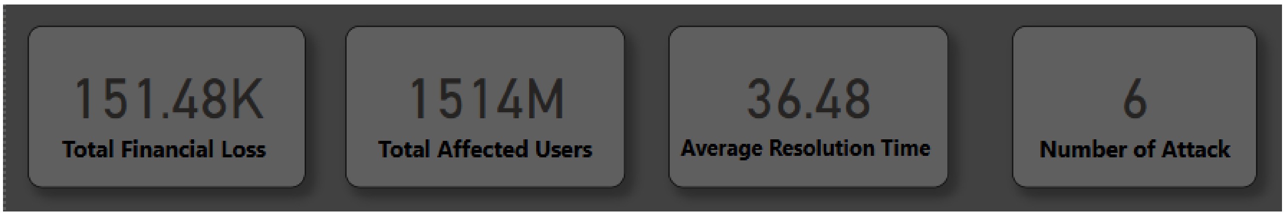
Global Cyber Security - Project

1. Key Performance Indicators (KPIs):

- **Total Financial Loss:** This indicates the total financial impact of the recorded attacks. The "K" is in thousands. This represents a significant sum lost due to cyberattacks.
- **Total Affected Users:** This is a very significant number, indicating 1.514 million affected users. This suggests either a very widespread impact or perhaps an aggregation over many years or a large scale incident.
- **Average Resolution Time:** An average resolution time of 36.48 hours (approximately 1.52 days) for cybersecurity incidents is a more typical and reasonable timeframe, though it still indicates significant effort is required for full mitigation and recovery.
- **Number of Attack:** This seems surprisingly low compared to the "Total Affected Users" and "Total Financial Loss."



