Global Cybersecurity Threats

By: Safaa samy mohamed

27/6/2026

(2015 : 2024)

https://github.com/Safaa9924/Global_Cybersecurity

Project current problem

1.**Hard to Identify Most Harmful Attacks:**
Too many attack types and impact measures (losses, users).

2. **Complex Relationships:**
NO link attack source, country, and financial impact

3.Lack of Visual Insight for Decision Makers:
Managers need quick, clear understanding

Solutions Applied

1.Used Pivot Tables, maps, and Stacked Bar Charts to highlight top attack types and losses.

2. Connected multiple variables (Country, Attack Type, Source, Loss) in visual layers.

3. Built visual reports with clear insights for stakeholders.

What Makes This Project Valuable

1. Tailored dashboards that directly address key retail pain points
2. Flexible filtering for granular analysis across attack type , attack source and citys
3. **Actionable Recommendations.**
4. **Helps security teams prioritize risks.**
5. **Visuals enable faster decision-making.**

Project Process

1

DATA CLEANING
&
PROCESSIN

SQL-PYTHON

2

ANLYSIS QUESTIONS

PYTHON

3

FORECASTING QUESTION

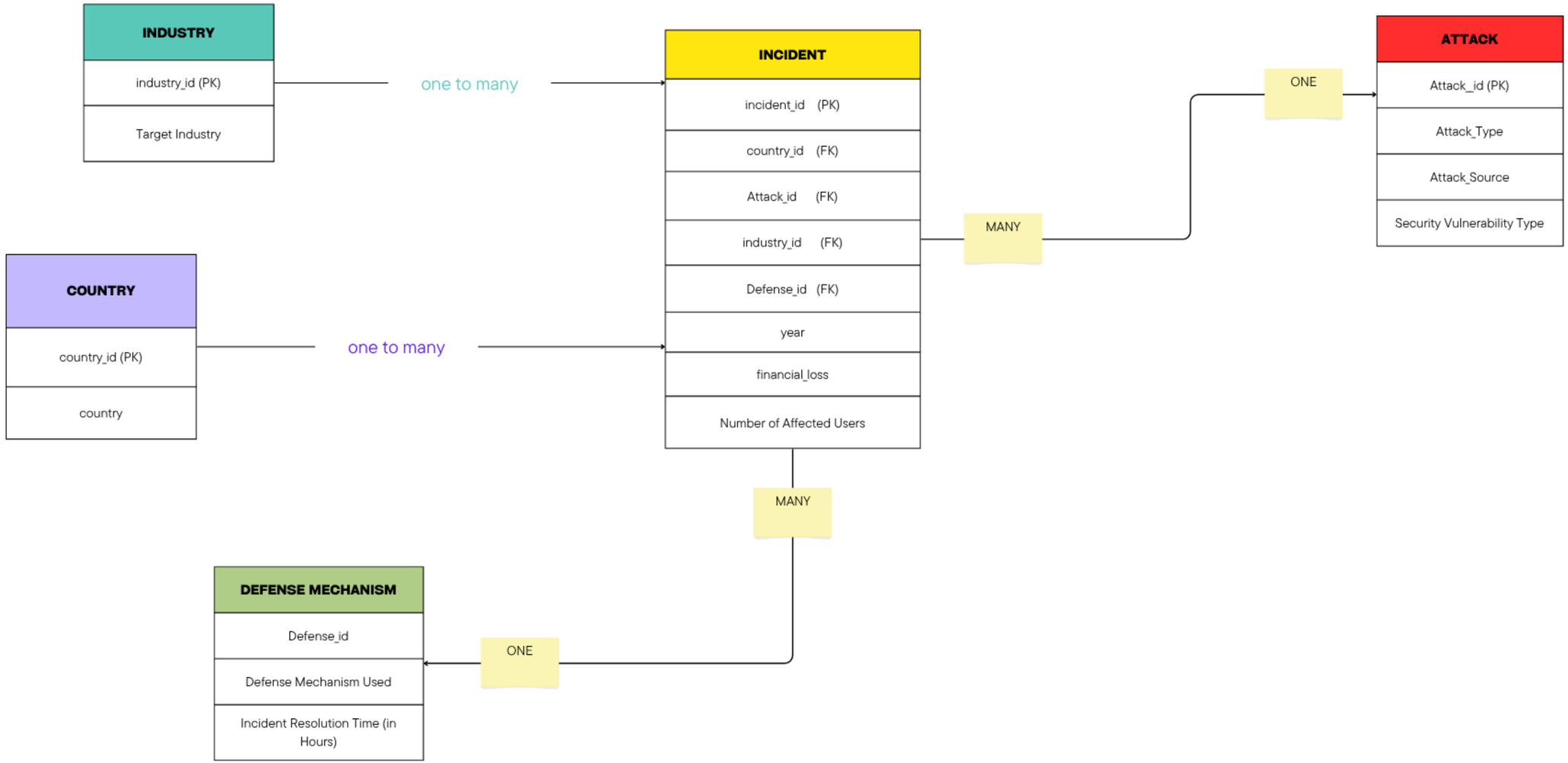
TABLEAU

4

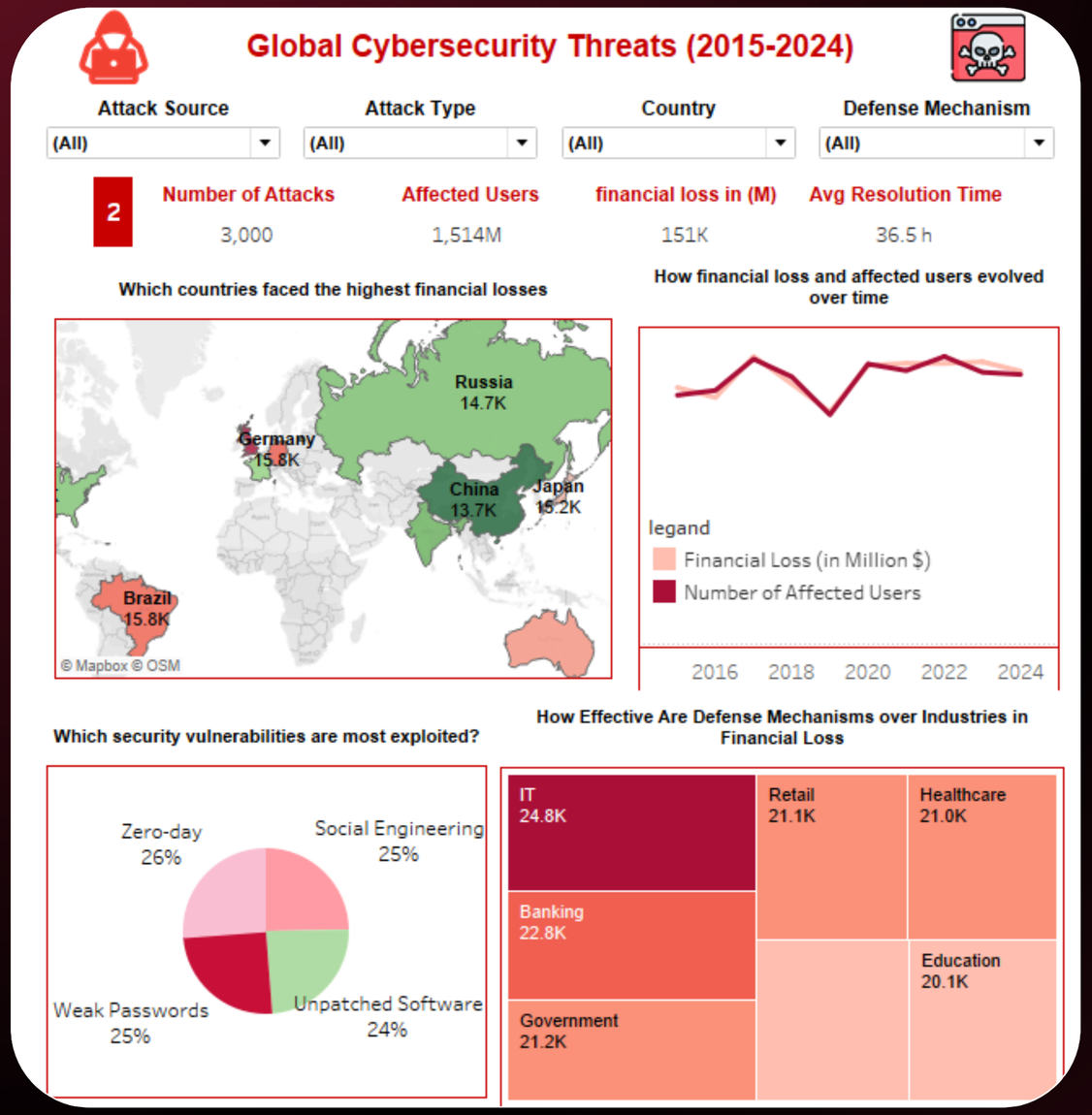
VISUALIZATION DASHBOARD
&PRESENTATION

