**Technical Report on Global Cybersecurity Threats (2015–2024)**

**1. Introduction**

This report provides an analytical overview of global cybersecurity threats from 2015 to 2024, highlighting key attack sources, affected industries, countries with the highest impacts, and types of vulnerabilities. The goal is to synthesize and interpret the visual data presented in the cybersecurity dashboard to inform better threat mitigation strategies.

**2. Purpose**

The purpose of this report is to:

* Analyze global cybersecurity trends and threats over the past decade.
* Identify the most vulnerable industries and the most impacted regions.
* Examine the nature of attacks, their sources, and consequences such as user impact and financial losses.
* Provide actionable insights and recommendations to improve cybersecurity defenses.

**3. Story of Data**

The dashboard integrates various data dimensions, including:

* **Attack types** (Phishing, Ransomware, DDoS, etc.)
* **Attack sources** (Hacker Groups, Insiders, Nation-states, Unknown)
* **Targeted industries** (IT, Banking, Healthcare, etc.)
* **Countries by attack origin and impact**
* **User impact and financial loss**
* **Security vulnerabilities exploited**

The narrative captures how cyber threats evolved, which sectors and nations were most affected, and what vulnerabilities were most exploited.

**4. Data Splitting and Preprocessing**

The dataset has been segmented by:

* **Time Frame**: 2015–2024
* **Geographic Scope**: Global, with specific country mentions
* **Sectors/Industries**: IT, Banking, Healthcare, etc.
* **Attack Characteristics**: Type, Source, and Resolution Time
* **Impacts**: User count, financial cost, and severity

Basic preprocessing likely involved cleaning missing values, standardizing country and industry names, categorizing attack types and sources, and aggregating data for visualization.

**5. Pre-Analysis**

Initial analysis focused on identifying:

* The most common **vulnerabilities** (e.g., Zero-day, Weak Passwords)
* **High-risk industries** such as IT and Banking
* Countries frequently used as **attack origins** or most **financially impacted**
* **Resolution times** for different types of attacks

This stage helped define the scope of key indicators to explore further.

**6. In-Analysis**

Significant trends and findings from the dashboard include:

* **Top Industry by Vulnerability**: IT leads with 478 incidents, followed by Banking and Healthcare.
* **Most Common Attack Type**: Phishing appears as the most frequently used method.
* **Most Vulnerable Country**: The UK is the top country by attack source frequency (321).
* **Highest Financial Loss**: Russia reported the largest losses, exceeding $16,500.
* **Most Affected Users**: Zero-day vulnerabilities impacted nearly 396 million users.
* **Sources of Attacks**: Hacker groups and unknown sources contribute heavily to DDoS and SQL injection attacks.
* **Resolution Time**: Phishing attacks have a median resolution time of 18,011–18,562 units (likely in minutes or hours).

**7. Post-Analysis and Insights**

* **IT Sector Is a Prime Target**: Likely due to its central role in infrastructure and data processing.
* **Zero-Day Exploits Pose Severe Risk**: With the highest user impact, urgent patching and early detection are crucial.
* **Human Factors Matter**: Social engineering and weak passwords still account for significant breaches.
* **Global Reach of Attacks**: While attacks originate from specific regions like the UK, their effects are global.
* **Insiders and Unknowns**: A high proportion of threats remain unattributed, suggesting gaps in tracking capabilities.

**8. Data Visualizations & Charts**

Key visual elements from the dashboard:

* **Bar Charts**: Show top industries by attack volume and country-wise attack sources.
* **Treemaps**: Display vulnerability types by number of affected users.
* **Pie Chart**: Compares incident resolution times by attack type.
* **World Map**: Illustrates countries by financial losses.
* **Stacked Bars**: Analyze attack types by source categories.

Each visual aids in storytelling and adds depth to understanding the cybersecurity landscape.

**9. Recommendations and Observations**

**Recommendations**

* **Prioritize IT Sector Security**: Given its high vulnerability rate.
* **Deploy Advanced Threat Detection**: Especially for Zero-day attacks and insider threats.
* **Enhance Password Policies and User Education**: To address common weaknesses.
* **Invest in Attribution Capabilities**: To better identify unknown sources.
* **Focus on Phishing Awareness**: As it remains the leading attack method.

**Observations**

* Human error and poor configurations still dominate the threat landscape.
* The response time to cyber incidents is improving but varies across attack types.
* Some countries may be underreporting due to lack of detection or political reasons.

**10. Conclusion**

The global cybersecurity threat landscape between 2015 and 2024 shows increasing complexity, with IT and Banking sectors facing significant threats from both internal and external actors. Zero-day vulnerabilities and phishing remain critical areas of concern, demanding continuous adaptation of security frameworks. Effective mitigation strategies must include technical controls, user education, and international collaboration.

**11. References & Appendices**

**References**

* Internal data visualizations extracted from the cybersecurity dashboard image.
* Global cybersecurity reports and statistical trends from entities like:
  + IBM X-Force Threat Intelligence Index
  + Verizon Data Breach Investigations Report (DBIR)
  + ENISA Threat Landscape Reports