COIT20265: Networks and Information Security Project (HT1, 2025)

**Project Plan  
Security Posture & Risk Assessment**

|  |  |
| --- | --- |
| Mian Fazal Ur Rehman | 12224256 |
| Theofill Jake Gepila Bautista | 12243209 |
| Sushila Karmacharya | 12205881 |
| Shihan Deshapriya Navimana Vidanage | 12231034 |

Tutor: **Azmat Ullah**

Unit Coordinator:  **Yufeng Lin**

**Overview**

**Project Topic**  
This project focuses on checking about Security Posture and Risk Assessment on how secure IT systems are and find ways to make them safer. The goal is to look at risks, identify weaknesses and provide recommendations and suggest improvements to protect against threats.

**Project, Aim**  
We want to help an organization understand its security risks and improve its protection against threats. By doing a risk assessment, we will highlight problem areas and suggest ways to fix them.

**Problem Statement**   
Companies face increasing risks from cyber threats like hacking, malware, and data leaks. Many of the companies don’t have clear strategy to deal with these issues. This project will analyse or examine their security, identify weak spots, and suggest solutions to make their systems safer.

**In Scope**

* We will review the company’s IT security setup to understand how well it protects against cyber threats.
* We will identify risks, weaknesses, and areas that need improvement.
* We will examine the company's security policies and how well they follow industry standards.
* We will suggest practical steps to strengthen security and reduce risks.
* We will create a detailed risk assessment report with all our findings and recommendations.

**Out of Scope**

* We won’t make any security changes or fixes ourselves.
* We won’t perform hacking, penetration testing, or any hands-on security testing.
* We won’t look at physical security risks, such as building access or surveillance systems.

**Who Will Benefit**

This project is useful for companies and organisations that want to improve their cybersecurity. The findings from our final report will help the company to make their systems safer and protect against cyber threats.

**Tasks**

|  |  |  |
| --- | --- | --- |
| **Task** | **Description** | **Deliverable(s)** |
| Understanding Requirements | Find out what security needs the organization has and what they are trying to protect. | Security requirements document |
| Identifying Assets | List important IT systems, data, and other assets that need protection. | Asset inventory list |
| Finding Potential Threats | Look at common cybersecurity risks like hacking, phishing, and malware. | Threat report |
| Checking for Weaknesses | Identify weak points in the network, applications, and data protection. | Vulnerability assessment report |
| Assessing Risks | Analyze how serious the risks are and their possible impact. | Risk assessment report - Risk matrix |
| Reviewing Security Measures | Check what security protections are already in place and if they follow industry standards. | Security controls report - Compliance checklist |
| Making Recommendations | Suggest practical ways to improve security and reduce risks. | Security improvement plan |
| Reviewing Policies | Check the organization’s security policies and suggest any necessary changes. | Policy review document |
| Planning for Security Incidents | Create a plan for how the company should respond to cyber attacks. | Incident response plan |
| Final Report & Presentation | Summarize all findings and recommendations in a final report and presentation. | Final report - Presentation slides |

**Roles & Justification**

|  |  |  |
| --- | --- | --- |
| **Student Name** | **Role** | **Justification** |
| Mian Fazal ur Rehman | Project Coordinator | Oversees project planning, ensures document structure aligns with the requirements, and manages overall workflow. Responsible for compiling and finalizing the project plan. |
| Theofill Jake Gepila Bautista | Security Assessment Specialist | Conducts interviews with IT and security personnel to evaluate the organization’s security posture. Gathers key insights for risk analysis and documentation. |
| Sushila Karmacharya | Risk Analyst | Identifies security risks related to network infrastructure, data, and identities. Develops mitigation strategies and ensures compliance with best practices. |
| Shihan Deshapriya Navimana Vidanage | Technical Lead & Compliance Analyst | Handles technical aspects such as resource allocation, scheduling, and ethical considerations. Ensures the project follows industry standards and professional guidelines. |

**Responsibilities**

| **Task** | **Technical Lead** | **Reviewer** |
| --- | --- | --- |
| Project Planning & Documentation | Mian Fazal Ur Rehman | Theofill Jake Gepila Bautista |
| Security Posture Assessment & Stakeholder Interviews | Theofill Jake Gepila Bautista | Sushila Karmacharya |
| Risk Analysis & Mitigation Strategies | Sushila Karmacharya | Shihan Deshapriya Navimana Vidanage |
| Technical Implementation, Scheduling & Compliance | Shihan Deshapriya Navimana Vidanage | Mian Fazal Ur Rehman |
| Report Writing & Final Review | Mian Fazal Ur Rehman | Sushila Karmacharya |
| Presentation Preparation | Theofill Jake Gepila Bautista | Shihan Deshapriya Navimana Vidanage |

**Resource Requirements**

The following resources are required to conduct the security posture assessment and risk analysis effectively. The resources are categorized into In-Kind (already available), Cash (to be purchased), and Personnel (effort estimation).

