Small and Medium Enterprises Cyber Exposure Dashboard

Cyber Risk Visualization and Decision Support Framework for SMEs

Ms. Sowmiya S[#1], Ms. Jenitha Harrys J[#2], Mr. Sajid Hussain M[#3]

Assistant Professor, Department of Computer Science with Cyber Security, Sri Ramakrishna College of Arts & Science, Coimbatore, India

III BSc Computer Science with Cyber Security, Department of Computer Science with Cyber Security, Sri Ramakrishna College of Arts & Science, Coimbatore, India

1ssowmiya@srcas.ac.in 2jenitaharrysj@gmail.com 3sajid29705@gmail.com

Abstract

Small and Medium Enterprises play a vital role in economic growth but often lack adequate cybersecurity infrastructure. Unlike large enterprises, these organizations frequently operate without dedicated security teams, advanced tools, or continuous monitoring systems, making them vulnerable to cyberattacks such as malware, phishing, ransomware, and data breaches. This paper presents the development of a Cyber Exposure Dashboard designed specifically for small and medium enterprises to monitor and manage cyber risk exposure effectively.

The proposed system aggregates cybersecurity data from vulnerability scanning tools, network monitoring systems, and security logs. It analyses risk indicators including exposed services, outdated software, misconfigurations, weak authentication practices, and known vulnerabilities. The processed data is visualized using interactive dashboards and risk indicators that provide clear insights into the organization's security posture. The system prioritizes risks based on severity and potential impact, enabling decision-makers to focus on critical vulnerabilities. By transforming complex technical data into intuitive visual metrics, the dashboard supports informed decision-making for both technical and non-technical stakeholders. The solution is scalable and cost-effective, ensuring accessibility for resource-constrained enterprises.

Overall, the Cyber Exposure Dashboard enhances cyber awareness, reduces security gaps, and strengthens resilience among small and medium enterprises operating in an evolving threat landscape.

Keywords—Cyber Exposure, Risk Dashboard, Vulnerability Analysis, Small and Medium Enterprises, Security Visualization

I. INTRODUCTION

Small and Medium Enterprises increasingly rely on information technology for daily operations, customer engagement, and business growth. While digital adoption improves efficiency and competitiveness, it also increases exposure to cyber threats such as phishing, ransomware, and data breaches. Unlike large organizations, smaller enterprises often operate with limited budgets and minimal cybersecurity expertise, resulting in higher vulnerability to cyber incidents.

Cyber exposure refers to the level of risk an organization faces due to weaknesses in its digital infrastructure, including exposed services, outdated software, misconfigurations, and unpatched vulnerabilities. Identifying and managing these risks remains challenging due to complex security tools and large volumes of data.

To address these challenges, this paper proposes a Cyber Exposure Dashboard that provides a centralized and user-friendly platform to visualize, analyze, and manage cyber risk exposure in real time. The primary objective is to simplify cybersecurity risk management by transforming complex data into actionable insights.

II. LITERATURE REVIEW

Several studies emphasize the cybersecurity challenges faced by small and medium enterprises.

Papathanasiou et al. (2024) propose a customized cybersecurity risk assessment framework derived from international standards and tailored for resource-constrained enterprises. The study highlights the importance of structured risk identification and employee awareness programs.

Idowu (2022) examines digital transformation risks in smaller organizations and emphasizes governance frameworks and scalable security strategies to balance innovation and protection.

The NIST Cybersecurity Framework Quick-Start Guide (2020) provides a structured and accessible cybersecurity model organized around five core functions: Govern, Identify, Protect, Detect, and Respond. It supports incremental improvement for organizations lacking mature cybersecurity programs.aa

These works collectively demonstrate the need for simplified, structured, and visualization-driven cybersecurity management systems for SMEs.

III. PROPOSED SYSTEM

The proposed system introduces a Cyber Exposure Dashboard designed to provide a centralized and real-time view of cybersecurity risk posture.

A. SME Cyber Exposure Dashboard

The system integrates technical vulnerabilities, human behavior risks, and organizational controls into a unified interface. It collects data from network logs, vulnerability scans, phishing simulations, user behavior analytics, and policy compliance checks.

A risk analysis engine evaluates threat likelihood, vulnerability severity, and business impact. Based on this evaluation, the system calculates an overall Cyber Exposure Score along with categorized risk indicators such as phishing susceptibility, patching gaps, and access control weaknesses.

IV. METHODOLOGY

A. System Implementation

The development follows a structured methodology including data collection, preprocessing, feature extraction, exposure analysis, visualization, validation, and testing.

1) Data Collection

Cybersecurity datasets in CSV format are collected and integrated into the dashboard system.

2) Data Preprocessing

Data cleaning involves removing duplicates, handling missing values, and normalizing exposure metrics to ensure reliability.

3) Risk Metric Definition

Key indicators such as total assets, exposure score, vulnerability severity, and risk classification are computed and categorized as Low, Moderate, or High.

4) Exposure Analysis

Statistical techniques identify high-risk assets and evaluate their contribution to overall cyber exposure.

5) Dashboard Development

Visualization tools are used to present Key Performance Indicators, asset distribution charts, and vulnerability comparison graphs.

6) System Validation

Functional and performance testing confirm accurate risk computation and smooth system operation.

V. RESULTS AND DISCUSSION

The dashboard successfully processed representative cybersecurity datasets and generated key security metrics including asset count, exposure levels, vulnerability distribution, and risk classification.

The visualization components transformed complex security data into intuitive charts and indicators, enabling clear interpretation of the organizational security posture. Risk prioritization supported structured remediation planning and efficient resource allocation.

Although the current implementation relies on static datasets, it provides a scalable foundation for future real-time integration and predictive analytics capabilities.

VI. CONCLUSION

The Cyber Exposure Dashboard addresses the growing need for simple and effective cybersecurity risk assessment tools tailored for small and medium enterprises. By integrating exposure metrics, asset analysis, and vulnerability assessment into a unified platform, the system enhances cyber awareness and resilience.

The dashboard supports proactive security management and enables informed decision-making for both technical and non-technical stakeholders. Future enhancements may include real-time monitoring, predictive modeling, and automated remediation guidance to further strengthen enterprise cybersecurity defenses.

REFERENCES

[1] S. Monge and C. E. Caicedo, Cybersecurity Data Science: Methods and Applications, Wiley, 2022.

[2] C. Wong, Security Metrics: A Beginner’s Guide, 2nd ed., McGraw Hill, 2023.

[3] M. G. Trenca, Cyber Risk Oversight: A Framework for Organizational Security, Springer, 2023.

[4] A. Hoog and R. Smith, SME Cybersecurity: A Practical Guide, Apress, 2024.
[5] E. D. Knapp and R. Samani, Applied Cybersecurity and the Smart Grid, Elsevier, 2024.
[6] A. Hudson and S. Andrews, Visualizing Cybersecurity: A Strategic Guide to Dashboards and Metrics, CRC Press, 2025.
[7] S. D. Wolthusen, Practical Cyber Intelligence, Wiley, 2025.
[8] S. Lahiri and D. Halder, Cyber Security Analytics, Springer, 2025.
[9] G. Webster and N. Hull, AI in Cybersecurity: Defending Small and Medium Enterprises, CRC Press, 2026.
[10] M. J. Brooks, Cyber Dashboards and Metrics, Apress, 2026.