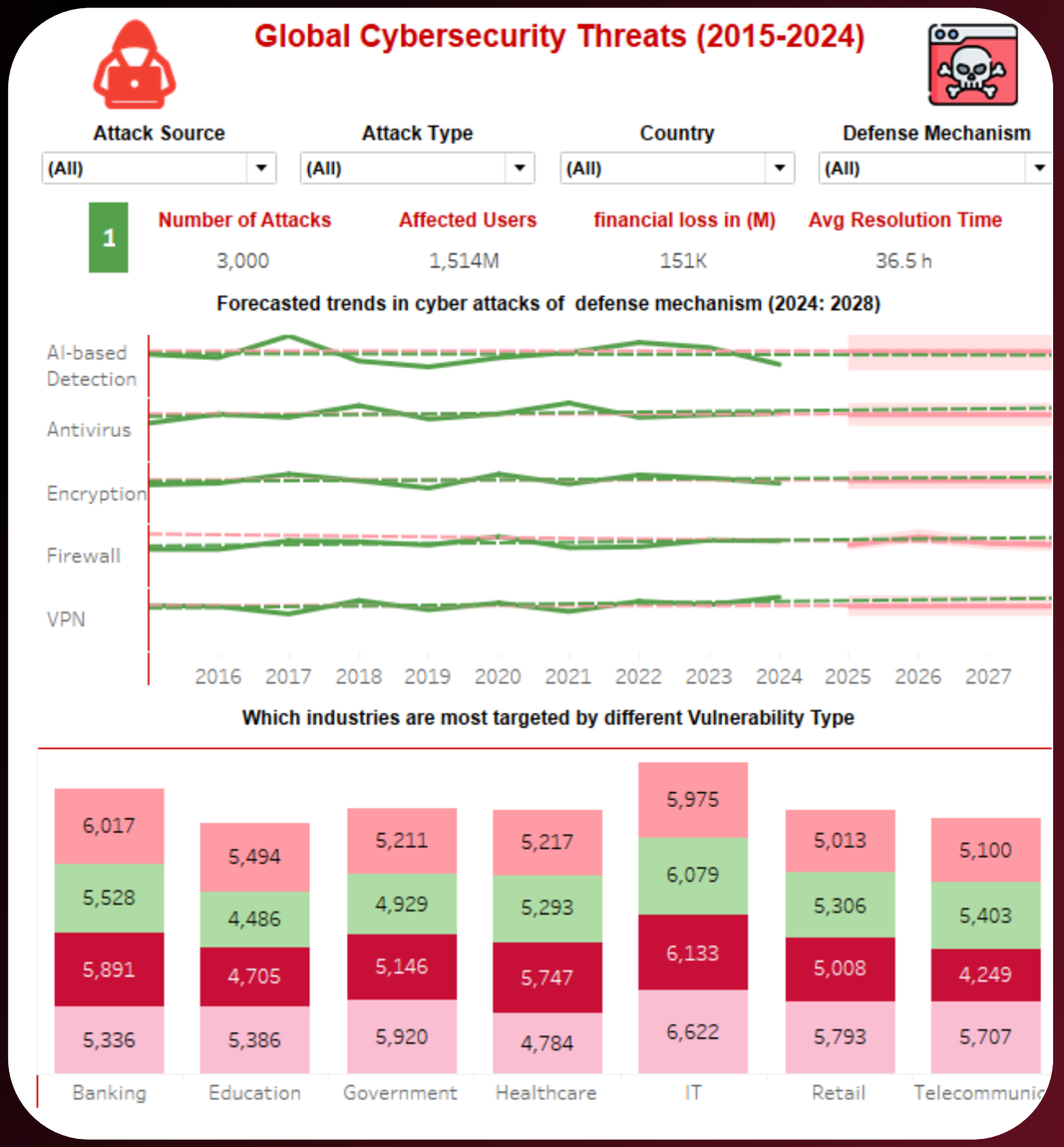
TABLEAU - CANVA

ERD Diagram using SQL



Insights Dashboard

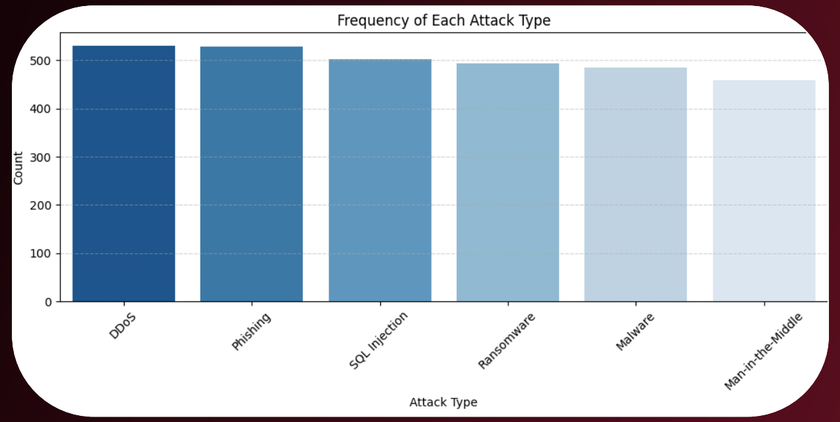




Most Important Insights

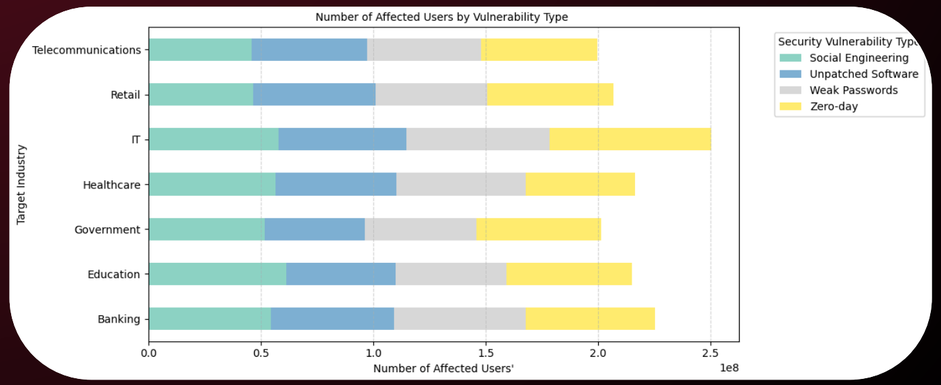
1. TOTAL NUMBR OF ATTACKS ARE **3000**

DDOS AND PHISHING POSE THE HIGHEST RISK IN TERMS OF FREQUENCY



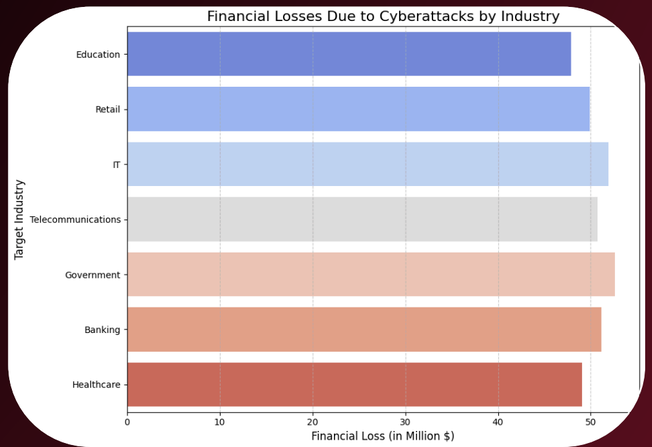
2. TOTAL AFFECTED USERS ARE **1.5 B**

THE BANKING AND IT SECTORS EXPERIENCED THE HIGHEST NUMBERS OF AFFECTED USERS



