administrative staff**: Handle sensitive employee data and ensure compliance with internal and external data protection regulations.
- **Third-party Vendors/Contractors**:
    - **Technology partners**: External vendors providing cloud, software, and cybersecurity services. These partners play an integral role in maintaining system availability and protecting Starbucks' infrastructure.
    - **Supply chain partners**: Starbucks works with various vendors to manage its supply chain, from coffee bean farmers to logistics companies. These partners may access certain business systems, requiring strong controls to prevent potential third-party risk.

4. Facilities and Supplies

Although Starbucks is a digitally-driven company, its physical facilities are integral to its operations. Security for these locations is essential to prevent unauthorized access, data breaches, or physical damage.

- **Retail Stores**:
  Starbucks' retail stores are where the majority of transactions occur, and they serve as the primary point of interaction with customers. Each location needs secure POS systems, Wi-Fi networks, and video surveillance to protect both physical and digital assets.
- **Data Centers**:
  Starbucks may use physical data centers to store critical data and backup systems. Protecting these centers from both physical and cyber threats is crucial for ensuring business continuity in the event of natural disasters, power outages, or attacks.
- **Corporate Offices**:
  Starbucks' global corporate offices house employees responsible for various administrative functions. Physical access to these offices needs to be tightly controlled to protect sensitive corporate data.
- **Backup and Disaster Recovery Facilities**:
  These facilities ensure that Starbucks can quickly restore operations after a disruption, such as a natural disaster or cyberattack. These are often off-site locations designed to safeguard backups of critical data and systems.

Categorization by Importance:

1. **Mission-critical**:
   - **Customer data**: Personal and financial information tied to the Starbucks Rewards program and digital transactions is crucial for maintaining customer trust.
   - **POS Systems**: In-store and online transaction systems are vital for daily operations.
   - **Cloud Infrastructure**: Starbucks' cloud environment stores sensitive business, customer, and financial data.
   - **Mobile Applications**: The Starbucks app is central to customer engagement and represents a significant revenue stream.
2. **Essential**:
   - **Employee data**: Payroll, HR information, and corporate communication systems ensure operational stability.
   - **Third-party vendors and partners**: Supply chain and technology vendors are key to continuous operations.
   - **Data centers and backup facilities**: Critical for disaster recovery and business continuity.
3. **Supportive**:

    - **Retail locations**: While important for physical operations, individual store locations have a lower impact on the company as a whole.
    - **Physical security**: Ensures the protection of facilities and tangible assets from theft, vandalism, or unauthorized access.

Step 3: Identifying Potential Threats and Vulnerabilities

In this step, the goal is to identify potential cybersecurity threats that Starbucks may face and the vulnerabilities in its systems and processes that could be exploited by these threats. We will categorize the threats into human, technological, operational, and environmental risks and then examine how these threats might exploit specific vulnerabilities within the organization.

1. Human Threats

Threat 1: Insider Threats (Employees or Contractors)
Insider threats can arise from employees, contractors, or third-party vendors who have access to Starbucks' internal systems. These threats can be intentional (malicious employees) or accidental (careless handling of data).

- **Vulnerabilities**:
    - **Inadequate access controls**: Employees may have access to systems and data beyond what is necessary for their roles, increasing the risk of unauthorized actions.
    - **Lack of monitoring**: Insufficient monitoring of user activities in internal systems may allow employees to access or exfiltrate sensitive data without being detected.
    - **Poor offboarding processes**: When employees leave the company, failure to immediately revoke their system access can create a vulnerability.

Potential Impact:

- Compromise of sensitive customer or employee data, including financial information, could lead to breaches, reputational damage, and regulatory fines.

Threat 2: Phishing Attacks
Phishing attacks involve tricking employees into revealing sensitive information, such as login credentials, through fraudulent emails or messages that appear legitimate. These types of attacks are widespread and often target employees at all levels of an organization.

- **Vulnerabilities**:
    - **Lack of employee cybersecurity awareness**: Employees may not be trained to recognize phishing attempts or social engineering tactics.

- **Inadequate email filtering systems**: A lack of advanced filtering tools may allow phishing emails to reach employees' inboxes.
- **Weak incident response**: If phishing attacks are not reported and responded to promptly, the impact could escalate.

