AI CAREER FOR WOMEN
Commerce

CYBER RISK ANALYSIS

A Project Report
submitted in partial fulfillment of the requirements
of
AICW project.

by

Drashti Upadhyay drashtiupadhyay912@gmail.com
Kiya Shah shahkiya52@gmail.com

Under the Guidance of
Jyoti Ma'am

ACKNOWLEDGEMENT

We sincerely thank everyone who supported us during this project.

We are deeply grateful to our guide, Jyoti Ma'am, for her invaluable guidance and constant encouragement. Her thoughtful feedback and constructive advice helped shape this work. Her trust in our abilities motivated us throughout this journey. Under her mentorship, we have grown both academically and professionally.

We also thank our peers and the institution for providing a supportive learning environment.

ABSTRACT

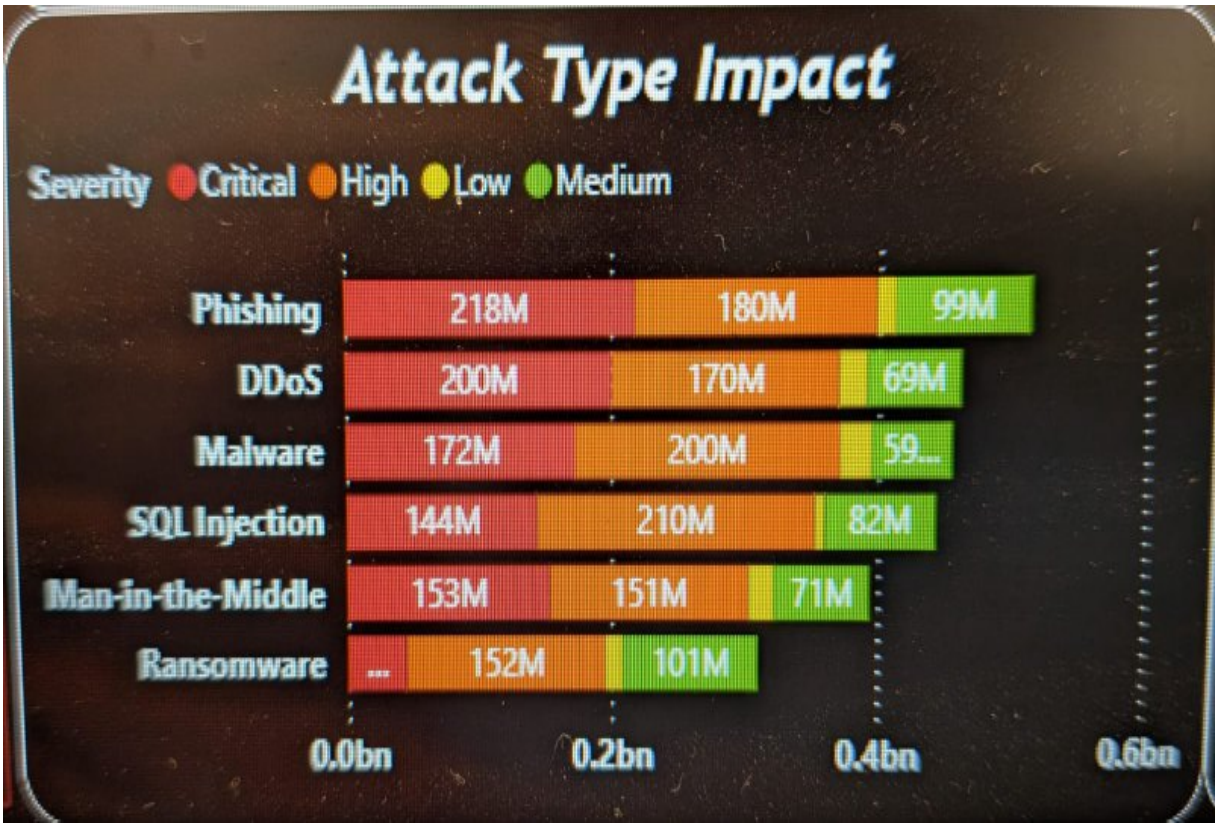
As more businesses go digital, they face growing cyber threats that can cause serious harm. This project, Cyber Risk Analysis, tackles this challenge by creating a visual dashboard to study cyber incidents. We examined data across attack types, regions, industries, and types of computer systems.

