DATA ANALYTICS WITH POWER BI

PROJECT REPORT

(Project Semester August - January 2025)

(Cyber Risk & Financial Impact Analysis Dashboard)

Submitted by:
Abhay Pratap Singh

Registration No. :12303939

Programme and Section: B-tech CSE K23CN
Course Code: INT374

Under the Guidance of
(Mr. Jaffar Amin Chacket)

Discipline of CSE/IT

School of Computer Science and Engineering

Lovely Professional University, Phagwara

CERTIFICATE

This is to certify that **Abhay Pratap Singh**, Registration No. **12303939**, has successfully completed the project titled **"*Cyber Risk & Financial Impact Analysis Dashboard*"** under my supervision. To the best of my knowledge, this work is the result of his/her original development, effort, and independent study.

Jaffar Amin Chacket, Assistant Professor School of Computer Science,

Lovely Professional University,

Phagwara, Punjab,

Date: 20/12/2025

DECLARATION

I, Abhay Pratap Singh, student of B.Tech CSE (K23CN), Lovely Professional University, hereby declare that the project titled "***Cyber Risk & Financial Impact Analysis Dashboard*** " is my original work prepared under the guidance of *Ms. Sadaf Quereshi*. This report does not contain any work previously submitted for any degree or diploma.

Date: 20/12/2025 Signature:

Registration No.: 12303939 Abhay Pratap Singh

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to **Mr. Jaffar Amin Chacket** , my mentor, for her constant guidance, encouragement, and invaluable support throughout the development of this project. Her expertise in Power BI, cybersecurity analytics, and data visualization greatly enhanced my understanding and helped me navigate challenges with confidence. I am truly grateful for the time and effort she invested in helping me improve the quality and clarity of this work.

I also extend my heartfelt thanks to **Lovely Professional University** for providing a conducive academic environment and access to digital tools that made this project possible. The resources and learning ecosystem offered by the university played a significant role in shaping my technical and analytical abilities.

My appreciation also goes to my **friends, classmates, and family members**, whose continuous motivation, constructive feedback, and emotional support kept me focused and inspired throughout the process. Their belief in my abilities gave me the confidence to complete this project successfully.

This project has been a valuable learning experience, helping me grow not only in technical skills but also in critical thinking, problem-solving, and decision-making. I am thankful to everyone who contributed directly or indirectly to this achievement.

TABLE OF CONTENTS

INTRODUCTION

Cybersecurity has rapidly become one of the most critical global concerns of the 21st century, driven by the world's increasing reliance on digital technologies. As organizations, governments, and individuals expand their digital footprints, the frequency, scale, and sophistication of cyberattacks have grown at an alarming rate. These attacks range from data breaches and ransomware incidents to identity theft and large-scale system disruptions, leading to severe financial losses, erosion of trust, and significant operational setbacks. The evolving threat landscape highlights the urgent need for advanced analytical tools that can help understand, anticipate, and mitigate cyber risks effectively.

This project, titled ***"Cyber Risk & Financial Impact Analysis Dashboard"***, was undertaken to analyze and visualize global cyber threat patterns using Microsoft Power BI. The dashboard provides a comprehensive overview of cyber incidents across countries, industries, and attack types over a ten-year period. It captures key elements such as severity levels, financial losses, affected users, attack sources, vulnerability types, and defense mechanism performance.

Through interactive visualizations, the dashboard transforms raw cybersecurity data into actionable intelligence, enabling users to explore trends, compare risks, and identify high-impact threats. The project also offered an opportunity to develop strong technical skills in data preprocessing, data modeling, DAX formulas, and visualization design. Overall, the work enhances understanding of global cybersecurity challenges and demonstrates the power of data analytics in supporting informed security decision-making.

SOURCE OF DATASET

The dataset used for this project was obtained from Kaggle, a globally recognized open-source data platform that provides high-quality, publicly accessible datasets contributed by researchers, data professionals, and cybersecurity enthusiasts. Kaggle is widely trusted for academic and analytical projects due to its well-structured datasets and extensive community validation. Specifically, the cybersecurity dataset used in this study was sourced from a curated collection focused on global cyber incidents, threat patterns, and organizational vulnerabilities.

The dataset contains a diverse range of attributes crucial for conducting meaningful cybersecurity analysis. It includes information on country-wise cyber incidents, various attack types (such as phishing, ransomware, malware, and MITM attacks), financial losses, affected user counts, and target industries impacted by each incident. Additionally, it features important operational details such as attack sources (Insider, Nation-State, Hacker Group), vulnerability types, defense mechanisms employed, and incident resolution time. These attributes collectively offer a multidimensional view of the global threat landscape.

Covering data from 2015 to 2024, the dataset enables a comprehensive multi-year analysis, allowing comparisons of trends, severity patterns, and evolving threats across regions and industries. Its structured and well-organized format made it highly suitable for transformation, modeling, and visualization using Microsoft Power BI. The richness and credibility of the dataset provided a strong foundation for building a meaningful, data-driven cybersecurity dashboard that supports insightful exploration and informed decision-making in the domain of cyber threat intelligence.

