### **Kitewdrks**

# Top 11 Data Breaches in 2024 and Their Risk **Exposure Scores**



Kiteworks' Risk Exposure Index provides a comprehensive framework for understanding breach severity through multiple dimensions. With over 1.7 billion individuals receiving breach notifications in 2024 alone, understanding these incidents through a multifaceted lens is critical for organizations seeking to protect their most valuable assets.

## **Risk Exposure Index Framework**

Risk Exposure Index (REI) evaluates breaches on a scale of 1-10 by weighing seven key factors:

10% **Attack Vector Sophistication** Evaluates the technical complexity of the attack methodology used.



**Number of Records Exposed** The raw count of compromised records serves as the foundation, though it tells only part of the story.

### 10%

**Supply Chain Impact Assessment** Measures the cascade effect on connected organizations and ecosystems.

### 10%

Ransomware Involvement Considers whether ransomware was deployed, ransom amounts, payment decisions, and operational impact duration.

### 20%

**Financial Impact Estimation** Calculates both direct costs (remediation, notification, legal fees) and indirect costs (business disruption, customer churn, reputational damage).

### 20% **Data Sensitivity** Classification

Assesses the nature of exposed information, from basic contact details to protected health information and financial data.

### 15%

**Regulatory Compliance Implications** Evaluates the regulatory landscape applicable to the breach, including potential penalties and notification requirements.