Our main goal was to spot high-risk areas, understand attack patterns, and measure impacts in a clear, visual way. The dashboard uses charts, graphs, and maps to make complex data easy to grasp.

Key findings show that phishing and malware attacks cause the most financial damage. The healthcare and banking sectors are most vulnerable,

and hybrid computer systems face higher losses than cloud-only setups. This project confirms that visual, data-driven tools are essential for smart and proactive cybersecurity planning.

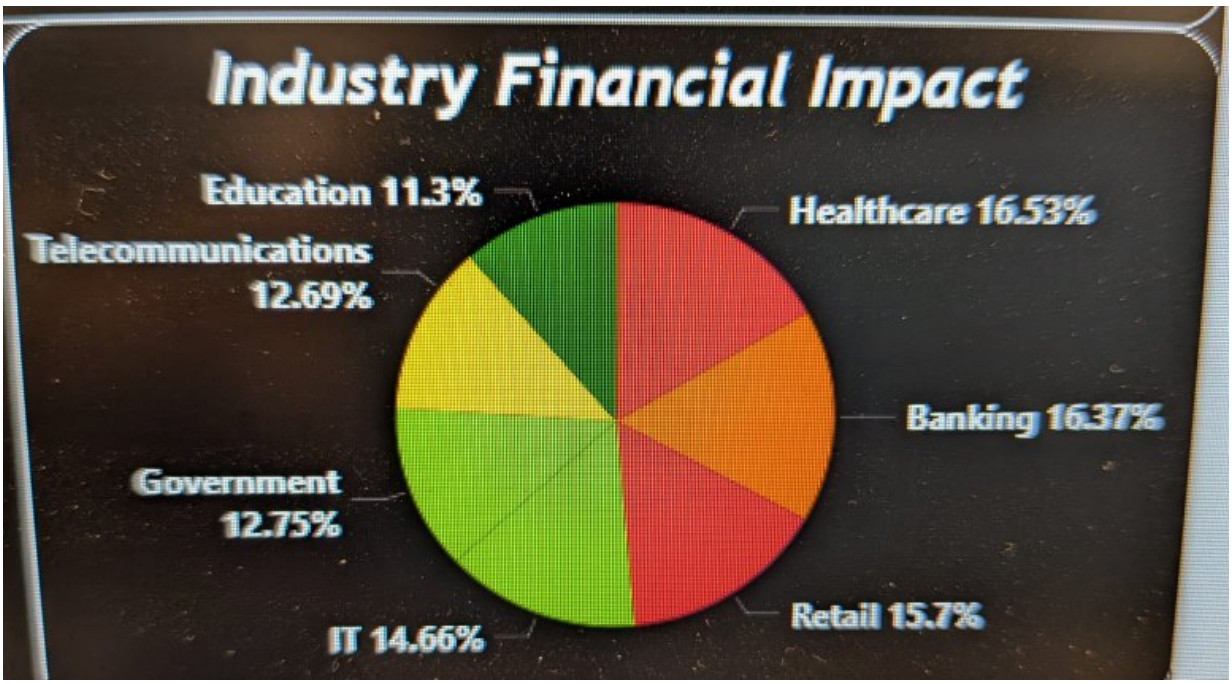
LIST OF FIGURES



· Phishing and Malware are the most severe in terms of user impact and frequency.

· Ransomware causes extreme financial damage despite lower frequency.

· DDoS, SQL Injection, and Man-in-the-Middle attacks are widespread but result in lower average losses.



· Healthcare (16.53%) and Banking (16.37%) are the most financially impacted sectors.

· Retail (15.7%) and IT (14.66%) follow closely, indicating broad targeting across industries.

