Cybersecurity Analyst Internship

Task Report

atalmamun@gmail.com

Task No: 28

Credit: Offensive Security

Table of Contents

1.0 EncryptEdge Labs Internship Task Report **3**
1.1 Introduction 3
1.2 Objective 3
1.3 Requirements 4
2.0 Introduction to Risk Assessment **4**
2.1 Importance of Risk Assessment in Cybersecurity 4
2.2 Key Components of a Risk Assessment 5
3.0 Chosen Scenario **7**
3.1 Organization Overview 7
3.2 Environment and Infrastructure 7
3.3 Key Information Assets 8
3.4 Common Threats 8
3.5 Known or Potential Vulnerabilities 9
4.0 Asset Identification **9**
4.1 Asset Table 10
4.2 Asset Categorization Rationale 11
5.0 Threat and Vulnerability Analysis **11**
5.1 Threat and Vulnerability Table 11
5.2 Summary of Findings 14
6.0 Risk Assessment Calculation **14**
6.1 Risk Calculation Table 14
6.2 Observations 16
7.0 Risk Prioritization **16**
7.1 Prioritized Risk Table 16
7.2 Risk Response Strategy 18
8.0 Conclusion **18**

1.0 EncryptEdge Labs Internship Task Report

1.1 Introduction

Risk assessment is a fundamental process within cybersecurity that enables organizations to identify, evaluate, and manage potential risks to their information systems and assets. As cyber threats continue to evolve in complexity and frequency, the importance of risk assessment has grown significantly. It allows organizations to proactively uncover vulnerabilities, determine the likelihood of potential threats, and assess the potential impact of security incidents. By systematically analyzing these elements, organizations can prioritize their security efforts and allocate resources more effectively to mitigate high-risk areas. This process plays a crucial role in enhancing the overall security posture of an organization and ensuring the confidentiality, integrity, and availability of critical information.

1.2 Objective

The primary objective of this task is to understand and apply the principles of cybersecurity risk assessment. Through the analysis of a hypothetical scenario, this report aims to:

- Explain the key components of risk assessment, including assets, threats, vulnerabilities, and impact.

- Conduct a structured risk assessment for a fictional organization by identifying critical assets, associated threats, and weaknesses.

- Evaluate the likelihood and impact of potential risks.

- Prioritize risks to support effective mitigation planning and informed decision-making.

1.3 Requirements

To successfully complete this task, the following requirements are addressed:

- A foundational understanding of risk assessment and its importance in cybersecurity.
- Use of a recognized risk assessment framework or template (e.g., NIST Risk Management Framework).
- Selection of a realistic hypothetical scenario for risk assessment.
- Identification and categorization of information assets based on their criticality.
- Analysis of threats and vulnerabilities related to the identified assets.
- Risk level calculation using a defined methodology (e.g., Likelihood × Impact).
- Prioritization of identified risks based on calculated severity.
- Presentation of findings in a clear, structured, and professionally formatted report.

2.0 Introduction to Risk Assessment

Risk assessment is a critical component of cybersecurity that allows organizations to systematically identify and manage risks to their information assets. It serves as the foundation for effective risk management, enabling informed decision-making, efficient allocation of security resources, and proactive protection against cyber threats.

2.1 Importance of Risk Assessment in Cybersecurity

In today’s interconnected digital landscape, organizations face a wide range of cyber threats, from malware and phishing to insider attacks and data breaches. Without a structured approach to assessing and addressing these risks, organizations may leave critical assets exposed to exploitation.

Risk assessment provides a framework for understanding potential security challenges before they cause damage. It helps organizations:

- Understand their threat landscape.
- Identify weaknesses in their systems and processes.
- Evaluate the potential consequences of security incidents.
- Prioritize security controls and mitigation strategies based on risk severity.

This proactive approach not only minimizes the likelihood of incidents but also reduces the financial, reputational, and operational impact when incidents do occur.

2.2 Key Components of a Risk Assessment

A comprehensive risk assessment typically involves the following core components:

2.2.1 Assets

Assets refer to anything of value to the organization that must be protected. These may include:

- Information assets (e.g., customer data, intellectual property)
- Hardware and software systems
- Business processes
- Personnel and facilities

Identifying and classifying assets is the first step in understanding what needs to be protected.

2.2.2 Threats

Threats are potential events or actions that could exploit vulnerabilities and cause harm to the organization. Examples include:

- Cyberattacks such as malware infections or ransomware
- Human threats such as phishing or insider sabotage
- Environmental threats like fire, flood, or power outage

2.2.3 Vulnerabilities

Vulnerabilities are weaknesses or gaps in a system or process that can be exploited by threats. Common vulnerabilities include:

- Outdated software or unpatched systems
- Weak authentication mechanisms
- Poor access controls or lack of employee training

2.2.4 Impact

Impact refers to the consequences or damage that could occur if a threat successfully exploits a vulnerability. Impacts may be:

- Financial (e.g., loss of revenue, regulatory fines)
- Operational (e.g., service disruption)
- Reputational (e.g., loss of customer trust)

Understanding the potential impact is crucial for prioritizing risks and developing mitigation strategies.