3. TTAL FINANCIAL LOSS IS **1.5** B

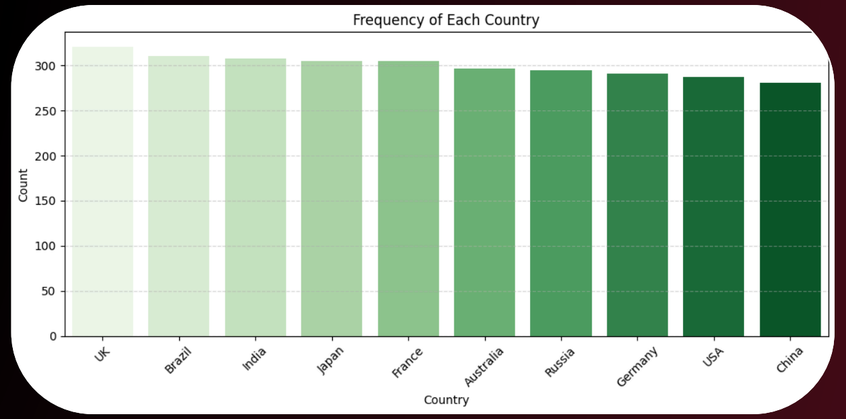
GOVERNMENT AND IT SECTORS INCURRED THE HIGHEST LOSSES,



Most Important Insights

4. CITY MOST ATTACKED

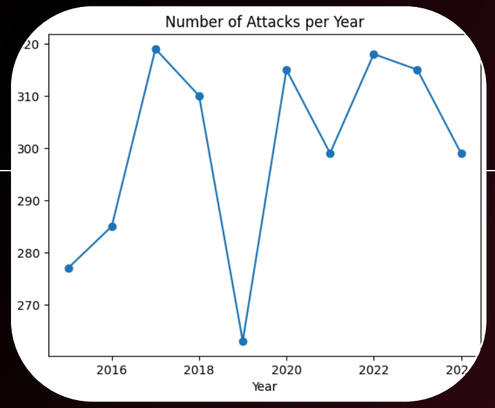
"UK" being the most targeted and "China" the least



5. Attacks over Years

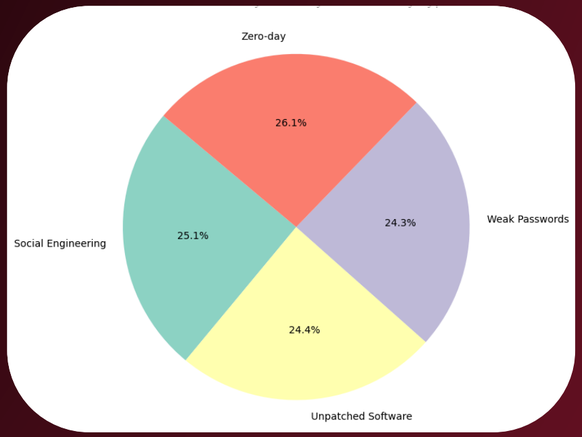
"2017", "2022" the hiest number of attack

