DATA VISUALIZATION, PRIVACY AND ETHICS PROJECT ON

"ANALYSIS AND IDENTIFICATION OF DATA BREACH INCIDENTS"

GROUP - 04

TEAM MEMBER'S NAME	ROLL ID
Krishna Sai Satvik Mukhe	2024H1540805P
Eswar Panduru	2024H1540841P
Praveen R	2024H1540843P
Harshavardhan Gulla	2024H1540846P
Kushal Devanabanda	2024H1540860P
Tharun Keshav Reddy	2024H1540868P

Key Insights

1. **Common Sectors Affected:**
   - The Web, government, healthcare and financial sectors have the highest number of breaches, especially the web sector on average has billions of records of lost in the breach and has the highest number of breaches.
   - The Retail, Tech and Telecom sectors have also experienced a notable number of breaches.
   - This shows that there is lot of exposure, disclosure and loss of personal information of the people, confidential information of the government, intellectual property and classified information of the companies.

2. **Scale of Data Breaches:**
   - On average 1.27 billion records have been lost.
   - The web sector with companies like Yahoo, VK etc has the highest recorded breach with 137 billion records.
   - The median breach size is 2 million records. This indicates that while some breaches are massive, most of the breaches are significantly smaller.

3. **Breach Methods:**
   - Hacking is the most common method of data breach and accounts for about 60% of the recorded cases due to its efficiency in exploiting weak points in systems.
   - Some of the other major methods used are Lost data, Stolen data, Poor security and Inside jobs.
   - Breaches occurred in the financial sector mainly due to hacking.
   - Breaches in both the government and healthcare sectors have occurred due to poor security setup and hacking.
   - All these breaches could be due to outdated IT infrastructure, poor security setups, human errors and lack of adaptability.

4. **Trend Over the Years:**
    - There has been a steady increase in the number of data breach cases from 2004 to 2010 and the highest numbers of breaches happened in 2011 (35 cases), 2013 (31 cases) and 2016 (33 cases).
    - After 2011, the trend fluctuates with alternate rise and fall.
    - In 2017 a sharp decline is observed. This is because companies started adopting cybersecurity measures like encryption and incident response plans. The EU introduced General Data Protection Regulation (GDPR), encouraged organizations to adopt more robust security measures.

5. **Sources of Breach Reports are Concentrated:**
    - The Guardian reported the highest number of cases, accounting for 71 billion breached records.
    - Beta News reported two cases, accounting for 137 billion breached records.

6. **Entities with Most Breaches:**
    - AOL, Citigroup, and Yahoo reported the highest number of breaches, each experiencing 3 incidents.
    - Other organizations like AT&T, Dropbox, Sony Pictures, Uber, and US Military experienced 2 breaches each.
    - Yahoo stands out as the organization with the largest total records lost, amounting to 1.5 billion records, despite having only three breaches.
    - The Unique Identification Authority of India (Aadhaar) reported a single breach but lost 1 billion records, highlighting the massive scale of this incident.

Recommendations

1. **Strengthen Cybersecurity Measures:**
    - Implement Multi-Factor Authentication across all systems so that an extra layer of protection is added against unauthorized access.
    - Ensure that the sensitive data is encrypted both in transit and at rest thus making it unreadable even if stolen.
    - Regularly update software and apply security patches to close vulnerabilities that hackers exploit.
    - Implement Firewalls and Intrusion Detection Systems to monitor and control network traffic and detect suspicious activities.

2. **Improve Organizational Practices:**
    - Organize regular cybersecurity training to educate employees about phishing, social engineering, and other threats.
    - Implement a "least privilege" policy, to ensure that the employees have access to the data that is only necessary for their roles.
    - Develop a robust incident response plan to quickly address breaches when they occur.

3. **Regulatory Compliance and Governance:**
   - Ensure compliance with regulations like GDPR, HIPAA, and PCI DSS. These laws enforce stricter data management practices that reduce breaches.
   - Conduct regular security audits and risk assessments to identify vulnerabilities proactively.

4. **Address Common Breach Methods:**
   - Implement threat detection tools powered by AI to identify and neutralize hacking attempts in real-time.
   - Conduct regular security assessments to identify misconfigurations or outdated systems.
   - Mandate encryptions for all portable devices and storage media.

5. **Collaboration Across Sectors:**
   - Governments and industries should collaborate and share threat intelligence to stay ahead of emerging cyber threats.

6. **Promote Transparency in Reporting:**
   - Encourage organizations to disclose breaches promptly while providing clear communication about their impact and mitigation steps. This helps build trust with the stakeholders and helps improve industry-wide practices.

Execution Plan

The following execution plan has been developed to implement the recommendations:

Category	Task	Phase	Timeline
Strengthen Cybersecurity Measures	Implement Multi-Factor Authentication (MFA)	Short-term	0–3 months
	Encrypt sensitive data	Short-term	0–3 months
	Apply software updates and patches	Short-term	0–3 months
	Install Firewalls and IDS/IPS	Mid-term	3–6 months
	Set up centralized log management	Mid-term	3–6 months
	Conduct penetration testing	Long-term	6–12 months
Improve Organizational Practices	Conduct cybersecurity training for employees	Short-term	0–3 months
	Implement least privilege policy	Short-term	0–3 months
	Develop and simulate incident response plan	Mid-term	3–6 months

Category	Task	Phase	Timeline
Regulatory Compliance and Governance	Update security policies and access controls	Mid-term	3–6 months
	Conduct compliance gap assessment	Short-term	0–3 months
	Assign a compliance officer	Short-term	0–3 months
	Conduct security audits and risk assessments	Mid-term	3–6 months
	Implement automated compliance reporting tools	Mid-term	3–6 months
Address Common Breach Methods	Install AI-based threat detection tools	Short-term	0–3 months
	Encrypt all portable devices and storage	Short-term	0–3 months
	Audit and replace outdated IT infrastructure	Mid-term	3–6 months
Collaboration Across Sectors	Join industry threat intelligence networks (ISACs)	Mid-term	3–6 months
	Participate in cybersecurity drills with CERTs	Mid-term	3–6 months
Promote Transparency in Reporting	Define internal breach reporting protocol	Short-term	0–3 months
	Create public communication templates for breaches	Short-term	0–3 months
	Build a public transparency dashboard	Long-term	6–12 months

References

Wikipedia

https://www.kaspersky.com/resource-center/definitions/data-breach

https://www.balbix.com/insights/data-breach-prevention-best-practices/

https://www.digitalguardian.com/blog/prevent-data-loss

https://www.mimecast.com/content/data-breach-prevention/