Potential Impact:

- Compromised user accounts could lead to unauthorized access to systems, data breaches, and further security incidents such as malware installation.

2. Technological Threats

Threat 3: Malware and Ransomware Attacks

Malware, including ransomware, poses a significant threat to Starbucks' operations. Attackers could use ransomware to encrypt critical data or systems, demanding payment to restore access. Malware could also be used to steal data or disrupt operations.

- **Vulnerabilities**:
  - **Unpatched software**: Outdated or unpatched systems, including POS terminals, mobile apps, or internal databases, may have vulnerabilities that can be exploited by malware.
  - **Lack of endpoint security**: Insufficient protections on employee devices, such as laptops or smartphones, could serve as entry points for malware.
  - **Weak email or website security**: Clicking on malicious links in phishing emails or compromised websites could introduce malware into Starbucks' network.

Potential Impact:

- Ransomware could disrupt operations by locking down POS systems, inventory systems, or corporate databases, leading to significant financial losses and reputational damage. Sensitive customer data could also be stolen.

Threat 4: Outdated or Compromised Mobile Applications

Starbucks' mobile app is central to its customer engagement strategy. If the app contains vulnerabilities, it could become a prime target for hackers, leading to a compromise of customer accounts and payment data.

- **Vulnerabilities**:
  - **Insecure coding practices**: If the mobile app is developed without following secure coding guidelines, vulnerabilities could be introduced.
  - **Lack of regular updates**: Failing to regularly update the app with security patches could leave it vulnerable to exploitation.

    - **Insecure APIs**: The application programming interfaces (APIs) that connect the mobile app to Starbucks' back-end systems may be vulnerable to attacks if not properly secured.

Potential Impact:

- A successful attack on the mobile app could compromise millions of user accounts, leading to identity theft, payment card fraud, and reputational damage for Starbucks.

3. Operational Threats

Threat 5: Third-Party Vendor Compromise
Starbucks relies heavily on third-party vendors for its supply chain, cloud services, and IT support. A compromise of one of these vendors could lead to disruptions in Starbucks' operations or expose sensitive data.

- **Vulnerabilities**:
    - **Weak vendor risk management**: Insufficient evaluation and monitoring of third-party vendors' security practices could lead to Starbucks' data being exposed via a vendor breach.
    - **Overreliance on third-party services**: Depending heavily on external providers without proper controls (e.g., cloud storage providers, payment gateways) increases the risk of disruptions in case of a vendor breach.
    - **Shared responsibility gaps**: In cloud services, there may be misunderstandings between Starbucks and the vendor about who is responsible for securing certain parts of the system.

Potential Impact:

- A breach of a vendor's system could expose Starbucks' customer or financial data, disrupt operations (such as ordering or payments), and harm the company's reputation.

4. Environmental Threats

Threat 6: Natural Disasters (Fires, Floods, Earthquakes)
Starbucks has a global presence, with physical stores, corporate offices, and data centers located around the world. Natural disasters such as fires, floods, or earthquakes could disrupt these physical assets, affecting both daily operations and data integrity.

- **Vulnerabilities**:

    - **Lack of disaster recovery and business continuity plans**: Without proper backup and recovery strategies, Starbucks may experience significant downtime or data loss during a natural disaster.
    - **Single-location data centers**: If critical data is stored in a single data center without geographical redundancy, it may be vulnerable to regional disasters.
    - **Inadequate physical security**: Insufficient fire suppression systems or flood protection measures in physical facilities could increase the risk of damage.

Potential Impact:

- A natural disaster could lead to extended store closures, data loss, or disruption of digital services, impacting revenue and customer trust.

5. Human Threats (External)

Threat 7: Social Engineering and Credential Stuffing Attacks
Attackers could use social engineering techniques to trick employees into divulging sensitive information or use credential stuffing (trying commonly used or leaked passwords) to gain unauthorized access to Starbucks systems.