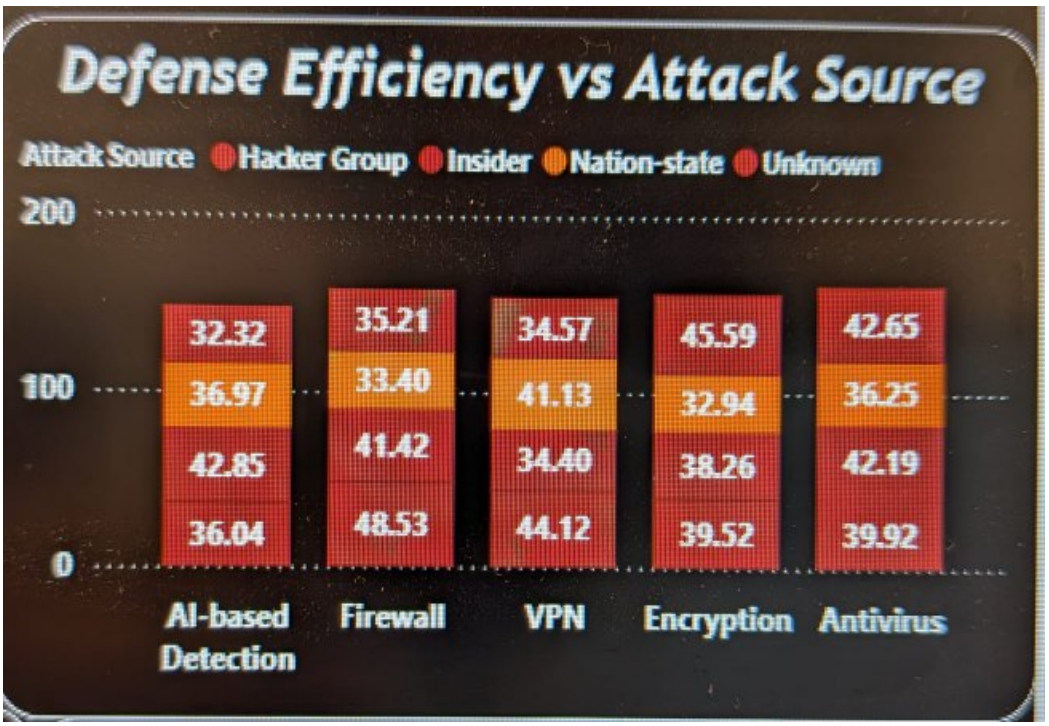
· Education, Government, and Telecom also face

significant but relatively lower financial losses.

· North America, Europe, and Asia show the highest density of cyber attacks.

· Threat actor types vary by region: Hacker groups dominate in developed regions, while insider threats are widespread globally.

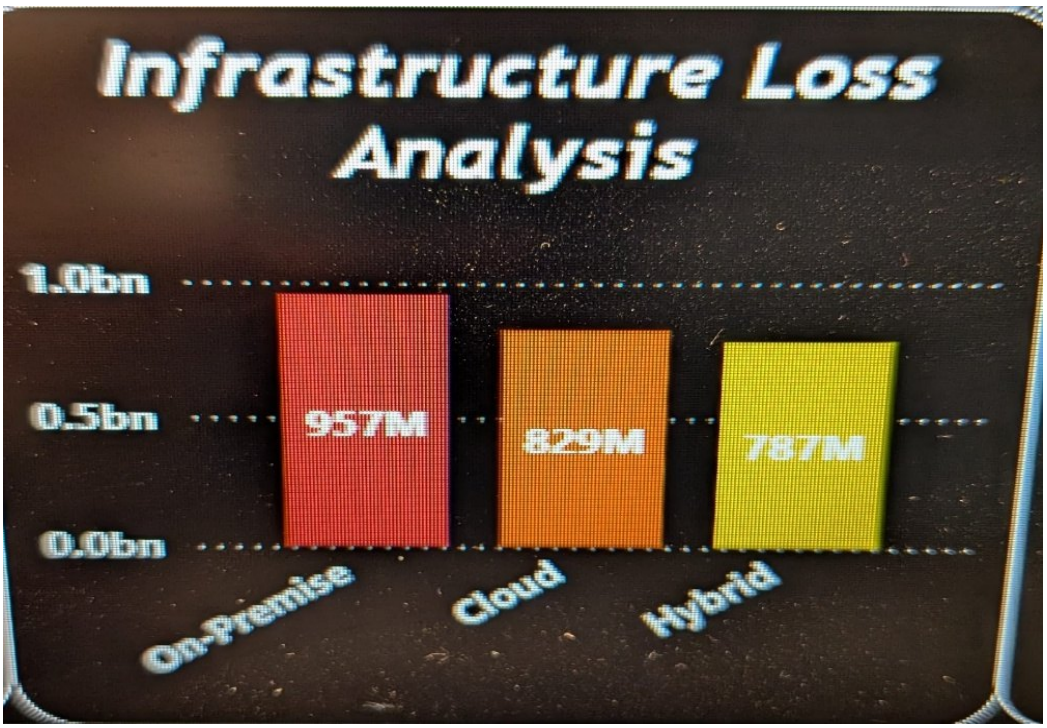
· Regional hotspots highlight the need for geographically tailored defense strategies.