### The resulting score provides a normalized measurement of breach severity:

# 8.5-10

Catastrophic Impact

7.0-8.4

Severe Impact Moderate to **High Impact** 

5.5-6.9

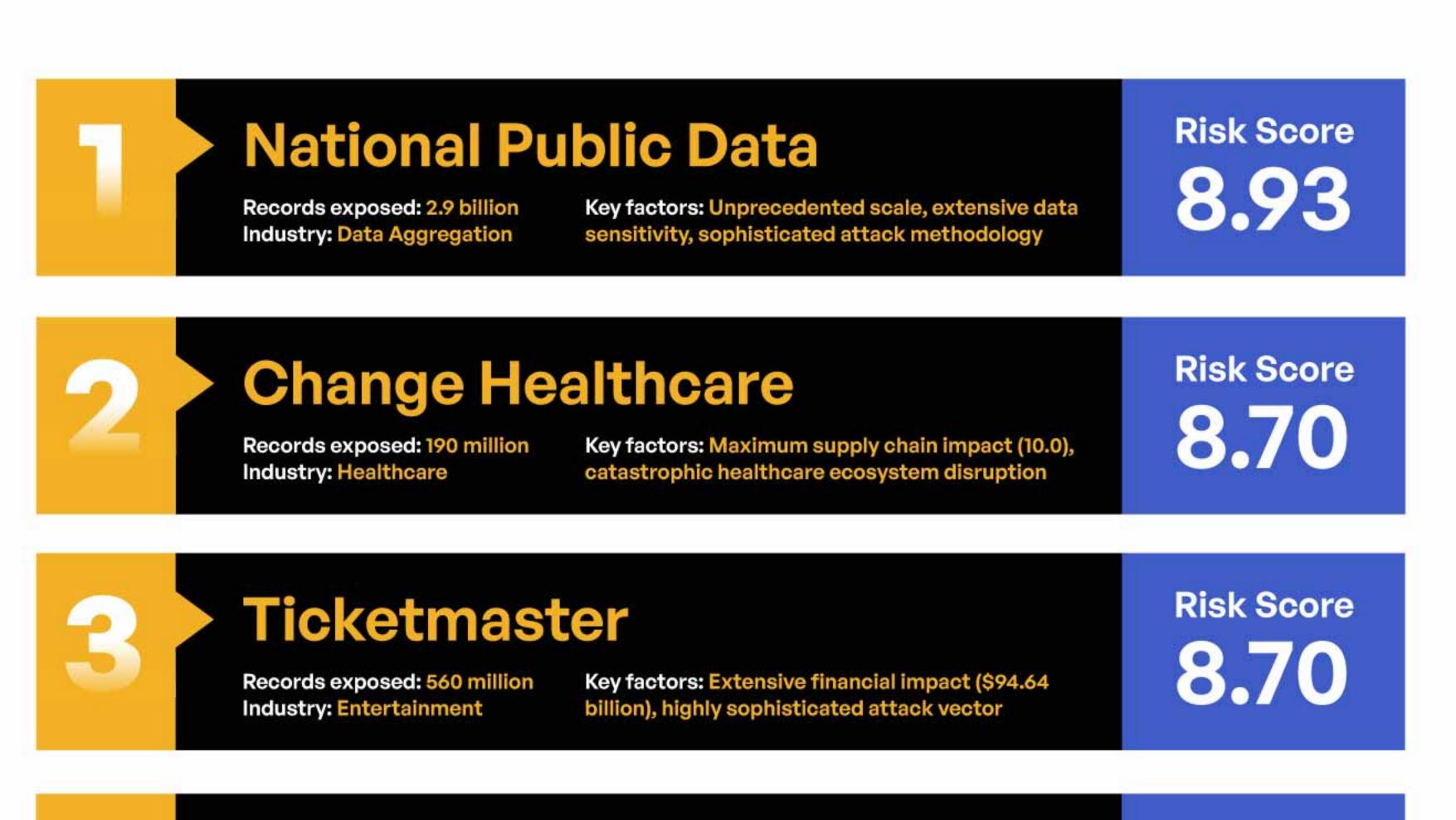
4.0 - 5.4

Moderate Impact

1.0-3.9

Limited Impact

## **Top 11 Breaches Ranked by Risk Score**







Key factors: High data sensitivity, exposure of 86 million Social Security numbers

**Risk Score** 8.50



## **Hot Topic**

Records exposed: 56.9 million Industry: Retail

Key factors: Complete payment card details exposed, significant supply chain impact

**Risk Score** 7.70

## LoanDepot

Records exposed: 16.9 million **Industry: Financial Services** 

Key factors: Highly sensitive financial documentation, ransomware involvement **Risk Score** 7.60

6

# **Kaiser Foundation Health Plan**

Records exposed: 13.4 million Industry: Healthcare

**Key factors: Protected health information** exposure, third-party supply chain vulnerability **Risk Score** 7.60



# **Dell Technologies**

**Records exposed: 49 million** Industry: Technology

### Key factors: Corporate espionage indicators, sophisticated spear-phishing methodology

**Risk Score** 7.20

## **DemandScience**

Records exposed: 122.8 million Industry: Marketing/Data

Key factors: Extensive record count, business impact from compromised primary assets

7.10

**Risk Score** 

## MC2 Data

**Records exposed: 100 million Industry: Data Analytics** 

Key factors: Consumer behavior profiles, significant financial impact

**Risk Score** 6.90

**U.S. Environmental Protection Agency** Records exposed: 8.46 million Industry: Government

Key factors: Critical infrastructure details, potential state-sponsored attack indicators

**Risk Score** 6.20

# **Key Risk Factor Correlations**

Analysis reveals the relative importance of different factors in determining breach severity:

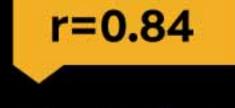












### Financial Impact:

Shows the strongest correlation with overall risk score, reflecting its role as both a consequence of other factors and a direct measure of organizational harm.



### Data Sensitivity:

**Demonstrates that** what was stolen often matters more than how much was taken, particularly in healthcare and financial services breaches.



### Regulatory **Compliance:**

**Organizations subject** to multiple regulatory regimes experienced 27% higher breach costs, reflecting both potential penalties and compliance complexity.



### Number of Records Exposed:

Shows moderate correlation with risk score, confirming its relevance while demonstrating it's far from the only important factor.



### Ransomware Involvement:

While the direct correlation with overall risk is modest, ransomware shows much stronger correlation with operational impact, highlighting its primary effect on business continuity.

## **Most Influential Risk Factors**

Multi-factor analysis across all breaches reveals the three most influential factors in determining breach severity:

## Data Sensitivity

-

Ø

The nature of compromised information proved the single most important factor in determining real-world impact, with financial and health data breaches creating the most significant individual harm.



# Financial Impact

The economic consequences for the breached organization and affected individuals strongly influenced overall risk assessment, with ecosystem disruption creating particularly severe impacts.



# Regulatory Compliance

The regulatory environment significantly shaped breach outcomes, with highly regulated industries facing more substantial consequences and response requirements.



### **Download the Full Report**

To access the complete analysis of 2024's most significant data breaches, including detailed case studies, mitigation strategies, and industry-specific insights, download the full report at

https://www.kiteworks.com/top-data-breaches-report/

**Kitewarks**