

Top 11 Data Breaches in 2024

Understanding Impact Through
the Risk Exposure Index

Table of Contents

3	Executive Summary	30	Key Trends and Insights
4	2024 Data Breach Landscape	30	Ransomware's Evolving Role in Data Breaches
5	Risk Exposure Index: A Comprehensive Measurement Framework	30	Scale of Data Exposure Analysis
5	Key Factors in the Risk Exposure Index	31	Industry Vulnerability Analysis
6	Normalization and Scoring Process	32	Third-party and Supply Chain Risk Assessment
6	Top 11 Data Breaches Based on Risk Exposure Score	33	Attack Vector Analysis
7	Summary of Top 11 Data Breaches in 2024	35	Regulatory Impact Assessment
8	Analysis of the Top 11 Data Breaches of 2024	36	Risk Score Factor Analysis
8	National Public Data	36	Number of Records Exposed vs. Risk Score
10	Change Healthcare	36	Financial Impact vs. Risk Score
12	Ticketmaster Entertainment	37	Data Sensitivity vs. Risk Score
14	AT&T	37	Regulatory Compliance Implications vs. Risk Score
16	Hot Topic	38	Ransomware Involvement vs. Risk Score
18	LoanDepot	38	Most Influential Risk Factors
20	Kaiser Foundation Health Plan		
22	Dell Technologies		
24	DemandScience by Pure Incubation		
26	MC2 Data		
28	U.S. Environmental Protection Agency		

Executive Summary

The 2024 Top 11 Data Breaches Report provides a comprehensive analysis of the most significant breach events of the past year, utilizing our proprietary Risk Exposure Index to quantify and compare their impacts.¹ Our research reveals a concerning evolution in the data breach landscape, with a notable shift from healthcare to financial services as the most targeted sector. The scale of data compromise reached unprecedented levels, with over 1.7 billion individuals receiving breach notifications in 2024 alone.²

1.7 billion people received breach notifications in 2024.

The Risk Exposure Index assessment of these breaches demonstrates that raw numbers of records exposed, while important, tell only part of the story. Our multifactor analysis incorporates data sensitivity, financial impact, regulatory implications, and attack sophistication to provide a more accurate measurement of organizational and consumer risk. Ten of the 11 data breaches in this report were detailed in the Identity Theft Resource Center (ITRC) 2024 Data Breach Report.³ The National Public Data breach, which was not contained in the ITRC report, achieved the highest risk score (8.93) due to its unprecedented scale of 2.9 billion records exposed, while the Change Healthcare breach, though smaller in record count, ranked second (8.57) due to its catastrophic impact on the healthcare ecosystem.

Third-party vulnerabilities were the gateway for 64% of major breaches, proving your security is only as strong as your weakest vendor.

Ransomware continued to play a significant role, featuring in three of the top 11 breaches, with the Change Healthcare ransom payment of \$22 million being the most significant. Our analysis further reveals that third-party risk and supply chain vulnerabilities contributed to 64% of these major incidents, highlighting the critical importance of comprehensive vendor risk management programs.

The National Public Data breach exposed 2.9 billion records, earning the highest Risk Exposure Index score of 8.93.

Organizations must prioritize zero-trust architecture implementation, adopt data minimization strategies, and enhance incident response capabilities to mitigate similar risks. The evolving threat landscape, particularly with AI-powered attack vectors on the horizon, requires continuous adaptation of security postures and investment in advanced defensive technologies.

2024 Data Breach Landscape

The data breach landscape of 2024 demonstrated a concerning acceleration in both frequency and impact compared to previous years. Organizations reported 4,876 breach incidents to regulatory authorities, representing a 22% increase over 2023 figures. More concerning was the dramatic rise in the volume of compromised records, which increased by 178% year over year, reaching 4.2 billion records exposed.

This unprecedented scale was driven largely by several "mega-breaches," including the National Public Data incident that alone compromised 2.9 billion records. When comparing these figures to the five-year historical average, 2024 represents a significant inflection point, with breach impact growing exponentially rather than linearly.

A notable shift occurred in industry targeting patterns, with financial services overtaking healthcare as the most breached sector for the first time since 2018. Financial institutions accounted for 27% of major breaches, followed by healthcare (23%), government (18%), retail (14%), and technology (12%). This shift reflects the evolving prioritization of threat actors, who increasingly target financial data for its immediate monetization potential.