- **Vulnerabilities**:
    - **Weak password policies**: If Starbucks allows employees or customers to use weak or reused passwords, this increases the risk of credential stuffing attacks.
    - **No multi-factor authentication (MFA)**: Without MFA, even if credentials are compromised, attackers could gain direct access to accounts.
    - **Poor employee training**: Employees unaware of social engineering tactics may be more susceptible to falling victim to these types of attacks.

Potential Impact:

- Attackers gaining access to internal systems via compromised credentials could lead to data theft, disruption of services, or manipulation of internal processes.

Vulnerability Summary

- **Weak passwords or lack of multi-factor authentication (MFA)**: This can leave systems vulnerable to brute-force attacks or unauthorized access.
- **Unpatched software or outdated systems**: If Starbucks' systems are not regularly updated with security patches, they may contain vulnerabilities that can be exploited.
- **Inadequate physical security measures**: Stores, data centers, or corporate offices may be at risk if proper security measures (such as surveillance or fire prevention) are not in place.

- **Lack of employee training**: Without adequate cybersecurity training, employees may fall victim to phishing, social engineering, or other attacks.
- **Over Reliance on third-party vendors**: If Starbucks doesn't adequately assess and monitor the security practices of its vendors, it could be exposed to third-party risks.

Step 4: Selecting a Risk Assessment Approach

1. Choosing the Qualitative Approach for Starbucks

Given Starbucks' business model, large customer base, and global presence, a **qualitative risk assessment** approach is most suitable. Here's why:

- **Complexity of Operations**:
  Starbucks operates across multiple channels (retail stores, mobile apps, online services, corporate offices, and supply chain networks), each facing different risks. Qualitative assessment allows Starbucks to quickly categorize risks at a high level without needing precise data for each business unit.
- **Customer and Employee Data Sensitivity**:
  Protecting personal and financial data is a high priority. Starbucks handles millions of customer transactions daily, and any compromise of this data could lead to reputational damage. A qualitative approach allows the company to prioritize risks associated with customer privacy, data breaches, and insider threats without needing exact dollar amounts to estimate the impact.
- **Time and Resource Constraints**:
  A quantitative approach would require Starbucks to gather extensive data on every potential risk (e.g., the probability of each type of cyberattack, the cost of each system's downtime). This data may not always be available, and collecting it could delay important decisions. A qualitative approach enables Starbucks to make timely decisions based on expert judgment.
- **Focus on Strategic Risk Management**:
  Starbucks needs to identify and manage cybersecurity risks at a strategic level. By focusing on qualitative descriptions like "high impact" or "medium likelihood," Starbucks can communicate risk priorities to senior management and make informed decisions without diving into technical details.

2. Steps in a Qualitative Risk Assessment

1. **Identify Risks**: Starbucks would identify risks through workshops, discussions with cybersecurity teams, reviewing past incidents, and consulting industry threat reports. For

example, a risk could be “data breach due to phishing attacks” or “ransomware targeting POS systems.”

2. **Assess Likelihood and Impact**: Each risk is evaluated in terms of its **likelihood** (e.g., how probable it is that the event will occur) and its **impact** (e.g., the severity of the consequences if it happens).
    - **Likelihood** could be classified as **Unlikely, Possible, Likely, or Certain**.
    - **Impact** could be classified as **Low, Medium, or High**.
3. For example, a ransomware attack targeting customer data may be categorized as “Likely” due to its prevalence in the industry and as having a “High” impact because of the potential for financial loss and reputational damage.
4. **Risk Prioritization**: Starbucks would rank risks based on their combination of likelihood and impact. Risks that are both **high impact and highly likely** should be prioritized for mitigation efforts. Lower-priority risks (e.g., those with low impact or unlikely occurrence) can be addressed later.
5. **Develop Mitigation Strategies**: After identifying and ranking risks, Starbucks would create mitigation plans. For example, to reduce the risk of a phishing attack, Starbucks could invest in employee training and deploy multi-factor authentication (MFA).
6. **Monitor and Review**: Risk assessments should be conducted regularly to ensure that new risks are identified, and mitigation efforts are effective. As the cyber threat landscape evolves, Starbucks would need to update its risk assessment.