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

DATA PREPROCESSING

Before conducting any analysis, the cybersecurity dataset had to be thoroughly cleaned and prepared to ensure accuracy and consistency in the visualizations. As with most real-world datasets, several irregularities were present, including missing values, inconsistent categories, and redundant entries. Proper preprocessing was therefore essential to avoid misleading insights and to build a reliable Power BI dashboard.

1. Handling Missing Values

One of the primary issues encountered was missing values, particularly in numerical fields such as financial loss and number of affected users. Instead of discarding incomplete records, appropriate imputation techniques were applied. Mean values were used to fill missing numerical data to preserve overall trends and ensure that valuable information was not lost. For categorical fields such as country, attack type, and vulnerability type, missing or inconsistent entries were manually corrected or standardized for uniformity.

2. Standardizing Categorical Fields

Categorical features contained inconsistencies due to variations in spelling, abbreviations, and naming conventions. Fields such as *Country*, *Attack Type*, and *Vulnerability Type* were carefully standardized to maintain uniformity across all dashboard filters and slicers. This step ensured consistent grouping and eliminated errors that could affect visual clarity and analysis accuracy.

3. Removing Duplicate Records

Duplicate rows were identified within the dataset, which could have artificially inflated incident counts or skewed severity analysis. These duplicates were removed to maintain the uniqueness of each cyber incident and ensure that the data accurately reflected real-world cyber events.

4. Transforming Numerical and Categorical Fields

To ensure accurate analysis for all five objectives, several numerical and categorical fields were transformed to improve interpretability and consistency. Numerical fields such as *Financial Loss*, *Loss per User*, and *Number of Affected Users* were formatted into standardized units (thousands, millions) for clearer visualization. This transformation made charts easier to read and enabled meaningful comparisons across years and countries. Additionally, categorical fields like *Attack Type*, *Defense Mechanism*, and *Target Industry* were reorganized into uniform categories to support smooth filtering across multiple dashboard pages.

5. Final Dataset Readiness

After completing all preprocessing steps, the dataset became well-structured, consistent, and fully prepared for visualization. These improvements significantly enhanced data quality and ensured that the Power BI dashboard would generate reliable, accurate, and insightful results. The preprocessing stage played a crucial role in transforming raw cybersecurity data into a clean foundation for analytical exploration.

ANALYSIS ON DATASET

i) General Description

The cybersecurity dataset used in this project provides a comprehensive view of global cyber incidents recorded between 2015 and 2024. It captures a wide range of attributes associated with cyberattacks, making it suitable for analyzing attack patterns, risk levels, and incident impact across countries and industries. Key variables in the dataset include the type of attack (such as phishing, ransomware, DDoS, and malware), target industry, country of occurrence, financial loss, number of affected users, attack source, vulnerability exploited, and defense mechanism implemented. Additional fields like incident resolution time and the derived severity score further enrich the understanding of how impactful and complex each incident was.

The dataset enables multi-dimensional analysis by combining both technical and operational aspects of cybersecurity incidents. For example, financial and user impact metrics help assess the magnitude of each attack, while industry and country attributes support comparative risk evaluation across regions and sectors. Attack sources and vulnerability types provide insights into the origin and nature of threats, whereas defense mechanism data reveals how effectively organizations respond to cyberattacks. Together, these variables offer a holistic view of global cyber risk, allowing meaningful visual exploration through Power BI dashboards.