"2019" the save year

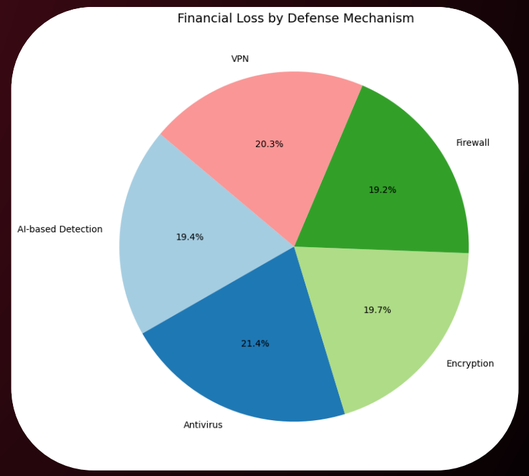


6. Security Vulnerability

Zero-day vulnerabilities accounted for the largest portion of financial loss, representing 26.1% of the total

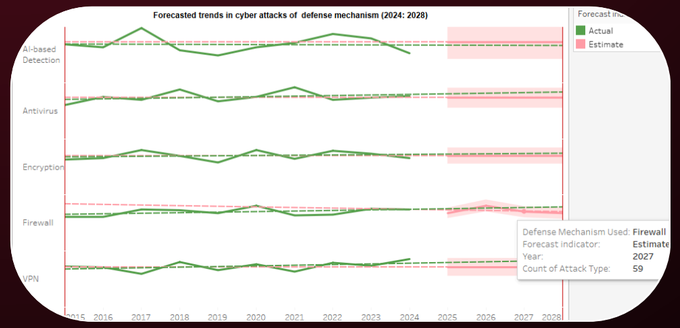


Most Important Insights



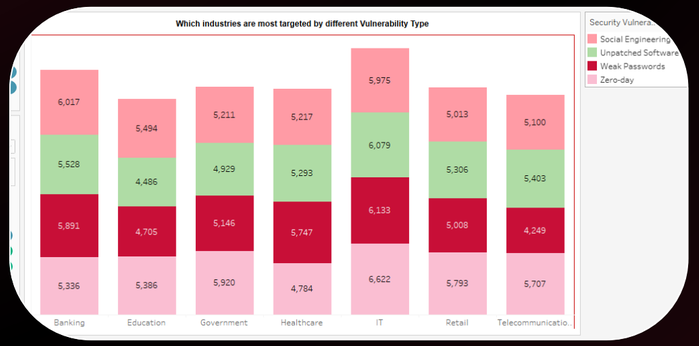
7.Defense Mechanism Used

Antivirus solutions accounted for the largest portion of the loss (21.4%),



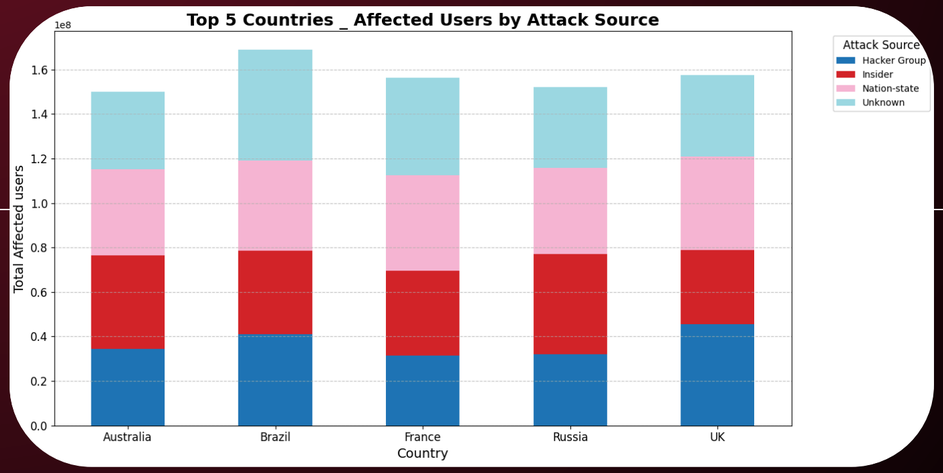
8. Forcasting attack for defense mechanism

