# Vulnerability Assessment Report

1st January 20XX

## Scenario

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.

### 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 database server is valuable to the business because it stores large amounts of the company's data on its network. The server data related to the business, its customers, campaigns, and analytics that help monitor the performance of marketing efforts.

## Risk Assessment

| Threat source | Threat event | Likelihood | Severity | Risk |
|---|---|---|---|---|
| Customer | Accidentally tampering with sensitive information | *1* | *3* | *3* |
| Hacker | Steal data and sensitive information by exploiting cyber resources | 3 | *3* | *9* |
| Employee | Accidentally alter data, disrupting company operations | *2* | *3* | *6* |

## Approach

Risks considered the data storage and management methods of the business. The likelihood of a threat occurrence and the impact of these potential events were weighed against the risks to day-to-day operational needs.

## Remediation Strategy

Implementation of authentication, authorization, and auditing mechanisms to ensure that only authorized users access the database server. This includes using strong passwords, role-based access controls, and multi-factor authentication to limit user privileges. Encryption of data in motion using TLS instead of SSL. IP allow-listing to corporate offices to prevent random users from the internet from connecting to the database.

# NIST SP 800-30 Rev. 1

---

## Guide to assessing risk

NIST SP 800-30 is a publication that provides guidance on performing risk assessments. It outlines strategies for identifying, analyzing, and remediating risks. Organizations use NIST SP 800-30 to gain insights into the potential likelihood and severity of risks—helping them make informed decisions about allocating resources, implementing controls, and prioritizing remediation efforts.

This four page document is adapted from NIST SP 800-30 Rev. 1. The term "Rev. 1" signifies that it is the first updated version of this publication. NIST occasionally revises its documents to incorporate new information, reflect changes in technology and regulatory requirements, or address feedback.

**Note:** NIST's Computer Security Resources Center contains more information on SP 800-30 Rev. 1.

## Threat sources

NIST SP 800-30 defines and categorizes threat sources as entities or circumstances that can negatively impact an organization's information systems. This information is useful for identifying and assessing potential risks. When referencing it, consider the intent/capabilities of either internal and external threat sources.

**Note:** The following table lists a few possible *threat sources* that could compromise a publicly accessible database server.

| Type | Examples | Description |
|---|---|---|
| **Human** | *Standard user*<br>• Employee<br>• Customer<br>*Privileged user*<br>• System administrator<br>*Group*<br>• Competitor<br>• Supplier<br>• Business partner<br>• Nation state<br>*Outsider*<br>• Hacker<br>• Hacktivist<br>• Advanced persistent threat (APT) | Threats arising from individuals or groups who might purposefully or accidentally exploit cyber resources. For example, they might alter data in a way that negatively impacts the company. Alternatively, they might intentionally steal data and damage business equipment. |

| | | |
|---|---|---|
| **Technological** | *Hardware*<br>• Storage<br>• Processing<br>• Communications<br>*Software*<br>• Operating system(s)<br>• Networking<br>• Malicious software | Threats that originate from non-human factors. For example, failures of equipment due to aging, resource depletion, or other circumstances. |
| **Environmental** | *Operational environment*<br>• Temperature controls<br>• Humidity controls<br>• Faulty power supplies<br>*Natural hazards*<br>• Power outages<br>• Extreme weather events | Threats that arise from accidental, non-human factors. For example, equipment failures caused by the operational environment. |

## Threat events

NIST SP 800-30 defines and categorizes threat events as actual instances where a threat source exploits a vulnerability and causes damage or harm to an organization's information systems. This information is useful for gaining insights into the types of risks that assets face. More effective controls and countermeasures can be identified by understanding possible threat events,

**Note:** The following table lists just a few possible *threat events* that could compromise a publicly accessible database server.

| **Examples** | **Description** |
|---|---|
| Perform reconnaissance and surveillance of organization | Threat source examines and assesses the company's vulnerabilities over time using various tools (e.g., scanning, physical observation). |
| Obtain sensitive information via exfiltration | Threat source installs malicious software on organizational systems to locate and acquire sensitive information. |
| Alter/Delete critical information | Threat source alters or deletes data that is critical to day-to-day business operations. |

| | |
|---|---|
| Craft counterfeit certificates. | Threat source compromises a certificate authority to make their connections appear legitimate. |
| Install persistent and targeted network sniffers on organizational information systems. | Threat source installs software designed to collect (sniff) network traffic over a continued period of time. |
| Conduct Denial of Service (DoS) attacks. | Threat source sends automated, excessive requests to overwhelm the system's operating capabilities. |
| Disrupt mission-critical operations. | Threat source compromises the integrity of information in such a way that prevents the business from carrying out critical operations. |
| Obfuscate future attacks. | Threat source takes actions to inhibit the effectiveness of the intrusion detection systems or auditing capabilities at the company. |
| Conduct "man-in-the-middle" attacks. | Threat source eavesdrops on sessions between internal and external systems. Later, they relay messages between organizational and external systems that make them believe they're talking directly to each other over a private connection. |

## Likelihood of a threat event

In general, the *likelihood* of a threat event should be a score based on a combination of factors. For example, any available evidence that you have, prior experience, and your expert judgment.

Consider the intent/capabilities of a threat source and potential threat events when producing a likelihood score.

| Qualitative values | Quantitative values | Description |
|---|---|---|
| High | 3 | Threat source is almost certain to initiate a security event. An event could have multiple, severe, or catastrophic effects on business operations and assets. |
| Moderate | 2 | Threat source is somewhat likely to initiate a security event. An event could significantly reduce |

| | | |
|---|---|---|
| | | the functionality of organizational operations and assets. |
| Low | 1 | Threat source is highly unlikely to initiate a security event. An event could have minor, negligible effects on business operations and assets. |

## Severity of a threat event

In general, the *severity* of a threat event is a measure of its potential impact to business operations. For example, would the event cause a business function to stop entirely? Might it temporarily disrupt a business process and go unnoticed?

Consider the business impact of *threat events* when producing a severity score.

| **Qualitative values** | **Quantitative values** | **Description** |
|---|---|---|
| High | 3 | Threat source is almost certain to initiate a security event. An event could have multiple, severe, or catastrophic effects on business operations and assets. |
| Moderate | 2 | Threat source is somewhat likely to initiate a security event. An event could significantly reduce the functionality of organizational operations and assets. |
| Low | 1 | Threat source is highly unlikely to initiate a security event. An event could have minor, negligible effects on business operations and assets. |