3. Why Starbucks Chose Qualitative Over Quantitative

While a **quantitative approach** would provide exact financial estimates of potential losses, Starbucks may not have access to all the necessary data to perform accurate calculations across its entire global operation. A quantitative approach would also be **more resource-intensive** and require in-depth analysis of historical data on breaches, system downtimes, and financial losses, which might not be feasible across such a large network.

Starbucks’ needs are better served by a qualitative approach for the following reasons:

- **Scalability**: Starbucks operates globally, and its risks vary depending on the region, market, and local regulations. A qualitative approach scales well across different business units, allowing flexibility in addressing specific local or regional threats.
- **Speed**: Starbucks needs to assess risks regularly and implement strategies quickly to respond to evolving cyber threats. A qualitative approach can provide a faster assessment and decision-making process compared to quantitative models that require extensive data analysis.
- **Focus on Key Priorities**: Starbucks’ main priority is protecting customer trust and ensuring the continuous operation of its stores, mobile apps, and supply chain. A qualitative approach allows Starbucks to focus on high-priority risks without being bogged down by complex calculations.

4. Examples of Using the Qualitative Approach at Starbucks

- **Ransomware Attack on POS Systems**:
  - **Likelihood**: Likely (due to the widespread use of ransomware in retail).
  - **Impact**: High (could disrupt in-store transactions globally and lead to significant revenue loss).
  - **Mitigation**: Implementing regular backups, patching vulnerabilities, and educating employees.
- **Data Breach from Phishing**:
  - **Likelihood**: Possible (based on the increasing number of phishing attempts targeting employees in similar industries).
  - **Impact**: High (exposure of sensitive customer data leading to reputational damage and legal consequences).
  - **Mitigation**: Strengthening MFA, phishing awareness training, and robust email filtering.

Step 5: Creating a Preliminary Risk Matrix

In Step 5, we take the potential threats identified in Step 3 and the qualitative risk assessment approach chosen in Step 4 to build a **Risk Matrix**. The purpose of this matrix is to visually map the risks Starbucks faces, based on two key factors:

1. **Impact**: The potential severity of each threat if it occurs (e.g., low, medium, high).
2. **Likelihood**: The probability of each threat occurring (e.g., unlikely, possible, likely).

The risk matrix allows Starbucks to prioritize threats by showing which ones pose the greatest risk to the organization. It helps in focusing mitigation efforts where they are most needed, balancing the likelihood of an event with its potential impact.

1. Understanding the Risk Matrix

The matrix is a grid where the **likelihood** of a threat is plotted on one axis (typically the vertical axis), and the **impact** is plotted on the other axis (typically the horizontal axis). This allows each threat to be placed within a specific area of the grid.

Here's a typical structure for a risk matrix:

	Low Impact	Medium Impact	High Impact
Unlikely	Low priority risk	Medium priority risk	Medium priority risk
Possible	Medium priority risk	Medium priority risk	High priority risk
Likely	Medium priority risk	High priority risk	Critical risk

- **Low priority risks**: These have either low impact or are unlikely to happen. These are not urgent but should still be monitored.
- **Medium priority risks**: These have a moderate chance of occurring or would cause medium impact. They should be mitigated, but they may not be the first focus.
- **High priority risks**: These are either likely to happen or would cause significant damage if they did. These should be addressed quickly.
- **Critical risks**: These are both likely to happen and have severe consequences. Starbucks should take immediate action to mitigate these risks.

2. Building Starbucks' Risk Matrix

Let's use the identified threats from Step 3 and categorize them into the matrix. This will help Starbucks prioritize its risk mitigation efforts.

Example Risk Matrix for Starbucks

Threat	Likelihood	Impact	Risk Category (Priority)
1. Insider Threats (Employees)	Possible	High	High Priority Risk
2. Phishing Attacks	Likely	High	Critical Risk
3. Ransomware Attacks	Possible	High	High Priority Risk
4. Outdated or Compromised Mobile App	Likely	Medium	High Priority Risk
5. Third-Party Vendor Compromise	Possible	High	High Priority Risk
6. Natural Disasters (Fires, Floods)	Unlikely	High	Medium Priority Risk
7. Social Engineering/Credential Stuffing	Likely	Medium	High Priority Risk

Let's break down how these threats fit into the matrix:

a. Critical Risks

These are the highest-priority risks that need immediate attention. They have both a high likelihood and high impact.