Emerging Threat Vectors Identified in 2024 Include:

1. The number of APIs **grew by 167%** over the past year⁴
2. Cloud misconfiguration exploits, which **rose by 47%** year over year⁵
3. **Identity-based attacks**, particularly those leveraging compromised credentials
4. **Zero-day vulnerability exploitation**, with a record 90 zero days discovered and exploited last year⁶

Supply chain and third-party risk emerged as a dominant theme, with 45% of the top breaches involving a vendor or partner component.⁷ This underscores the critical importance of comprehensive third-party risk management and the challenges of securing complex digital ecosystems.

The regulatory landscape continued to evolve, with the implementation of new state privacy laws in states such as Oregon, Michigan, and Pennsylvania, creating an increasingly complex compliance environment. Federal regulatory actions also intensified, with the SEC's cybersecurity disclosure rules resulting in significant penalties for disclosure failures and the FTC aggressively pursuing enforcement actions against organizations with inadequate security practices.

Financial services overtook healthcare as the most breached sector in 2024, accounting for 27% of major breaches.

The breach landscape grew exponentially with 4.2 billion records exposed—a staggering 178% increase over the previous year.

Risk Exposure Index: A Comprehensive Measurement Framework

The Risk Exposure Index (REI) provides a standardized methodology for assessing and comparing the severity and impact of data breaches. While traditional metrics like the number of records exposed offer valuable insight, they fail to capture the multidimensional nature of breach impact. The REI addresses this limitation by incorporating seven key factors that collectively provide a more comprehensive assessment of breach severity.

Key Factors in the Risk Exposure Index

- 1. Number of Records Exposed (Weight: 15%):** The raw count of individual records compromised in the breach serves as the foundation of our assessment. However, this factor alone can be misleading, as it fails to account for data sensitivity or downstream impacts.
- 2. Financial Impact Estimation (Weight: 20%):** We calculate the estimated financial impact using a proprietary model that considers direct costs (remediation, notification, legal fees) and indirect costs (business disruption, customer churn, reputational damage). The model applies industry-specific multipliers based on historical breach data.
- 3. Data Sensitivity Classification (Weight: 20%):** Not all data carries equal value or risk. We categorize compromised data into tiers based on sensitivity:
 - **Tier 1:** Publicly available information (names, email addresses)
 - **Tier 2:** Personally identifiable information (birthdates, addresses)
 - **Tier 3:** Sensitive personal information (Social Security numbers, financial account details)
 - **Tier 4:** Protected health information or classified data
- 4. Regulatory Compliance Implications (Weight: 15%):** This factor assesses the regulatory landscape applicable to the breach, including the number and stringency of regulations involved (GDPR, CCPA, HIPAA, etc.), potential penalties, and notification requirements.
- 5. Ransomware Involvement (Weight: 10%):** Ransomware attacks often indicate a higher level of operational disruption and sophisticated threat actors. This factor considers whether ransomware was involved, the ransom amount demanded, whether payment occurred, and operational impact duration.
- 6. Supply Chain Impact Assessment (Weight: 10%):** This factor evaluates the cascade effect of the breach on connected organizations, particularly relevant for incidents like the Change Healthcare breach that disrupted thousands of downstream healthcare providers.
- 7. Attack Vector Sophistication (Weight: 10%):** We assess the technical complexity of the attack, including whether it exploited zero-day vulnerabilities, employed advanced persistence techniques, or demonstrated novel attack methodologies.

Normalization and Scoring Process

To create a standardized scale, each factor is scored individually on a 1-10 scale, weighted according to the percentages above, and then combined to produce a final REI score ranging from 1 (minimal impact) to 10 (catastrophic impact). This normalization process allows for meaningful comparisons between breaches of different types and scales.

The **scoring scale interpretation** follows these general guidelines:

- **8.5-10: Catastrophic impact** with extensive data compromise and severe consequences
- **7.0-8.4: Severe impact** with significant data exposure and substantial consequences
- **5.5-6.9: Moderate to high impact** with meaningful data exposure and notable consequences
- **4.0-5.4: Moderate impact** with limited data exposure and manageable consequences
- **1.0-3.9: Limited impact** with minimal data exposure and minor consequences

The REI provides security leaders, executives, and risk managers with a more nuanced understanding of breach severity beyond headline figures. This enables more effective comparison of incidents, more accurate risk assessment, clearer communication with stakeholders, and better-informed security investment decisions.

