

CYBERSECURITY PROJECT

Presented By Sanyukta Kulkarni

MINOR PROJECT :1

Project Overview & SME Cyber Risks

Project Overview

- Cybersecurity Risk Assessment Framework for SMEs
- Identifies threats, evaluates vulnerabilities, and guides mitigation

Common SME Risks

- Phishing, ransomware, insider threats
- Weak passwords & unpatched systems
- Data breaches, cloud misconfigurations, DDoS, third-party risks

Risk Assessment & Evaluation

NIST CSF-Based Model

- Identify – Assets & threats
- Protect – MFA, firewalls, encryption, training
- Detect – Monitoring & anomaly detection
- Respond – Incident handling
- Recover – Backups & continuity

Risk Metric

- $\text{Score} = \text{Likelihood} \times \text{Impact}$
- High-priority: Phishing, ransomware, weak passwords, cloud misconfigurations
- Helps SMEs prioritize security measures

Mitigation, Case Studies & Conclusion

Mitigation Strategies

- Technical: MFA, patching, encryption, backups, network segmentation
- Administrative: Policies, training, vendor checks, incident response
- Physical: Restricted access, CCTV

Case Studies & Findings

- Retail: MFA + segmentation → 90% less unauthorized access
- IT: IAM + logging → secured cloud
- Manufacturing: Backups + protection → fast recovery

Conclusion

- SMEs can improve cybersecurity with structured frameworks
- Best practices: MFA, patching, backups, monitoring, least privilege access

MINOR PROJECT :2

Project Overview & SME Cyber Risks

Project Overview

- Framework to identify, assess, and mitigate cybersecurity risks in SMEs.
- Validated using real-world SME case studies.

Common SME Risks

- Phishing & social engineering
- Ransomware attacks
- Insider threats
- Weak passwords & unpatched systems
- Data breaches & cloud misconfigurations
- DDoS attacks & third-party vendor risks

Risk Assessment Model & Evaluation

NIST CSF-Based Model

- Identify – Assets, threats, vulnerabilities
- Protect – MFA, firewalls, encryption, training
- Detect – Monitoring, anomaly detection
- Respond – Incident handling & containment
- Recover – Backups & business continuity

Risk Evaluation Metric

- Risk Score = Likelihood × Impact
- High-priority threats: Phishing, ransomware, weak passwords, cloud misconfigurations
- Helps SMEs prioritize security investments

Mitigation, Case Studies & Conclusion

Mitigation Strategies

- Technical:* MFA, patching, encryption, backups, network segmentation
- Administrative:* Policies, employee training, vendor checks, incident response
- Physical:* Locked rooms, CCTV, restricted access

Case Studies

- Retail: MFA + segmentation → 90% reduction in unauthorized access
- IT: IAM + logging → secured cloud
- Manufacturing: Backups + endpoint protection → fast ransomware recovery

Conclusion

- SMEs can improve cybersecurity even with limited resources.
- Best practices: MFA, training, patching, backups, monitoring, least privilege access.
- Provides a scalable framework to manage evolving cyber risks.

MAJOR PROJECT

Introduction

Phishing Awareness Simulation Using Social Engineering Techniques

- Phishing is one of the most common cybersecurity threats today.
- Attackers trick users by imitating trusted services to steal information.
- This project simulates a *safe, controlled, ethical phishing scenario* to study:
 - 1) How phishing attacks work
 - 2) How users react
 - 3) How awareness can be improved

Problem & Objectives

Problem Statement

- Humans are the weakest link in cybersecurity.
- Many users fall for phishing emails due to lack of awareness.

Project Objectives

- Understand phishing techniques.
- Design a realistic but harmless phishing email.
- Create a fake login page (no data stored).
- Run a controlled simulation with consent.
- Analyse user behavior & improve awareness.

Simulation & Results

Phishing Simulation Steps

- Shared fake email with link to a demo login page.
- Participants were informed and consented.
- No personal data collected.

Key Results

- 5 participants
- 4 clicked the link (80% click rate)
- 3 attempted to enter data (60% victim rate)
- 0 reported the email (0% reporting rate)

Findings:

- Urgent tone influenced clicks.
- Users with low awareness were more likely to fall for it.

Countermeasures & Conclusion

Prevention Strategies

- Use anti-spam filters, DNS filtering, MFA.
- Conduct regular awareness training.
- Teach users to check URLs, sender address, attachments.
- Follow organizational cybersecurity policies.

Conclusion

- The project shows how easily users can fall for phishing.
- Awareness, training, and strong policies greatly reduce the risk.
- Simulation helps build a stronger cybersecurity culture.

THANKYOU