It forecasts for the three years 2025-2028 the same number of attacks except for the firewall. It forecasts 57, 67, 59, and 57.It forecasts for "AI-based Detection" the number of attacks is 61.For 'Antivirus,' 'Encryption,' and 'VPN,' the number of attacks was 62, 59, and 60, respectively.



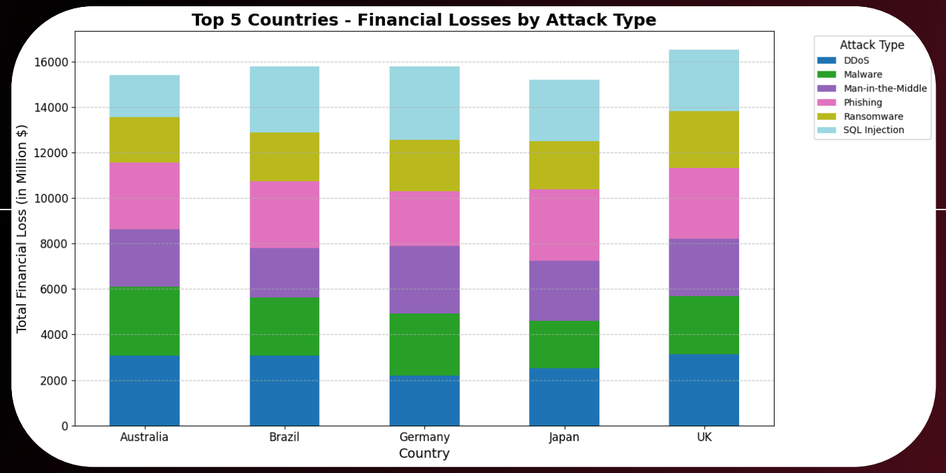
9. Target Industry by vulnerability type

In the IT industry, Zero-day vulnerabilities were responsible for the highest financial losses.In the Education sector, Social engineering attacks led to the greatest share of losses



10. Attack Source

A large portion of cyberattacks remain unattributed, with “Unknown” sources being the most reported.



11. Attack Type

Australia and the UK experienced the highest financial losses due to DDoS attacks, indicating they were the most targeted by this attack type.

Brazil and Germany suffered the most financial impact from SQL Injection attacks

Recomended action plan

1

ENHANCE THREAT DETECTION

PRIORITIZE MONITORING AND EARLY DETECTION OF DDOS AND PHISHING ATTACKS, WHICH ARE THE MOST FREQUENT THREATS.

2

SECTOR-SPECIFIC RISK MITIGATION

FOCUS DEFENSE STRATEGIES ON BANKING, IT, AND GOVERNMENT SECTORS DUE TO HIGH USER IMPACT AND FINANCIAL LOSSES.

3

ZERO-DAY PROTECTION DEVELOPMENT

INVEST IN RESEARCH AND DEPLOYMENT OF ADVANCED TOOLS TO DETECT AND RESPOND TO ZERO-DAY VULNERABILITIES, WHICH CAUSE THE HIGHEST LOSSES.

4

GEOGRAPHIC AND TEMPORAL AWARENESS

ALLOCATE MORE CYBERSECURITY RESOURCES IN UK AND DURING HISTORICALLY HIGH-ATTACK YEARS LIKE 2017 AND 2022.

5

OPTIMIZE DEFENSE MECHANISMS

REEVALUATE THE COST-EFFECTIVENESS OF COMMON TOOLS LIKE ANTIVIRUS.

Thankyou

https://github.com/Safaa9924/Global_Cybersecurity