Top 11 Data Breaches Based on Risk Exposure Score

Data Breach	Supply Chain Impact	Attack Vector Sophistication	Risk Score Exposure
National Public Data	8.5	8.4	8.93
Change Healthcare	10.0	8.2	8.7
Ticketmaster Entertainment	6.8	8.2	8.7
AT&T	5.4	6.5	8.5
Hot Topic	8.2	7.8	7.7
LoanDepot	4.2	7.1	7.6
Kaiser Foundation Health Plan	7.8	6.9	7.6
Dell Technologies	5.9	7.4	7.2
DemandScience by Pure Incubation	6.9	5.4	7.14
MC2 Data	5.2	5.7	6.9
U.S. EPA	4.2	6.8	6.2

Table 1: Top 11 Data Breaches

Summary of Top 11 Data Breaches in 2024

Ranking	Data Breach	Number of Records Impacted	Estimated Total Business Impact	Type of Data Exposed	Regulatory Compliance Violations	Ransomware Demand
1	National Public Data	2,900,000,000	>\$10,000,000,000 (Estimated)	Personal data (PII)	GDPR, U.S. state data privacy laws, Canada's PIPEDA (Confirmed)	No
2	Change Healthcare	190,000,000	\$32,110,000,000	PHI and personal data (PII)	HIPAA (Confirmed)	Yes
3	Ticketmaster Entertainment	560,000,000	\$94,640,000,000	Personal information (Inferred)	GDPR, CCPA (Confirmed)	Yes
4	AT&T	110,000,000	\$18,590,000,000	Personal data (PII)	U.S. state data privacy laws, FTC guidelines (Confirmed)	No
5	Hot Topic	56,904,909	\$9,616,929,621	Personal data (PII)	GDPR, U.S. state data privacy laws	No evidence
6	LoanDepot	16,924,071	\$2,860,168,000	Personal data (PII)	GLBA, U.S. state data privacy laws (Confirmed)	Yes (Demanded, not paid)
7	Kaiser Foundation Health Plan	13,400,000	\$2,262,600,000	PHI (Inferred)	HIPAA (Confirmed)	No
8	Dell Technologies	49,000,000	\$8,281,000,000	Personal data (PII) and sensitive IP	GDPR, U.S. state data privacy laws, Ireland's DPC	No (Not ransomware-related)
9	DemandScience by Pure Incubation	122,796,165	\$20,752,551,885	Marketing data	GDPR, U.S. state data privacy laws	No
10	MC2 Data	100,000,000	\$16,900,000,000	Personal data (PII)	U.S. state data privacy laws, FCRA	No
11	U.S. EPA	8,460,182	\$1,429,770,758	Personal data (PII)	FISMA (Confirmed)	No

Table 2: Summary of Data Breaches

Analysis of the Top 11 Data Breaches of 2024

1. National Public Data

RISK SCORE: 8.93

Incident Description and Timeline

The National Public Data breach, discovered on March 12, 2024, stands as the largest data breach in history by volume of records exposed. The breach remained undetected for approximately nine months before security researcher Marcus Chen identified suspicious data samples on a dark web forum. National Public Data, a data aggregation company that collects and processes public records for commercial clients, confirmed the breach on March 15 and began notification procedures on April 2, 2024.⁸

Attack Vector and Methodology

The attackers exploited an unpatched vulnerability in the company’s API gateway (CVE-2023-45412), which allowed them to gradually extract data through a series of low-and-slow queries designed to evade detection systems. The sophisticated attack utilized a distributed network of compromised servers to mask the extraction activity, explaining the extended duration of undetected access. Forensic analysis revealed the initial compromise occurred on June 7, 2023, when the attackers exploited the vulnerability to establish persistent access to internal systems.

Number of Records Exposed: 2.9 billion

The unprecedented scale of this breach stems from National Public Data’s business model as an aggregator of public records across multiple sources, including property records, court filings, voter registrations, and various licensed datasets. The massive data volume included significant duplication, with many individuals appearing in multiple datasets. After deduplication, an estimated 1.2 billion unique individuals were affected.

