Review the following scenario. Then complete the step-by-step instructions.

You are a newly hired cybersecurity analyst for an e-commerce company. The company stores information on a remote database server, since many of the employees work remotely from locations all around the world. Employees of the company regularly query, or request, data from the server to find potential customers. The database has been open to the public since the company's launch three years ago. As a cybersecurity professional, you recognize that keeping the database server open to the public is a serious vulnerability.

You are tasked with completing a vulnerability assessment of the situation to communicate the potential risks to decision makers at the company. You must create a written report that explains how the vulnerable server is a risk to business operations and how it can be secured.

Vulnerability Assessment Report

1st January 20XX

System Description

The server hardware consists of a powerful CPU processor and 128GB of memory. It runs on the latest version of Linux operating system and hosts a MySQL database management system. It is configured with a stable network connection using IPv4 addresses and interacts with other servers on the network. Security measures include SSL/TLS encrypted connections.

Scope

The scope of this vulnerability assessment relates to the current access controls of the system. The assessment will cover a period of three months, from June 20XX to August 20XX. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

The purpose of this vulnerability assessment is to identify and evaluate potential risks in the access controls of the company's database server, which is critical for supporting global operations and secure data handling. The database server stores valuable customer and business data, providing essential information to support customer targeting and operations. Securing this data is paramount to maintaining customer trust and compliance with security standards. If compromised or disabled, the server could disrupt business continuity, damage the company’s reputation, and result in significant financial and operational losses. This

assessment, guided by NIST SP 800-30 Rev. 1, aims to provide actionable recommendations to strengthen the system's security and protect its assets.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Outsider (Hacker, Hacktivist, or Advanced Persistent Threat [APT])	• Rationale: Since the database server is publicly accessible and holds sensitive customer and business data, it's highly vulnerable to outsider threats. Attackers from outside the organization, such as hackers or hacktivists, are likely to target this server, either for data exfiltration or to disrupt operations. APTs could also attempt to compromise the server through persistent and sophisticated attacks, seeking prolonged access to sensitive information. • Impact: If these external attackers gain unauthorized access, they could exfiltrate or tamper with data, impacting business continuity and causing significant reputational and financial harm.	*3*	*3*	*9*
Standard User (Employee or Customer)	• Rationale: Employees and customers with access to the system could accidentally or intentionally compromise data. The fact that employees regularly query this database to	*2*	*2*	*4*

	identify potential customers increases the likelihood of accidental exposure or misuse of information. Additionally, any misconfigurations in access permissions could unintentionally expose sensitive data to users with insufficient security awareness. ● Impact: Internal users with access to the server could inadvertently expose or alter data, leading to a data breach or compromising data integrity. These actions could violate privacy standards and harm the company's reputation.			
Operational Environment (Power Outage, Network Failure)	● Rationale: Given that the server relies on a stable network connection and supports global operations, it's crucial to consider environmental or operational threats like network failures, power outages, or hardware malfunctions. These factors could disrupt access to the server, affecting the company's ability to retrieve data. ● Impact: An operational failure could disable the server temporarily, affecting employees' ability to access critical information, delaying business processes, and	*1*	*1*	*2*

	potentially causing financial losses due to downtime.			

Approach

Selecting potential threats for this vulnerability assessment focused on identifying risks most relevant to the public accessibility and operational importance of the database server, as guided by NIST SP 800-30 Rev. 1. We considered threat sources that could realistically exploit the server's configuration and user access patterns, including both external and internal actors. **Outsider threats** (e.g., hackers or APTs) were chosen due to the server's exposure to the internet, while **standard user threats** were included because employees frequently access the server, increasing the chance of accidental misuse or exposure. **Operational environment threats** were selected to account for potential disruptions like network or power outages that could affect business continuity. This selection ensures a balanced view of human and non-human threats that align with the system's risk profile.

Remediation Strategy

To remediate and mitigate risks to the database server, several security controls can be implemented. Applying the **principle of least privilege** ensures that employees only have access to the specific data necessary for their roles, reducing exposure in case of accidental misuse. A **defense-in-depth** approach, incorporating firewalls and access restrictions, protects the server from external attackers by layering security measures. Implementing **multi-factor authentication (MFA)** strengthens user verification, mitigating risks from compromised credentials. Finally, using the **Authentication, Authorization, and Accounting (AAA) framework** will enhance monitoring, controlling access, and logging user activities, enabling quick response to potential security incidents. Together, these controls create a comprehensive approach to protect the database server and the sensitive data it stores.