Objective 1: Analyze the Number of Affected Users Across Countries

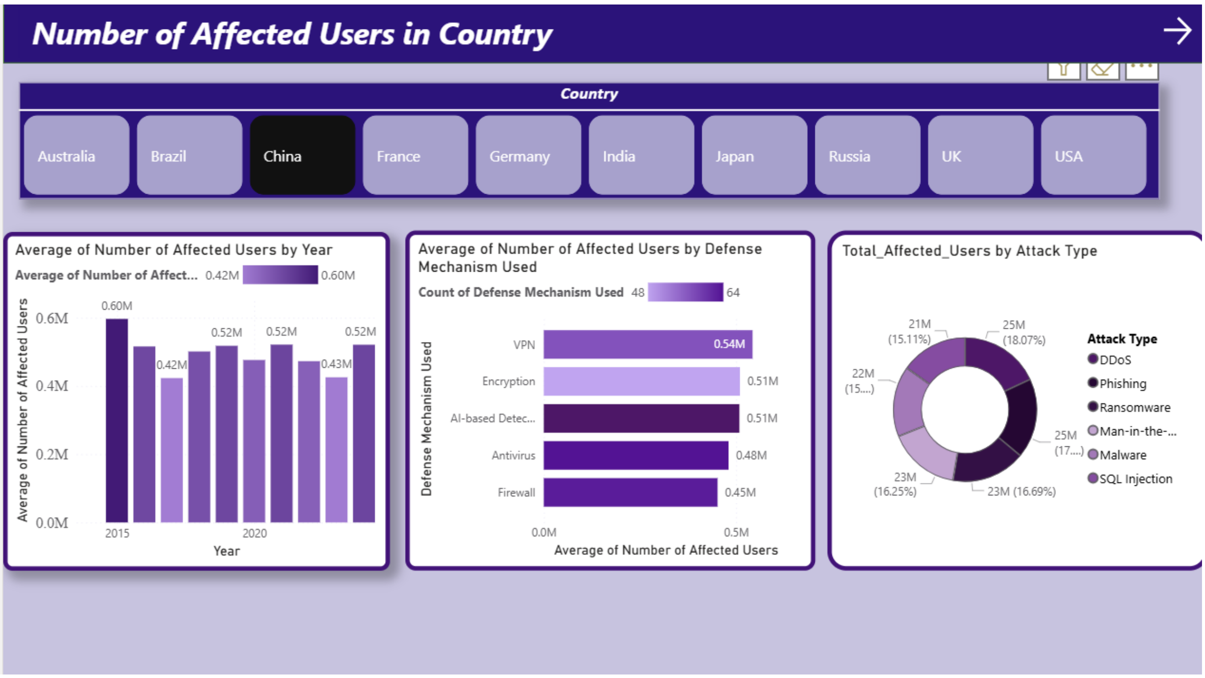
ii) Specific Requirements

The first objective aimed to understand how cyber incidents impact users across different countries by analyzing the number of affected users associated with various attack types and defense mechanisms. Since the scale of user impact is a key indicator of the seriousness of cyber threats, this objective focused on identifying nations experiencing the highest average number of affected users. It also required comparing how different defense mechanisms influenced user-level damage and evaluating yearly trends to determine whether affected user counts were rising or declining. The goal was to highlight which regions face greater exposure and which security strategies contribute to minimizing user impact.

iii) Analysis Results

The analysis revealed significant variation in affected user counts among countries. Nations with larger digital footprints—such as India, USA, China, and Germany—recorded higher average numbers of impacted users, indicating broader exposure to large-scale attacks. In contrast, countries with smaller populations or stronger defense frameworks showed comparatively lower user impact. Attack types like ransomware and DDoS were found to affect the highest number of users globally. The study also showed that advanced defense mechanisms such as AI-based Detection consistently resulted in fewer affected users, while traditional measures like antivirus alone had limited effectiveness. Year-wise patterns indicated fluctuating but generally rising user impact across the decade, demonstrating the growing reach of cyberattacks.

iv) Visualization



Several Power BI visuals supported this objective. A Clustered Column Chart displayed the average number of affected users by year, showing upward or downward patterns over time. A Donut Chart highlighted the distribution of total affected users by attack type, identifying which threats impacted the most people. Additionally, a Bar Chart comparing affected users by defense mechanism within each country provided insight into how security strategies influence user-level exposure. A country slicer enabled users to interactively filter the dashboard and compare user impact across nations.