3.0 Chosen Scenario

To perform the risk assessment, a hypothetical organization has been selected: a **small e-commerce business** that operates an online retail store. This organization relies heavily on digital infrastructure to manage customer data, process transactions, and maintain business operations.

3.1 Organization Overview

The chosen organization is a small-to-medium-sized online store specializing in electronics and accessories. It serves customers globally and conducts all sales through its website. The business operates with a small IT team responsible for website management, cybersecurity, and system maintenance.

3.2 Environment and Infrastructure

The organization's digital environment consists of:

- A web-based e-commerce platform hosted on cloud servers.

- A customer database storing personal and payment information.
- An internal employee system for administrative tasks and order fulfillment.
- Payment gateway integrations with third-party financial service providers.

3.3 Key Information Assets

The critical information assets of the organization include:

- **Customer Personal Data** (names, addresses, email addresses, etc.)
- **Payment Information** (credit card data, billing information, stored securely)
- **Web Server and Application Code** (platform source code and backend logic)
- **Employee Credentials** (usernames and passwords for admin access)
- **Sales and Transaction Records** (stored for business analytics and financial reporting)

3.4 Common Threats

Given the digital nature of the business, common threats include:

- **Phishing Attacks** targeting customers and employees.
- **SQL Injection** or other web-based attacks on the online store.

- **Data Breaches** through unauthorized access to the customer database.
- **DDoS Attacks** to disrupt online services.
- **Insider Threats** from disgruntled employees or misconfigured access rights.

3.5 Known or Potential Vulnerabilities

Some vulnerabilities that may exist in the current environment are:

- **Outdated CMS or e-commerce platform plugins**.
- **Lack of Multi-Factor Authentication (MFA)** for admin users.
- **Weak password policies** for employee accounts.
- **Inadequate logging and monitoring** of server activity.
- **Improper encryption** or storage of sensitive customer data.

4.0 Asset Identification

Identifying and categorizing critical assets is a fundamental step in the risk assessment process. For the chosen e-commerce business scenario, the following table outlines the primary information assets along with their assigned criticality levels based on their importance to the organization’s operations and data security.

4.1 Asset Table

Asset	**Description**	**Criticality Level**
Customer Personal Data	Includes names, email addresses, phone numbers, and shipping addresses.	Critical
Payment Information	Credit card and billing information collected during transactions.	Critical
E-commerce Web Server	Hosts the website and handles customer interaction and transactions.	High
Application Source Code	Backend and frontend codebase that powers the online store.	High
Employee Credentials	Admin and staff login details used for internal access and site management.	High
Transaction and Order Records	Historical sales data used for reporting, accounting, and analytics.	Medium
Product Inventory Database	Digital catalog of products available for sale including prices and stock data.	Medium
Email and Communication System	Used for internal communication and customer service interactions.	Low

4.2 Asset Categorization Rationale

- **Critical** assets include any information that, if compromised, would result in major financial, legal, or reputational damage, particularly sensitive customer data and payment details.

- **High** assets are essential for daily operations and security (e.g., web server, employee accounts).

- **Medium** assets support operations but do not pose immediate critical risk if temporarily unavailable.

- **Low** assets are non-sensitive and would have minimal impact on core operations if compromised.

5.0 Threat and Vulnerability Analysis

This section analyzes the potential threats and vulnerabilities related to each key asset of the hypothetical e-commerce business. Understanding these relationships helps in assessing the risk level and planning effective mitigation strategies.

5.1 Threat and Vulnerability Table

Asset	Threats	Vulnerabilities

Customer Personal Data	- Data breach - Unauthorized access	- Weak access controls - Lack of data encryption - Insecure storage or backups
Payment Information	- Credit card fraud - Interception of payment data	- Insecure payment gateway integration - Outdated SSL/TLS - Absence of PCI-DSS compliance
E-commerce Web Server	- DDoS attacks - Web application exploits (e.g., XSS)	- Outdated server software - Lack of traffic filtering - Unpatched CMS vulnerabilities
Application Source Code	- Code injection - Exploitation of logic flaws	- Lack of secure coding practices - Poor version control - Public exposure of sensitive files
Employee Credentials	- Credential theft - Insider threats	- Weak passwords - No multi-factor authentication (MFA) - Shared accounts

Transaction Records	- Data leakage - Tampering of transaction history	- Inadequate logging and access controls - No integrity checks
Inventory Database	- Unauthorized data manipulation - Ransomware attacks	- No regular backups - Poor access segregation - Lack of database activity monitoring
Email Communication System	- Phishing - Email spoofing	- No SPF/DKIM records - Inadequate spam filtering - Untrained staff on phishing recognition

5.2 Summary of Findings

The analysis shows that many of the organization’s critical and high-priority assets are exposed to threats due to common cybersecurity weaknesses. These include outdated systems, poor authentication mechanisms, and insufficient encryption or access controls. The presence of these vulnerabilities increases the risk of data breaches, service disruptions, and financial loss.