- **Phishing Attacks (Likely and High Impact)**: Phishing attacks are prevalent in many industries, especially retail and customer-focused businesses like Starbucks. Given Starbucks' large employee base and frequent customer interactions, the likelihood of phishing attempts is high. The impact is also severe, as successful phishing attacks can lead to data breaches, financial fraud, and reputational damage. **Mitigation** strategies such as stronger employee training, enhanced email filtering systems, and multi-factor authentication (MFA) are crucial.

b. High Priority Risks

These are also significant risks, either because they are likely to happen or because their impact is severe. Starbucks should take proactive steps to mitigate them.

- **Insider Threats (Possible and High Impact)**: Insider threats, whether malicious or accidental, pose a significant risk due to the sensitive customer and operational data Starbucks manages. Though not as likely as phishing, they can be damaging. Strengthening internal access controls, monitoring employee activity, and improving offboarding processes can mitigate this risk.
- **Ransomware Attacks (Possible and High Impact)**: The possibility of ransomware attacks exists due to Starbucks' vast network and reliance on point-of-sale (POS) systems and other digital platforms. Ransomware could cripple store operations. Regular system backups, software patches, and staff training will be crucial mitigation strategies.
- **Outdated or Compromised Mobile App (Likely and Medium Impact)**: Given that Starbucks heavily relies on its mobile app for customer loyalty programs, mobile ordering, and payments, vulnerabilities in the app could lead to significant customer data breaches. Regular updates, secure coding practices, and rigorous app security testing should be enforced.
- **Third-Party Vendor Compromise (Possible and High Impact)**: Starbucks relies on third-party vendors for its supply chain, cloud services, and IT infrastructure. A breach at a vendor could expose sensitive information. Starbucks must improve vendor risk management practices, requiring vendors to comply with robust cybersecurity standards.
- **Social Engineering/Credential Stuffing (Likely and Medium Impact)**: Social engineering and credential stuffing are fairly common, particularly with reused passwords or weak password policies. The likelihood is high, and while the impact may not be catastrophic initially, it could lead to more severe breaches. Implementing MFA and strong password policies can reduce this risk.

c. Medium Priority Risks

These risks may occur less frequently or have less severe impacts, but they should still be addressed in the cybersecurity plan.

- **Natural Disasters (Unlikely and High Impact)**: Although the likelihood of natural disasters like floods or earthquakes may be low, their potential impact on Starbucks' physical stores, data centers, or regional operations can be high. Starbucks needs disaster recovery and business continuity plans, along with geographic redundancy for data storage.

3. Mapping the Threats on a Risk Matrix Chart

Visually representing these threats in a matrix can help Starbucks' security teams and leadership easily grasp the priority areas for mitigation efforts. Here's how the risk matrix for Starbucks would look:

Likelihood/Impact	Low Impact	Medium Impact	High Impact
Unlikely	Low Priority Risk	Social Engineering	Natural Disasters
Possible	Low Priority Risk	Third-Party Vendor	Insider Threats, Ransomware
Likely	Low Priority Risk	Compromised Mobile App	Phishing Attacks

In this matrix:

- **Phishing attacks** are both likely and high-impact, so they are at the highest level of criticality.
- **Ransomware** and **insider threats** are less likely but still have a high impact, making them high-priority risks.
- **Third-party vendor compromise** is less likely but could have high consequences, placing it in the medium-high category.
- **Natural disasters** are unlikely, but their impact is high, placing them lower on the priority list for mitigation but still worth attention in contingency planning.

4. Why Starbucks Should Use a Risk Matrix

The risk matrix helps Starbucks focus its cybersecurity resources efficiently. It enables Starbucks to:

- **Prioritize high-risk areas** like phishing and ransomware.
- **Allocate resources** to address the most critical risks first.
- **Communicate risk** to leadership and stakeholders effectively using a clear visual tool.
- **Guide decision-making** on where to invest in cybersecurity tools, employee training, and disaster recovery planning.

By using this matrix, Starbucks can better manage its cybersecurity risks, ensure the protection of customer data, and maintain its operations securely and efficiently.