Objective 2: Examine How Cyberattacks Have Evolved Over Time Globally

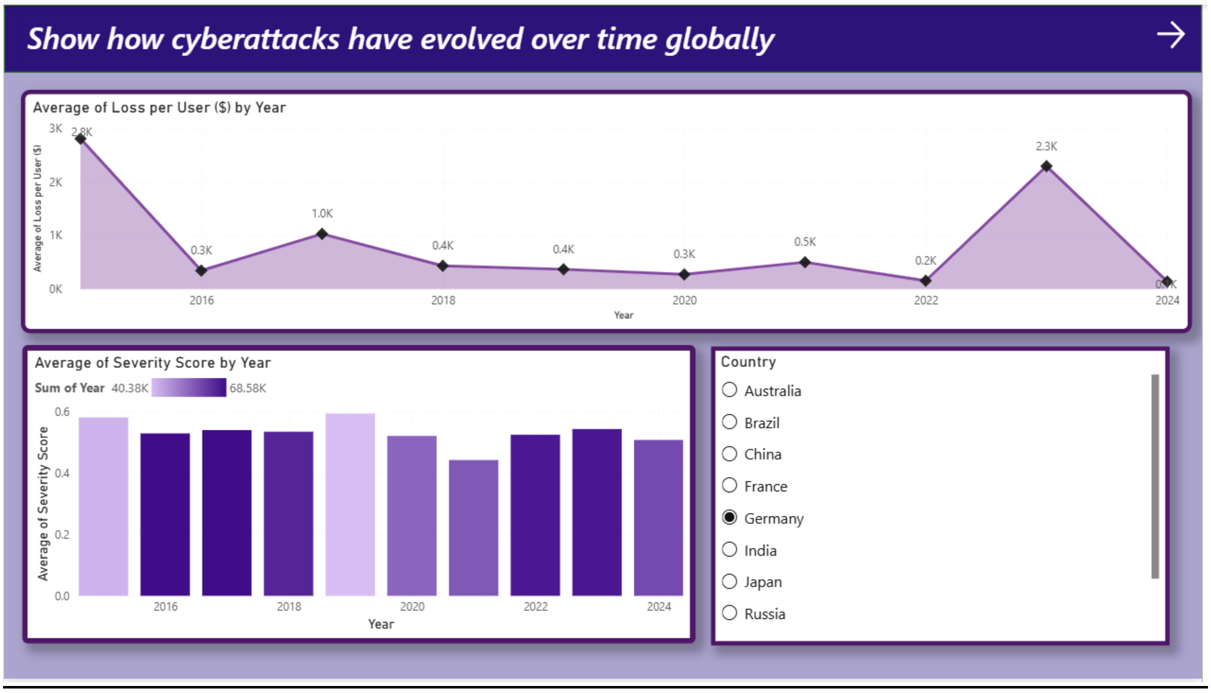
ii) Specific Requirements

The second objective focused on understanding the global evolution of cyberattacks over a ten-year period, analyzing how factors such as loss per user and severity score have changed with time. The purpose was to observe long-term trends in cyber threat intensity, determine whether attacks are becoming more severe, and identify any significant fluctuations across specific years. This objective required year-wise comparison of attack metrics and aimed to provide clarity on whether global cybersecurity risks are escalating due to technological expansion, increased digital dependency, or sophisticated attack methods.

iii) Analysis Results

The analysis revealed notable year-to-year fluctuations in both loss per user and severity score, indicating dynamic shifts in cyber threat landscapes. Certain years—particularly after 2018 and 2020—showed significant spikes in average loss per user, highlighting periods where attacks were more damaging, possibly due to advanced ransomware campaigns or widespread data breaches. Severity scores also exhibited a gradual upward trend, suggesting that cyber incidents were becoming more impactful and complex over time. The results indicate that while the number of attacks may fluctuate, their intensity and cost implications have generally increased, emphasizing the growing need for robust cybersecurity strategies at global, industry, and organizational levels.

iv) Visualization


Show how cyberattacks have evolved over time globally
→
Average of Loss per User ($) by Year
Average of Loss per User ($)
3K
2K
1K
0K
2.8K
0.3K
1.0K
0.4K
0.4K
0.3K
0.5K
0.2K
2.3K
0.1K
2016
2018
2020
2022
2024
Year
Average of Severity Score by Year
Sum of Year 40.38K
68.58K
Average of Severity Score
0.6
0.4
0.2
0.0
2016
2018
2020
2022
2024
Year

Country
○ Australia
○ Brazil
○ China
○ France
● Germany
○ India
○ Japan
○ Russia

This objective was supported by multiple Power BI visuals. An Area Chart illustrated the year-wise changes in average loss per user, making it easy to identify sharp increases or declines. A Column Chart displayed the average severity score by year, helping assess the seriousness of attacks over time. A country slicer allowed users to analyze temporal trends for specific nations, offering deeper insight into localized threat patterns. Collectively, these visuals enabled an interactive understanding of how global cyberattack behavior has evolved over the past decade.