· Antivirus and Encryption are the most effective defenses across all attack sources.

· AI-based Detection and Firewalls perform moderately but vary by threat type.

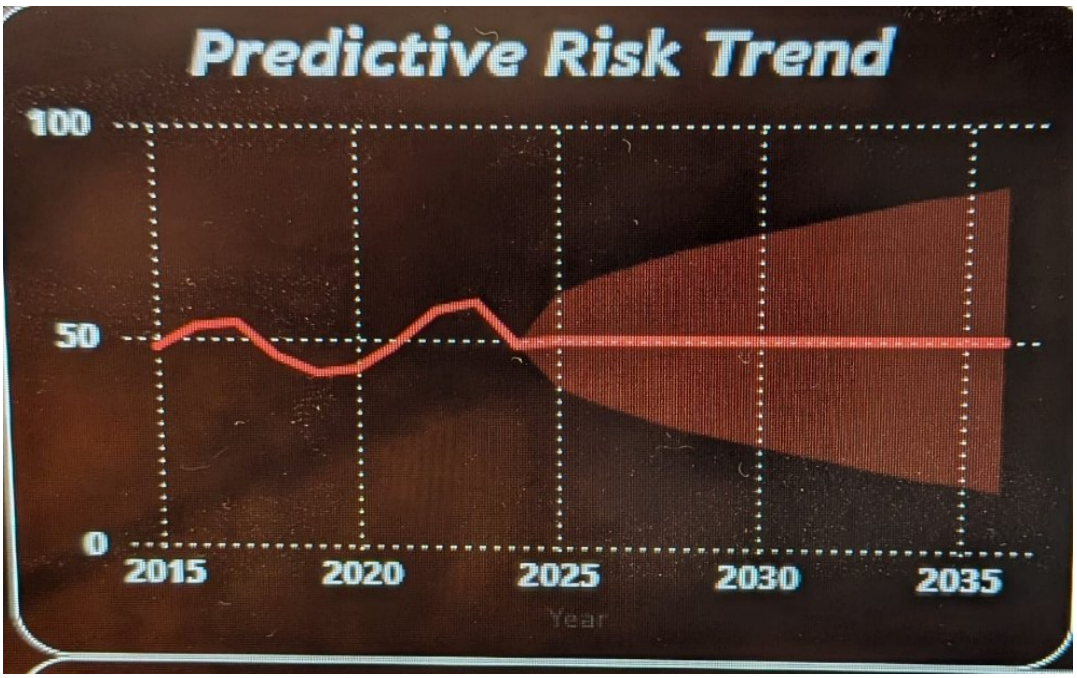
· Insider and Unknown threats remain challenging, with defense efficiency often below 50%.



On-Premise systems suffer the highest financial loss per incident.

· Hybrid infrastructure follows, indicating complexity-related vulnerabilities.

· Cloud-based systems show the lowest loss, supporting the security benefits of managed cloud environments.