151.48K
Total Financial Loss

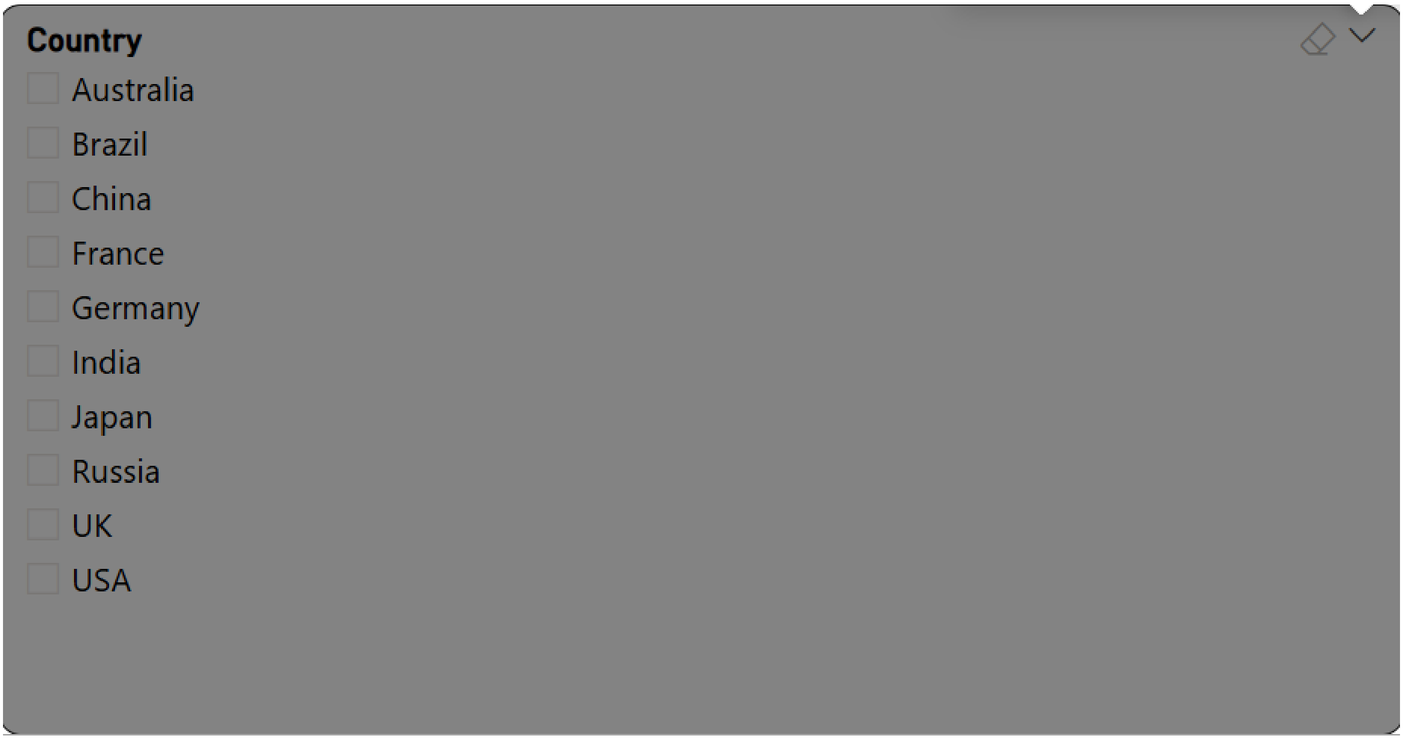
1514M
Total Affected Users

36.48
Average Resolution Time

6
Number of Attack

2. Country Filter :

- Lists several countries (Australia, Brazil, China, France, Germany, India, Japan, Russia, UK, USA).
- Currently, **no countries are selected**, meaning all the KPIs and other visualizations are displaying aggregated data from all these listed countries. This filter is crucial for regional analysis.



Country

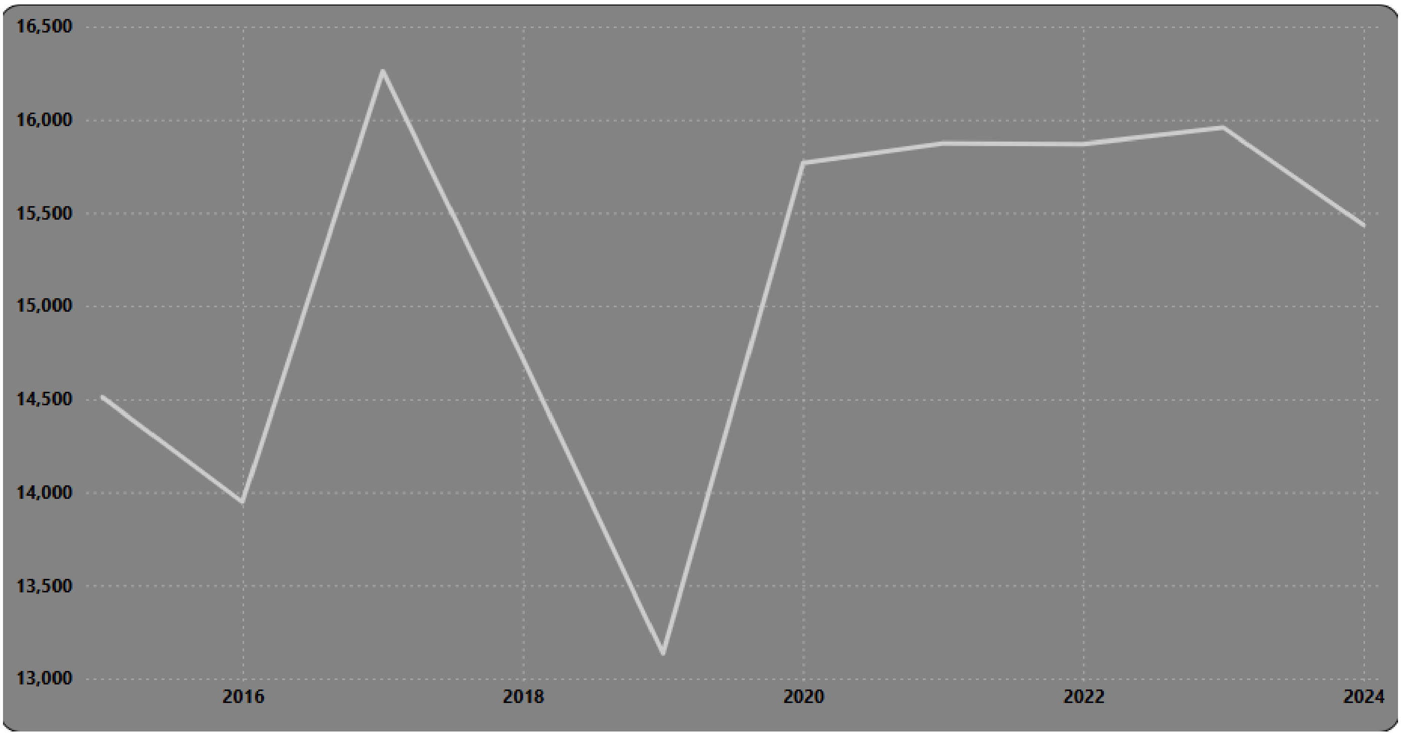
□ Australia
□ Brazil
□ China
□ France
□ Germany
□ India
□ Japan
□ Russia
□ UK
□ USA

3. Total Financial Loss by Year (Line Chart):

The chart shows a **volatile trend in financial loss over the years**.