Objective 3: Compare Which Countries Face the Most Cybersecurity Issues

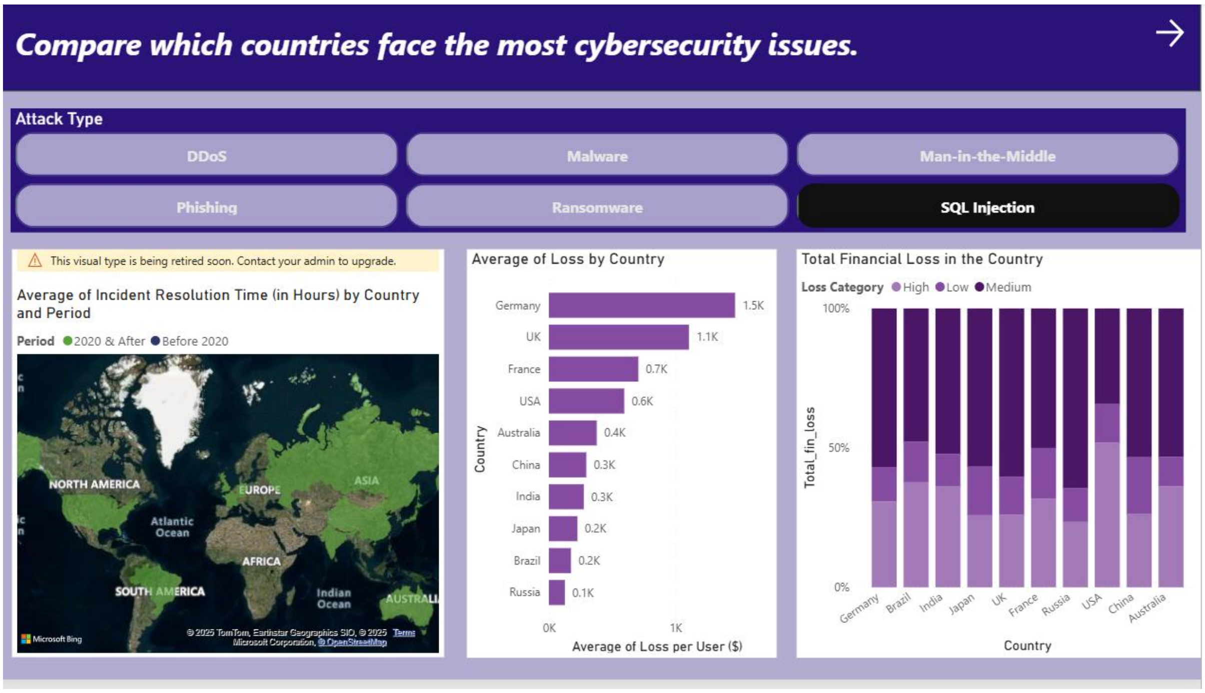
ii) Specific Requirements

The third objective aimed to analyze which countries face the highest cybersecurity risks by comparing financial losses, incident counts, and loss categories across nations. Since cyber threats vary widely across geopolitical, economic, and technological landscapes, the goal was to identify which countries are disproportionately affected and understand the severity of incidents they experience. This objective required evaluating both the magnitude and distribution of financial losses, observing how attack categories differ among nations, and identifying whether post-2020 digital acceleration contributed to increased vulnerabilities. The analysis also incorporated an understanding of how global attack patterns shift over time and across regions.

iii) Analysis Results

The analysis showed that countries such as India, USA, China, and France faced the highest financial losses, indicating larger digital ecosystems and greater exposure to high-impact attacks. Several nations displayed a significant rise in high-loss incidents after 2020, reflecting an increase in sophisticated threats like ransomware and targeted intrusions. Countries with stronger cybersecurity frameworks experienced fewer severe incidents, while others showed a higher concentration of medium- and high-severity attacks. The data also revealed distinct variation in attack patterns based on region, with some countries experiencing more phishing incidents and others facing more DDoS or malware-related breaches. These findings highlight global disparities in cybersecurity readiness and threat exposure.

iv) Visualization



Compare which countries face the most cybersecurity issues.

⚠ This visual type is being retired soon. Contact your admin to upgrade.

Multiple Power BI visuals were used to support this objective. A Map Visualization displayed country-wise incident averages, helping identify global cybersecurity hotspots. A Clustered Bar Chart highlighted differences in financial loss across countries, making it easy to compare risk levels. Additionally, a Stacked Column Chart represented each nation's distribution of Low, Medium, and High loss categories, offering insight into severity patterns rather than just frequency. Attack Type slicers enabled users to explore country-wise impact specific to different forms of cyberattacks. Together, these visuals provided a comprehensive comparison of how various countries experience cybersecurity challenges.