· Cyber attacks are projected to rise steadily from 2015 to 2035, with accelerated growth after 2025.

· Social Engineering and Unpatched Software are expected to be primary future attack vectors.

· The trend highlights the urgent need for proactive and predictive cybersecurity measures.

CHAPTER 1

Introduction

1.1 Problem Statement:

Cyberattacks are becoming more common and advanced. Organizations collect lots of security data, but they often struggle to make sense of it quickly. Without clear insights, it’s hard to prioritize threats or use resources wisely, leaving them exposed to risk.

1.2 Motivation;

- We wanted to bridge the gap between raw data and clear understanding.
- A visual dashboard helps security teams and leaders see the big picture—understanding what threats matter most, where weaknesses are, and what attacks cost.

1.3 Objective:

· To analyze and compare risks of different cyber attacks

· To identify which regions and industries are at highest risk

· To check how well current security measures

are working

· To present all findings in an interactive, easy-to-use dashboard

1.4 Scope of the Project:

This project works with past cyber incident data. It focuses on common attack types, compares impacts across different industries, and looks at risks for on-site, cloud, and mixed computer systems.

CHAPTER 2

Literature Survey

2.1 Previous studies highlight the importance of cybersecurity analytics in identifying vulnerabilities and reducing response time.

2.2 Existing solutions:

- NIST Cybersecurity Framework: Focuses on Identify, Protect, Detect, Respond, and Recover.
- ISO/IEC 27001: International standards for information security management systems.
- CIS Controls (formerly CIS 20): A prioritized set of actions designed to stop the most common cyberattacks.

2.3 Existing solutions often lack integrated visualization, making dashboards a valuable enhancement for cyber risk assessment.

CHAPTER 3

Proposed Methodology

3.1 System Design

We built a system that takes in cyber incident data, processes it, and displays results on a

visual dashboard.

3.2 Analysis Modules

We broke the analysis into five parts

1. Risk Score Analysis – Measures overall danger levels

2. Attack Type Analysis – Looks at damage from different attacks

3. Geographical Analysis – Shows where attacks happen most

4. Defense Efficiency Analysis – Tests how well security tools work

5. Industry Impact Analysis – Finds which sectors are hit hardest

3.3 Data Flow

Our process followed these steps:

1. Data Collection – Gathering past incident records

2. Data Cleaning – Organizing and preparing the data

3. Risk Rating – Labeling incidents as Low, Medium, High, or Critical

4. Visualization – Creating charts and maps

5. Insight Generation – Drawing useful conclusions

3.4 Advantages

Easy interpretation of complex data
Faster decisionmaking
Improved risk prioritization

3.5 Requirement Specification

1. Hardware Requirements: Computer with minimum 8GB RAM

2. Software Requirements: Data visualization tools, analytics software

CHAPTER 4

Implementation and Result

4.1 Dashboard Results

- Average Risk Score: Medium to High
- Total Users Affected: 252 million
- Total Financial Loss: $0.03 Million
- Average Recovery Time: 38.69 hours

4.2 Key Findings

- Phishing and malware caused the most financial harm
- Healthcare and banking were the most targeted industries

- Hybrid systems had higher losses than cloud systems
- Antivirus and encryption were the most effective security tools

CHAPTER 5

Discussion and Conclusion

5.1 Key Insights

The dashboard made it easy to spot trends and weaknesses. It helped show where attention and resources are needed most.

5.2 Project Links

- GitHub Repository: [Link to be added]
- Video Demonstration: [Link to be added]

5.3 Limitations

- We used past data, not live threats
- The scope was limited to certain industries and attack types

5.4 Future Work

· Connect to real-time threat data

· Use AI to predict future attacks

· Add alerts for high-risk events

· Test in more industries and regions

5.5 Conclusion

This Cyber Risk Analysis Dashboard turns complex data into clear visuals. It helps organizations understand their risks, improve their defenses, and make smarter decisions. By using such tools, businesses can build stronger cyber resilience and reduce potential losses.

REFERENCES

https://www.kaggle.com/datasets/atharvasoundankar/global-cybersecurity-threats-2015-2024