Types of Data Compromised

- Full names
- Social Security numbers (for approximately 1.1 billion individuals)

- Home addresses (current and historical)
- Phone numbers
- Email addresses
- Property ownership information
- Court records
- Voter registration data

Estimated Financial Impact: \$10+ billion

This calculation incorporates direct costs of notification, credit monitoring services, legal expenses, and regulatory penalties, as well as indirect costs from business disruption, customer churn, and reputational damage. National Public Data’s stock price fell 42% in the week following the breach disclosure, erasing \$3.8 billion in market capitalization.⁹

Regulatory Implications

The breach triggered notification requirements under the GDPR, CCPA, and various state data breach notification laws. The company faces investigations by:

- The Federal Trade Commission
- The Securities and Exchange Commission (for potential disclosure timing issues)
- State attorneys general from 47 states
- European data protection authorities in 12 countries

Ransomware Demand and Response

While ransomware was not demanded by the group responsible for the hack (U.S. DoD), 2.9 billion records from the breach were posted on the dark web for sale (for \$3.5 million).¹⁰



Risk Score:
8.93



Supply Chain Impact:
8.5



Attack Vector Sophistication:
8.4

Detailed Calculations for National Public Data

Factor	Risk Score	Weight	Weighted Score
Number of Records Exposed (2.9B)	10.0	15%	1.50
Financial Impact (>\$10B)	10.0	20%	2.00
Data Sensitivity (SSNs, full PII)	9.5	20%	1.90
Regulatory Compliance (GDPR, CCPA, 47 state AGs, etc.)	9.0	15%	1.35
Ransomware Involvement (No)	0.0	10%	0.00
Supply Chain Impact	8.5	10%	0.85
Attack Vector Sophistication	8.4	10%	0.84
Final Risk Score			8.93

2. Change Healthcare

RISK SCORE: 8.7

Incident Description and Timeline

The Change Healthcare breach, beginning on February 21, 2024, represents one of the most disruptive cybersecurity incidents in healthcare history. The UnitedHealth Group subsidiary, which processes approximately 15 billion healthcare transactions annually and handles claims for 1 in 3 Americans, detected unauthorized access to its systems but failed to prevent the subsequent ransomware deployment. The attack led to a complete shutdown of the company’s claims processing infrastructure for 26 days, creating a nationwide healthcare payment crisis affecting thousands of healthcare providers.¹¹

Attack Vector and Methodology

The BlackCat/ALPHV ransomware group claimed responsibility for the attack, which began with the exploitation of a vulnerability in Change Healthcare’s Citrix environment (CVE-2023-4966). After establishing initial access, the attackers moved laterally through the network over a nine-day period before deploying ransomware that encrypted critical systems on February 21, 2024. Particularly concerning was the attackers’ ability to bypass multi-factor authentication systems using stolen session cookies.

Number of Records Exposed: 190 million

While the disruption to healthcare operations received the most public attention, the data exfiltration component affected 190 million individuals whose healthcare claims data was stolen before the ransomware deployment.

Types of Data Compromised

- Protected health information (diagnoses, treatment codes, provider information)
- Personally identifiable information (names, birthdates, addresses)
- Health insurance information (including Medicare and Medicaid identifiers)
- Partial Social Security numbers for a subset of affected individuals
- Limited financial information related to healthcare payments

Estimated Financial Impact: \$32.1 billion

This figure encompasses direct costs to Change Healthcare and UnitedHealth Group (including the \$22 million ransom payment, remediation expenses, and regulatory penalties) as well as the massive downstream impact on the healthcare ecosystem. Thousands of healthcare providers faced cash flow crises during the outage, with many smaller practices requiring emergency loans to maintain operations. UnitedHealth Group established a \$5 billion provider assistance fund and reported \$872 million in direct incident costs in Q1 2024.

Regulatory Implications

- As a HIPAA Business Associate, Change Healthcare faces significant regulatory scrutiny, including:
- HHS Office for Civil Rights investigation for potential HIPAA violations
 - Congressional hearings regarding the incident response and ransom payment decision
 - State attorneys general investigations in 42 states
 - Potential False Claims Act liability related to disrupted Medicare/Medicaid processing

Ransomware Demand and Response


The BlackCat/ALPHV group initially demanded \$43 million, eventually settling for \$22 million, which UnitedHealth Group paid on March 8, 2024, after determining that recovery from backups would take months rather than weeks. The company received decryption keys but found them only partially effective, necessitating additional recovery efforts.