Objective 4: Identify Which Attack Types Are Most Dangerous

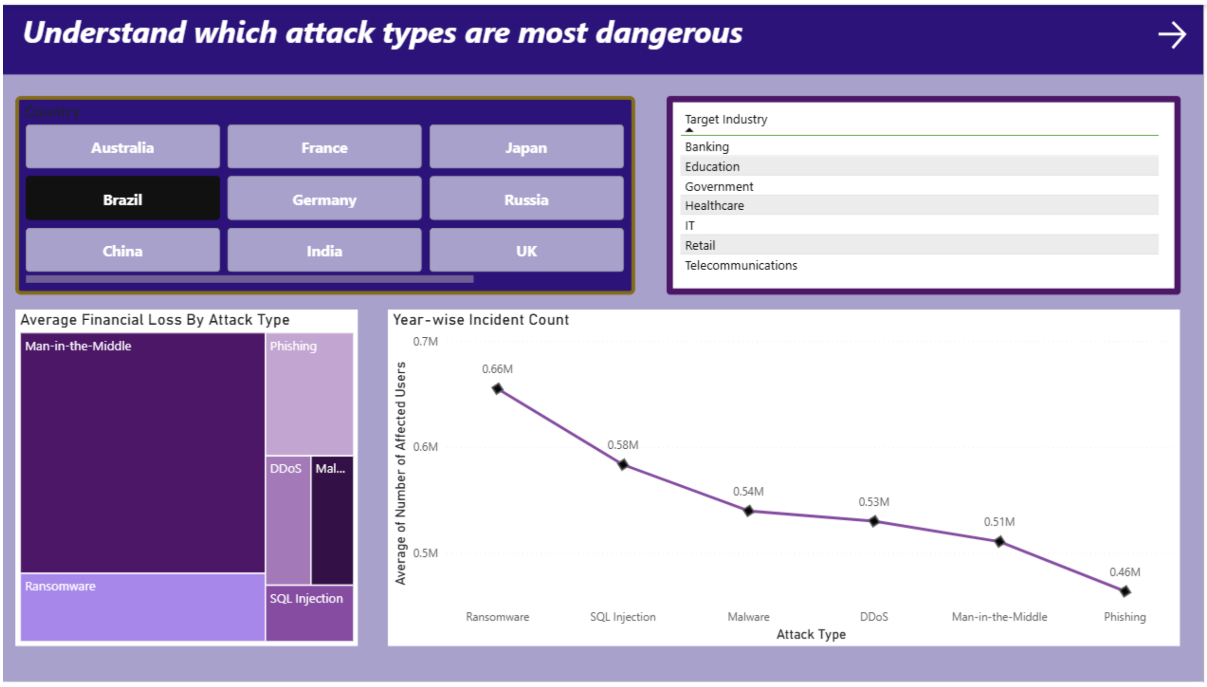
ii) Specific Requirements

The fourth objective aimed to determine which categories of cyberattacks pose the greatest danger in terms of overall severity, financial impact, and user exposure. Each attack type—such as ransomware, phishing, DDoS, or data breaches—has its own behavior and consequences. This objective required analyzing how damaging each attack type is, understanding the average loss per user associated with each method, and identifying which threats consistently fall into Medium or High severity categories. The primary goal was to highlight attack techniques that organizations should prioritize when developing cybersecurity strategies and defense mechanisms.

iii) Analysis Results

The findings indicated that Ransomware was one of the most dangerous forms of attack, showing the highest financial losses and consistently high severity scores. DDoS attacks significantly affected user access, resulting in substantial loss per user in several countries, especially those with high digital dependency. Phishing attacks, although more common, demonstrated moderate severity but affected a large number of users globally. Malware and Insider Attacks showed high severity in industries like finance and IT due to their potential to compromise sensitive systems. Overall, the analysis revealed that attack types differ significantly not only in how often they occur but also in how devastating their outcomes can be, depending on context and target.

iv) Visualization



Power BI visualizations played a central role in conveying these insights. A Pie Chart illustrated the share of each attack type based on average affected users, highlighting widespread threats. A Column Chart displayed the average loss per user by attack category, making it easy to compare the financial danger posed by different attack types. Additionally, a Scatter Visual plotted severity score against loss per user, with each bubble representing an attack type, helping identify threats that are both severe and costly. Slicers for Country and Attack Source allowed deeper exploration of how attack types vary across different environments and regions.

Objective 5: Identify Vulnerable Industries and Evaluate Defense Mechanism Effectiveness Across Years

ii) Specific Requirements

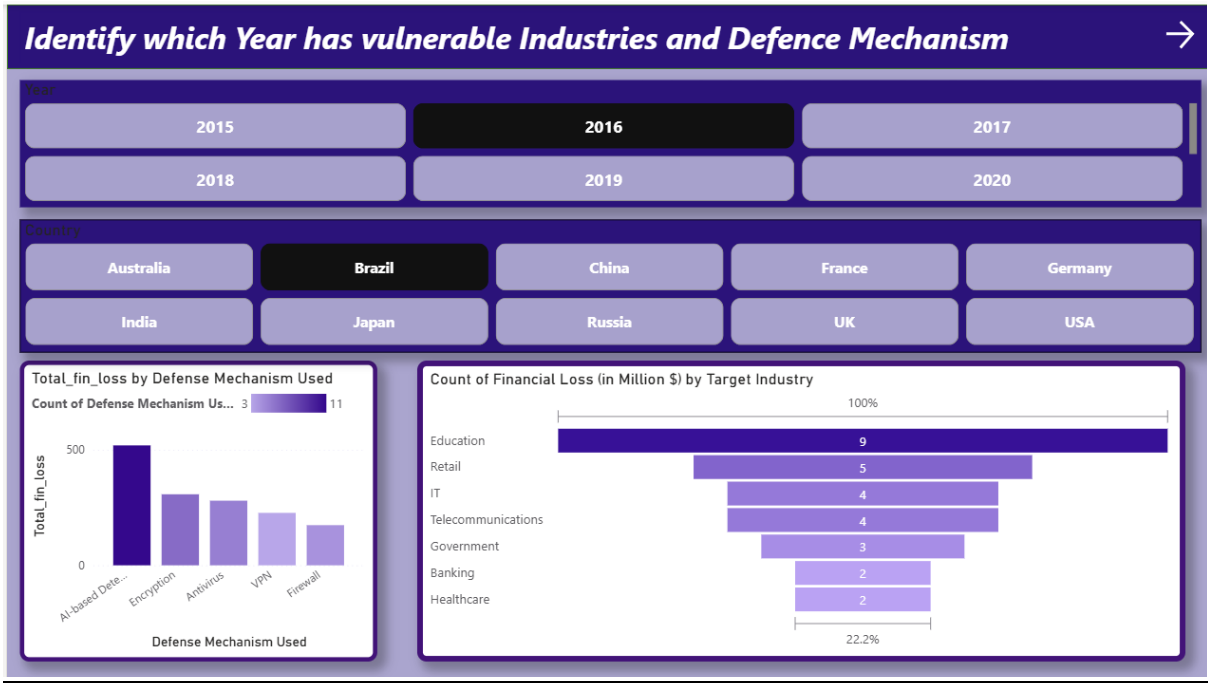
The fifth objective aimed to analyze which industries are most vulnerable to cyberattacks and how different defense mechanisms perform across various years. Since industries differ in their technological exposure, data sensitivity, and operational dependency on digital systems, the objective required evaluating industry-wise attack patterns, financial loss distribution, and security effectiveness. Additionally, the analysis needed to compare how vulnerability and defense performance changed over time, especially during years of heightened cyber activity. The primary goal was to determine which industries consistently faced severe attacks and which defense strategies were most helpful in mitigating impact.

