Solution:

Step 1: Identify all potential threats

Personal/Sensitive data: As Sam's Scoops recent expansion the company have seen a large influx of customer data which includes sensitive information such as customers' name, addresses, credit card details, and other personal data. This sensitive data can be the target of malicious attackers

Personal Computers: Employees using personal computers for work can increase the attack surafce. These devices serve as attacking vectors that potential attackers can exploit to get to the company's network.

Cyber attacks: Due to everchanging landscape of online businesses, new attacks started to emerge on daily basis. Sam's Scoops' employees can become target of social engineering attacks or ransomware attacks

APTs: Advanced persistent threats are another type of attacks that malicious actors used to maintain the access to a system over a long period of time.

DDoS: Sam's Scoops can be targeted by a distributed denial of services attacks which an attacker carry out by flooding the server with unnecessary requests.

Step 2: Evaluate risks

- The leak/loss of personal or sensitive data of customers can lead to reputational loss for the business. Furthermore it could also lead to hefty fines if the business failed to comply with industry standards and regulations. The likelihood of attack to steal senstive data is high as the number of malicious attacks to steal sensitive information is increasing day by day
- Personal computers used by employees on company's network are a major vulnerability. The access level these devices possess can pose a threat to the company. If these devices fall into the hand of an malicious attacker, then the chance of unauthorize access to the system increases.
- As Sam's Scoops expands the potential attack surface increases. Also the likelihood of cyber attacks on the company increases as well. Company could face some common cyber attacks such as Man-in-the-Middle attacks and ransomware attacks. These attacks could disrupt company's operations and can also lead major financial loss.
- APTs can lead to prolonged unauthorized access to a system. Malicious actors tend to exfiltrate sensitive data over a long period of time under this attack. They also maintains the backdoor access to the system for future attacks. APTs can lead to data breaches of the sensitive data which could be fatal to the organization
- DDoS attacks can use company's IoT devices to flood the company server with illegitimate requests. DDoS can lead to server downtime which can result in server not responding to legitimate request which could lead to operation disruptions. And also it could lead to reputational damage.

Step 3: Develop countermeasures for each threat

- Sam's Scoops' should ensure that the business are complying with the appropriate regulations such PCI DSS to protect data and information systems. Sam's Scoops needs to make sure the sensitive customers' data is protected at all costs using techniques like Full disk encryption, AES, and SHAW256 etc.
- Personal computers used by employees needs to be provided with endpoint security such as installation of anti-malwares and full disc data encryption. Also, the employees should be educated about the other potential threats that devices pose that malicious actors could target.
- Encryption can be used to prevent/deter Man-in-the-Middle attacks. By encrypting the network traffic the data is converted into unreadable form of text that can only be brought back to original form using the appropriate decrypt key. Sam's Scoops should only carry out their internet activities over secured transmission protocols such as TLS SSL. Sam's Scoops can also incorporate the use of digital certificates, digital signatures to better protect the customers' data.
- To protect Sam's Scoops from APTs the company should incorporate the use of IDPS devices, Anti-malware softwares, NextGen Firewalls and SIEM or network traffic monitoring systems.
- To prevent DDoS attacks firewalls need to be incorporated by Sam's Scoops. Also, network segmentation of devices can help reducing the chances of DDoS.

Step 4: Design a comprehensive data protection strategy

Data Backups: Sam's Scoops should incorporate different data backup strategies such as incremental backup, full backup and database backup in order to secure data. Incremental backups will allow the organzations to have frequent backups while also saving time. Before backing up data, it should first be classify and prioritize according to its importance. Database backup should also be incorporated to save data related to the customers which can be required in the future in case of loss of current database data.
Data Encryption: All the data on the organizations network and devices should always be encrypted. Full disk encryption should be mandated for BYOD devices. All the network transmission should be done using secure protocols like TLS SSL.

Step 5: Develop a phishing avoidance strategy

Educate/Train Employess: The company should educate employees about social engineering tactics that the attackers employ. Also the employees should be trained how to spot phishing emails. This can be done by sending simulated phishing attacks to employees email to check to see if employees fall for the trap or not. If an employee clicks on the simulated phishing email, that employee should enrolled into the training for spotting the phishing emails.

Step 6: Create a personal device policy

BYOD Policy: With BYOD policy, Sam's Scoops' employees can bring their own devices to connect to company's network and can use it for work related task. These devices can also be used for remote connections. However, these devices are potential threat vectors can be exploited by malicious actor. It is very important for Sam's Scoops to secure these devices so they don't pose any risk of data breach.
Scope: The scope of the BYOD policy is to secure all the employees' personal devices that will be used on company's network and for work related tasks to reduce the risk of unauthorized access, data breach and operation disruptions. Endpoint security is the main task of the BYOD policy. Under this policy, all the personal devices used by employees for work related tasks needs to have anti-malware softwares installed on their systems. Also, the devices should be configured to do auto updates whenever there is a critical update available for an app or operating system. These devices are only allowed to communicate on secure channel that offers encryption to protect data from malicious actors. All the devices should have the least access required to do the job and the access management should be audited or monitored regularly so as to avoid escalation of privileges.
Mobile Device Management: MDM can be used to remotely control and secure employee devices. This solution centralized the app updates, security configurations and data wipes. Regular updates should be conducted to the appropriate applications. Moreover, blacklisting of unwanted or unsecure apps should be incorporated.
Training: All the employees should be regularly educated about the threats their personal device can pose to the organizations. Moreover, they should be trained to securing these devices to best of their abilities.

Step 7: Implement MFA and biometric security measures

MFA: All the devices in the Sam's Scoops organiztion must be protected using MFA to only allow the authorized access to appropriate authenticated identities. Microsoft Azure Directory can be solution to authenticate and authorize identities through a centralized system. It also uses identity federation technology to allow single sign on for multiple resources thus reducing the chances of failed attempts and to remember a number of passwords.
Biometric measures: Most of the devices nowadays have biometric security feature. The use of this feature can add an extra layer of security. Unlike passwords, the biometric security cannot be guessed by an hacker thus making it harder for the malicious actors to steal the sensitive info.

Step 9:Propose a plan for continuous monitoring and improvement

IDPS: The use of IDPS will allow Sam's Scoops to detect possible intrusions into the company's network which will enable them to take the appropriate measures in a timely manner to stop the unauthorized access.
Network monitors and SIEM tools: The company can constantly monitor network traffic by using different tools like WireShark, tcpdump and Ettercap. These tools will allow the network traffic detection in real time. They will allow Sam's Scoops to capture network traffic which can be analyzed by them to see any possible attempts of intrusion or data exfiltration. SIEM tools will Sam's Scoops to have network monitor data in an centralized app with dashboards which sends alerts about possible intrusions.