- Losses were relatively low in 2015, peaked around 2017, dipped significantly in 2018, spiked again around 2019, and then showed another dip in 2020.
- In the year 2019 there was a covid-19, the attack was low as compared to other years and then in the year 2020 the attack issue has peaked as compared to 2019.

TOTAL FINANCIAL LOSS BY YEAR

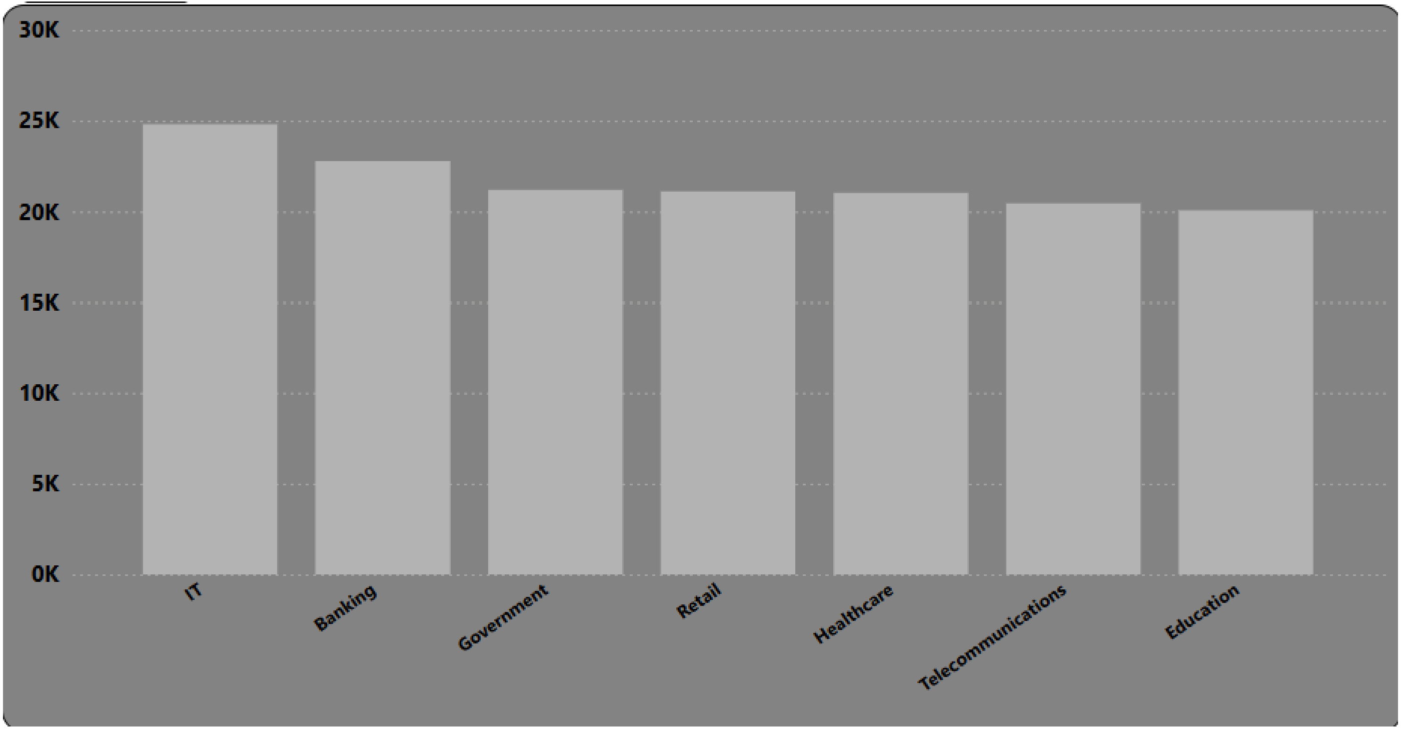


4. **Sum of Financial Loss (Bar Chart):**

- This chart breaks down the financial loss by industry sector.
- **IT** and **Banking** sectors incur the highest financial losses, standing out significantly.
- **Government, Retail, Healthcare, Telecommunications, and Education** follow, with fairly similar levels of loss among them.
- This highlights the critical need for robust cybersecurity in the IT and financial sectors due to their higher financial exposure to attacks.