iii) Analysis Results

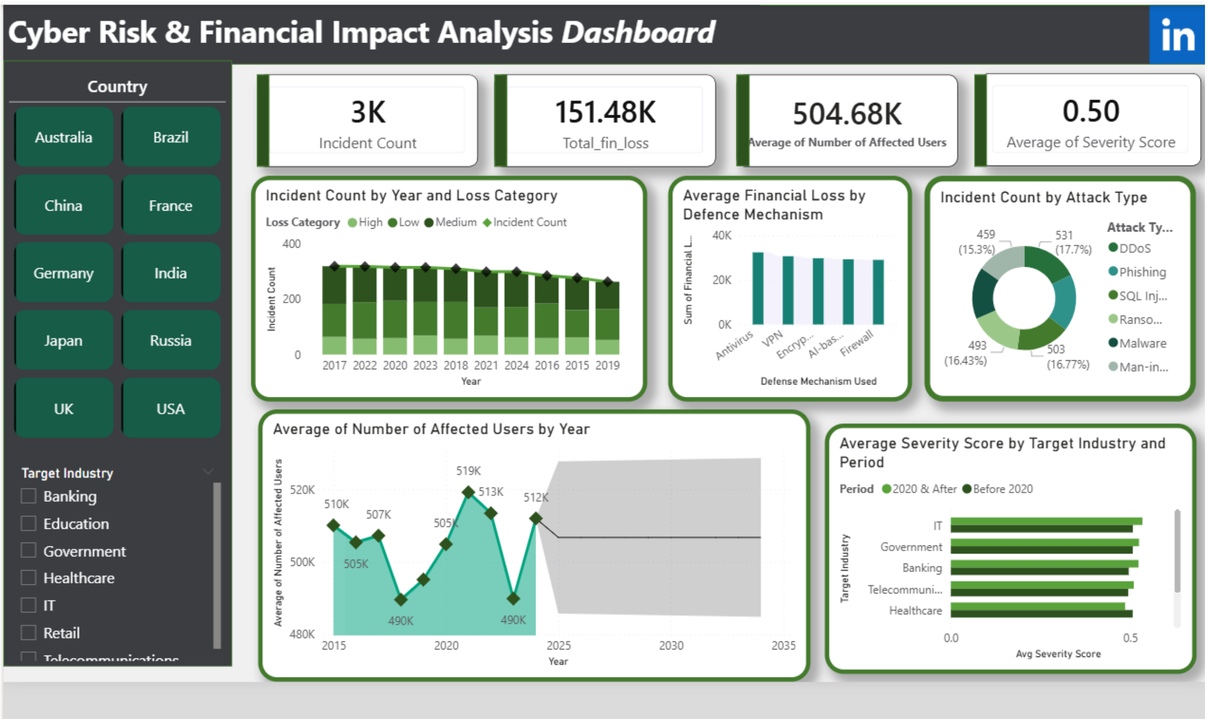
The results showed that industries such as Information Technology, Finance, and Telecom experienced high vulnerability due to the large volume of digital assets and sensitive information they handle. These sectors displayed higher severity scores and greater financial losses, indicating sustained exposure to sophisticated threats. Meanwhile, industries like Retail and Education experienced frequent but lower-severity incidents, primarily associated with phishing and credential-based attacks.

In terms of defense mechanisms, AI-based Detection and Multi-layered Security Systems were found to be significantly more effective, showing reduced severity scores and shorter resolution times across multiple years. Traditional tools, such as basic antivirus solutions, offered limited protection, particularly against modern attack types like ransomware. Year-wise comparison revealed that vulnerability trends fluctuated, with certain years showing increased exposure due to global shifts in digital behavior, remote work adoption, and evolving threat techniques.

iv) Visualization



Power BI visuals were used extensively to illustrate industry vulnerability and defense performance. A Column Chart displayed industry-wise average loss per user, helping identify sectors with the highest impact. A Bar Chart showed the industry-year breakdown of severity scores, highlighting fluctuations in vulnerability over time. A Stacked Column Chart illustrated how defense mechanisms performed across different industries, providing insight into the relationship between security strategies and incident severity. Slicers for Year and Attack Type allowed users to explore changes dynamically across different time frames and threat categories.