**In-Kind Resources (Existing Tools & Services)**

| **Resource** | **Justification** | **Cost/License** |
| --- | --- | --- |
| Wireshark | Used for packet capture and network traffic analysis during security assessment. | Free (GNU GPL2) |
| Nmap | Network scanning tool to identify open ports and potential vulnerabilities. | Free (Open Source) |
| Kali Linux | Security testing platform with pre-installed penetration testing tools. | Free (Open Source) |
| Microsoft Azure (Trial) | Cloud environment for simulating security controls and network configurations. | Free (Student Trial) |
| Virtual Machines (VMs) | Used to simulate different attack scenarios and assess security defences. | Available through University Lab |

**Cash Resources (Paid Licenses & Subscriptions)**

| **Resource** | **Justification** | **Estimated Cost** |
| --- | --- | --- |
| Premium SIEM Tool (Splunk/QRadar) | Security Information and Event Management (SIEM) tool for log analysis and threat detection. | $300 (Trial/Paid License) |
| Penetration Testing Tools (Burp Suite Pro) | Advanced security testing for web applications and APIs. | $400 (Annual License) |
| Cloud Security Service (AWS GuardDuty) | Used for detecting security threats in cloud environments. | $250 (Usage-Based) |

**Personnel Resources (Time & Effort Estimation)**

| **Resource** | **Justification** | **Estimated Cost** |
| --- | --- | --- |
| Security Assessor | Conducts interviews, gathers security posture details, and documents findings. | 80 hours ($50/hr) = $4,000 |
| Risk Analyst | Evaluates risks, analyses vulnerabilities, and provides mitigation strategies. | 90 hours ($50/hr) = $4,500 |
| Technical Lead | Implements project schedule, oversees ethical concerns, and finalizes reports. | 70 hours ($50/hr) = $3,500 |

**Project Risks and Mitigation**

|  |  |  |
| --- | --- | --- |
| **Risk ID** | **Risk** | **Mitigation** |
| R001 | Miscommunication or unclear roles within the team are causing conflicts | * Clearly define and document all team roles and responsibilities at the start of the project. * Implement weekly synchronization meetings to proactively address any emerging concerns. * Establish and adhere to a formal conflict resolution protocol, such as seeking supervisor consultation to resolve disputes efficiently |
| R002 | Technical failures for collaboration tools | * Store files in multi-cloud backups (Google Drive) |
| R003 | Unable to secure a partner organization | * Collaborate with a local small business * Partner with the university’s IT department as a fallback |
| R004 | Lacking stakeholder participation | * Offer flexible interview times via in-person or virtual * Partner with a employee of an organization to encourage participation |
| R005 | Overlapping academic deadlines | * Communicate with team members and create a shared team calendar to track conflicts. |
| R006 | Client withdrawal  mid-project | * Identify a backup organization |

**Schedule**

**A screenshot of a computer

AI-generated content may be incorrect.**

**Ethical and Professional Issues**

|  |  |  |  |
| --- | --- | --- | --- |
| **Risk ID** | **Issue** | **Mitigation** | **ACS Code Reference** |
| E001 | **Informed Consent** (e.g., stakeholders unaware of how interview data will be used | * Provide a participant information sheet explaining the project’s purpose, data usage, and anonymity guarantees. * Obtain signed consent forms before interviews. | Sec. 1.1: Public interest  Sec. 3.1: Confidentiality |
| E002 | **Post-Project Misuse of Risk Report** | * Apply data retention policy – delete data 30 days post-project * Add a disclaimer | Sec. 1.2: Intellectual property;  Sec. 3.3: System security. |
| E003 | **Cultural Insensitivity During Interviews** | * Pre-Interview Research about the organization * Used of simple language. Avoid jargons | Sec. 1.4: Respect diversity; Sec. 5.2: Ethical decisions. |
| **E005** | **Data Integrity Risks (manipulation of findings).** | * Use version control (GitHub for scripts, Google Docs with edit history). * Conduct peer reviews of analysis. | Sec. 2.2: Honesty;  Sec. 2.1: Competence. |