SUM OF FINANCIAL LOSS

0

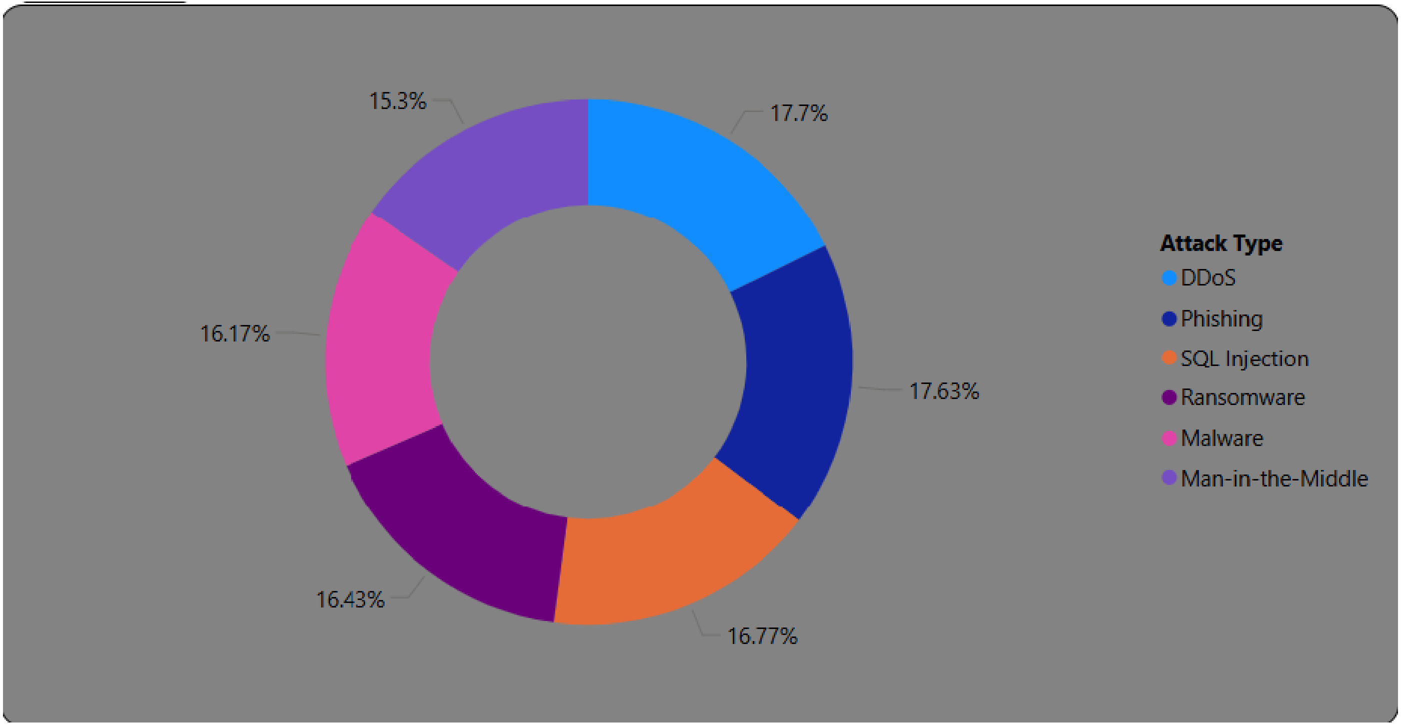


0

5. **Count of Attack Source by Attack Type (Donut Chart):**

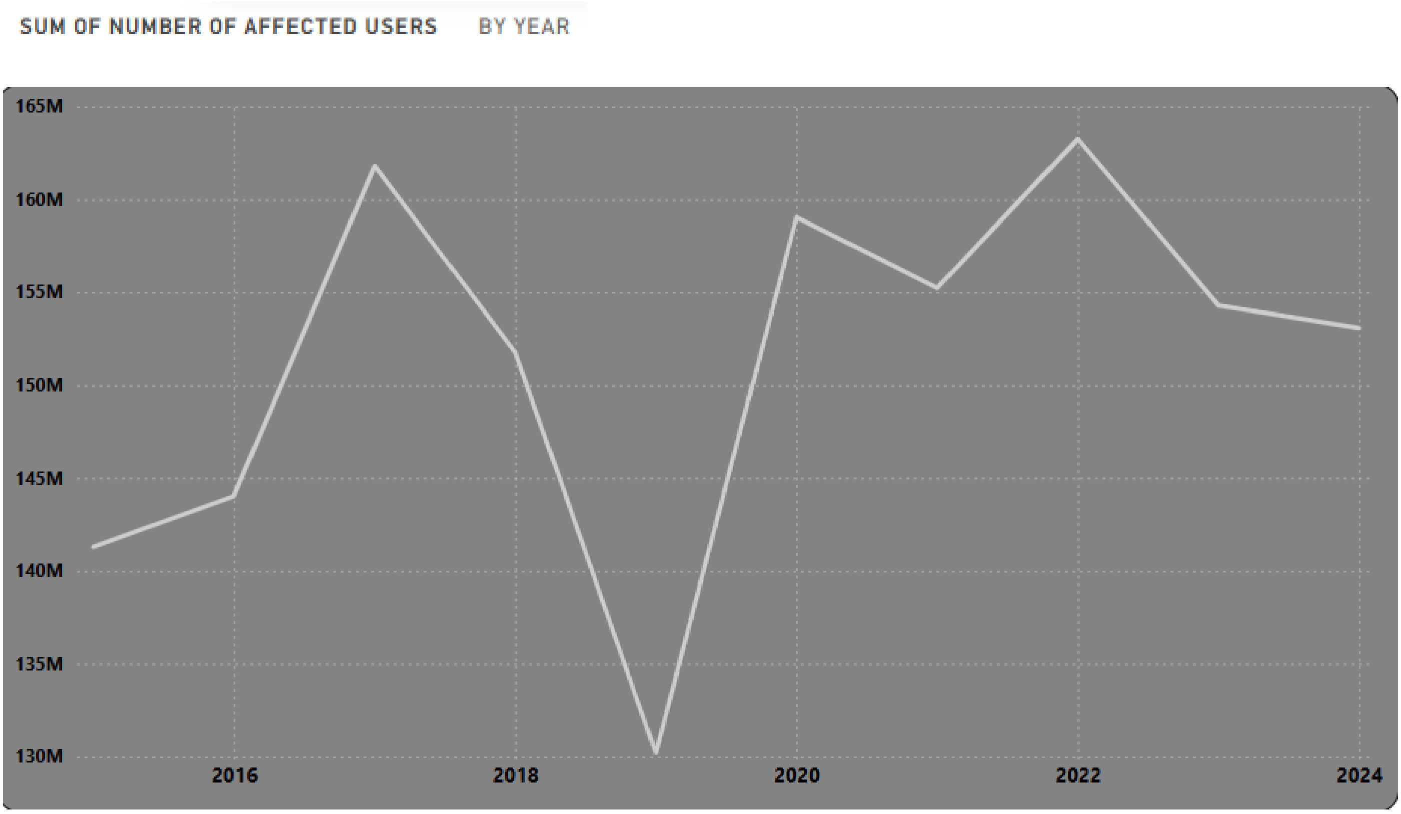
- Illustrates the distribution of different cyberattack types.
- T00he distribution is fairly even, indicating a diverse threat landscape:
    - **DDoS (17.7%)** and **Phishing (17.63%)** are slightly more prevalent.
    - **SQL Injection (16.77%)**, **Ransomware (16.43%)**, **Malware (16.17%)**, and **Man-in-the-Middle (15.3%)** follow closely.
- Given the even distribution of attack types, organizations must implement comprehensive defenses against a variety of methods.

COUNT OF ATTACK SOURCE BY ATTACK TYPE



6. **Sum of Number of Affected Users by Year (Line Chart):**

- This chart depicts the trend of affected users annually from 2015 onwards.
- The trend is **highly fluctuating**:
    - A relatively low number in 2015, rising to a peak around 2017, then a sharp dip in 2018 (indicating a year with significantly fewer affected users, perhaps due to successful preventative measures or a lack of major widespread incidents).
    - The numbers rebound strongly in 2019-2020, followed by a slight decline into 2021.


SUM OF NUMBER OF AFFECTED USERS BY YEAR
165M
160M
155M
150M
145M
140M
135M
130M