CONCLUSION

This project offered a comprehensive exploration of global cybersecurity trends using an interactive Power BI dashboard. By examining data from 2015 to 2024, the analysis highlighted the continuous rise in cyber incidents and the growing sophistication of threat actors. Through the use of visual tools, the project effectively showcased how factors such as attack type, country, industry, and defense mechanisms influence the overall risk landscape. The addition of derived metrics like Severity Score and Loss Category further enriched the analysis, allowing for clearer understanding of which incidents caused the most significant damage.

The dashboard revealed that ransomware, phishing, and insider attacks continue to dominate the cybersecurity space, each differing in scale and impact. Countries with advanced digital infrastructures faced higher financial losses, while industries such as IT, finance, and healthcare appeared most vulnerable due to the sensitivity and volume of data they handle. Defense strategies also varied in effectiveness, with AI-based detection and multi-layered security frameworks proving to be the most reliable. These insights underscore the importance of adapting cybersecurity strategies to both technological advancements and evolving cybercriminal behavior.

Overall, this project strengthened my analytical, visualization, and data interpretation skills. It demonstrated how structured data, when transformed through Power BI, can generate meaningful insights that support informed decision-making. Beyond technical learning, the project highlighted the urgency of building stronger cybersecurity awareness and resilience across organizations and sectors as the digital world continues to expand.

FUTURE SCOPE

The study can be expanded further by:

1. Integrating real-time cyber threat intelligence feeds from global monitoring systems.

2. Applying predictive analytics and machine learning to forecast attack trends and severity.

3. Incorporating organization-specific risk scores and automated alert mechanisms.

4. Developing mobile-friendly or web-based versions of the dashboard for quick decision-making.

5. Including advanced visualizations such as network graphs and attacker path mapping.

REFERENCE:

1. Cybersecurity & Infrastructure Security Agency (CISA) Threat Reports

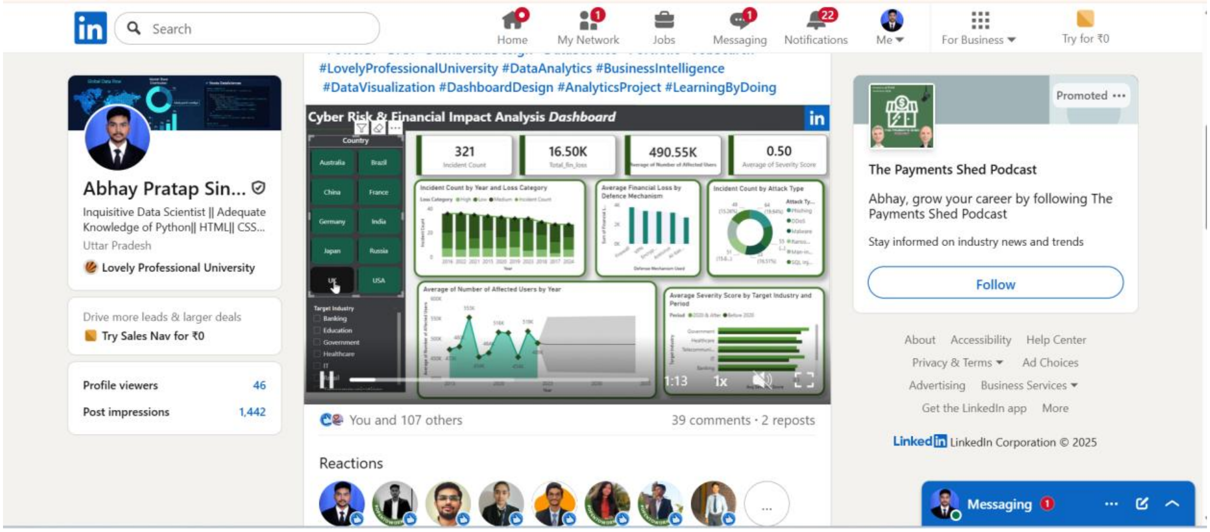
2. IBM Security – Cost of a Data Breach Report

3. Verizon Data Breach Investigations Report (DBIR)

4. National Institute of Standards and Technology (NIST) Cybersecurity Framework

5. Microsoft Power BI Documentation

LINKEDIN



#LovelyProfessionalUniversity #DataAnalytics #BusinessIntelligence #DataVisualization #DashboardDesign #AnalyticsProject #LearningByDoing

Abhay Pratap Sin...

Inquisitive Data Scientist || Adequate Knowledge of Python|| HTML|| CSS...

Uttar Pradesh

Lovely Professional University

Drive more leads & larger deals

Try Sales Nav for ₹0

Profile viewers	46
Post impressions	1,442

You and 107 others

39 comments · 2 reposts

Reactions

The Payments Shed Podcast

Abhay, grow your career by following The Payments Shed Podcast

Stay informed on industry news and trends

LinkedIn Corporation © 2025

Github
Dataset