6.0 Risk Assessment Calculation

To quantify and evaluate the cybersecurity risks associated with the identified assets, each threat is assessed based on its **likelihood** of occurrence and the **impact** it would have if it materialized. A simple risk calculation formula is used:

Risk Level=Likelihood×Impact

Where both **Likelihood** and **Impact** are rated on a scale of 1 (Low), 2 (Medium), and 3 (High). The resulting **Risk Level** values range from 1 to 9 and are categorized as follows:

- **1–3**: Low Risk
- **4–6**: Medium Risk
- **7–9**: High Risk

6.1 Risk Calculation Table

Asset	Threat	Likelihood	Impact	Risk Level	Risk Category
Customer Personal Data	Data breach	3 (High)	3 (High)	9	High
Payment Information	Credit card fraud	3 (High)	3 (High)	9	High
Web Server	DDoS attack	2 (Medium)	3 (High)	6	Medium
Application Source Code	Code injection	2 (Medium)	2 (Medium)	4	Medium
Employee Credentials	Credential theft	3 (High)	2 (Medium)	6	Medium
Transaction Records	Data leakage	2 (Medium)	2 (Medium)	4	Medium
Inventory Database	Ransomware	2 (Medium)	2 (Medium)	4	Medium
Email System	Phishing attack	3 (High)	1 (Low)	3	Low

6.2 Observations

The most critical risks identified are:

- Unauthorized access to **customer personal data** and **payment information**, both of which scored a maximum risk level of **9 (High)** due to the severe consequences of breaches and the high probability of such attacks occurring in the e-commerce sector.

- Other assets such as **employee credentials** and **web server** also show significant risks that require mitigation, although at slightly lower levels.

7.0 Risk Prioritization

Following the risk calculation, it is essential to prioritize the identified risks to ensure that mitigation efforts focus on the most critical areas first. Risks are ranked from highest to lowest based on their calculated severity (Risk Level), and those with a **High Risk** rating are flagged for immediate action.

7.1 Prioritized Risk Table

Priority	Asset	Threat	Risk Level	Risk Category	Action Required

1	Customer Personal Data	Data breach	9	High	Immediate mitigation
2	Payment Information	Credit card fraud	9	High	Immediate mitigation
3	Web Server	DDoS attack	6	Medium	Short-term mitigation
4	Employee Credentials	Credential theft	6	Medium	Short-term mitigation
5	Application Source Code	Code injection	4	Medium	Medium-term mitigation
6	Transaction Records	Data leakage	4	Medium	Medium-term mitigation
7	Inventory Database	Ransomware attack	4	Medium	Medium-term mitigation
8	Email System	Phishing attack	3	Low	Routine monitoring and awareness

7.2 Risk Response Strategy

Based on the prioritization, the following risk response strategies are recommended:

- **High-Risk Items (Priority 1–2)**:
  Require **immediate remediation**. Implement robust access controls, encryption, and compliance with data protection standards such as **PCI-DSS** and **GDPR**.

- **Medium-Risk Items (Priority 3–7)**:
  Should be addressed in the **short- to medium-term**. Apply software updates, improve employee authentication processes, and strengthen secure coding practices.

- **Low-Risk Item (Priority 8)**:
  Can be managed through **ongoing monitoring**, employee phishing training, and email security enhancements such as SPF/DKIM implementation.

8.0 Conclusion

Conducting a thorough risk assessment is an essential practice for any organization aiming to protect its information assets and maintain operational resilience. Through this exercise, a structured analysis was performed on a hypothetical e-commerce business to identify, evaluate, and prioritize cybersecurity risks.

The assessment revealed that **customer personal data** and **payment information** are the most critical assets, with the highest risk levels due to their sensitivity and the high probability of targeted attacks. Additional risks were identified across infrastructure components such as the **web server**, **employee credentials**, and **application code**, highlighting areas where improved security controls are necessary.

This risk assessment process provided valuable insights into the organization's threat landscape and underscored the importance of:

- Implementing layered security controls,
- Regularly updating software and infrastructure,
- Enforcing strong authentication policies,
- Continuously monitoring systems for vulnerabilities and unusual activity.

More broadly, this exercise emphasized that **risk assessment is not a one-time event**, but a continuous cycle that must adapt to emerging threats, evolving technologies, and organizational changes. By routinely assessing and addressing risks, businesses can enhance their security posture, reduce exposure, and build trust with customers and stakeholders.

EncryptEdge Labs

This Internship Task report was developed on [April, 29, 2025]

By:

atalmamun@gmail.com