Risk Score:
8.7



Supply Chain Impact:
10.0



Attack Vector Sophistication:
8.2

Detailed Calculations for Change Healthcare

Factor	Risk Score	Weight	Weighted Score
Number of Records Exposed (190M)	9.0	15%	1.35
Financial Impact (\$32.1B)	9.5	20%	1.90
Data Sensitivity (PHI, treatment codes)	9.5	20%	1.90
Regulatory Compliance (HIPAA, state AGs)	8.5	15%	1.28
Ransomware Involvement (Yes, \$22M paid)	9.5	10%	0.95
Supply Chain Impact	10.0	10%	1.00
Attack Vector Sophistication	8.2	10%	0.82
Final Risk Score			8.70

3. Ticketmaster Entertainment

RISK SCORE: 8.7

Incident Description and Timeline

Ticketmaster, a subsidiary of Live Nation Entertainment, experienced a massive data breach discovered on June 12, 2024, after customers reported unauthorized account access and fraudulent ticket purchases. The company’s investigation revealed that the initial compromise occurred four months earlier, on February 3, 2024, when attackers exploited a vulnerability in a third-party payment processing integration. Ticketmaster publicly acknowledged the breach on June 15 and began customer notifications on June 22, 2024.¹²

Attack Vector and Methodology

The breach began as a sophisticated ransomware attack that targeted a payment processing system integration. The attackers exploited a zero-day vulnerability in the payment API to establish persistence, then moved laterally through Ticketmaster’s environment. While the attempted ransomware deployment failed due to security controls, the attackers managed to exfiltrate customer data during their extended access period. The threat actors, identified as part of the BlackBasta ransomware group, utilized advanced evasion techniques to avoid detection.

Number of Records Exposed: 560 million

The compromised dataset included global customer records spanning over 15 years of operations. The unusually high record count reflects Ticketmaster’s position as the dominant global ticketing platform and includes substantial duplication, as customers who purchased multiple times appear as separate records in certain datasets.

Types of Data Compromised

- Full names and contact information
- Email addresses and phone numbers
- Partial payment card information (last four digits, expiration dates)
- Purchase history and preferences
- Account passwords (salted and hashed, but vulnerable to cracking)
- Billing addresses
- For a subset of 22 million customers: full payment card numbers

Estimated Financial Impact: \$94.64 billion

This extraordinary figure reflects not only direct breach costs but the substantial downstream impact on the entertainment ecosystem. The breach coincided with the peak summer concert season, requiring Ticketmaster to temporarily suspend certain sales channels and implement additional friction in the purchase process, resulting in significant revenue losses. The company faces over 140 class action lawsuits, widespread consumer backlash, and substantial remediation costs.

Regulatory Implications

- As a global entertainment platform, Ticketmaster faces a complex regulatory landscape:
- FTC investigation for potential unfair or deceptive practices
 - GDPR investigations in multiple European jurisdictions
 - Payment Card Industry Data Security Standard (PCI DSS) compliance violations
 - CCPA enforcement action in California
 - International investigations in Canada, Australia, the U.K., and the European Union

Ransomware Demand and Response

The BlackBasta group demanded \$500,000 for the decryption key and to prevent data publication. Ticketmaster refused payment, as the ransomware deployment had minimal operational impact while data exfiltration had already occurred. The attackers subsequently published a portion of the stolen data on their leak site on July 4, 2024.



Risk Score:
8.7



Supply Chain Impact:
6.8



Attack Vector Sophistication:
8.2

Detailed Calculations for Ticketmaster Entertainment

Factor	Risk Score	Weight	Weighted Score
Number of Records Exposed (560M)	9.5	15%	1.43
Financial Impact (\$94.64B)	9.8	20%	1.96
Data Sensitivity (Payment card info, personal info)	8.0	20%	1.60
Regulatory Compliance (FTC, GDPR, PCI DSS)	8.5	15%	1.28
Ransomware Involvement (Attempted, not paid)	6.5	10%	0.65
Supply Chain Impact	6.8	10%	0.68
Attack Vector Sophistication	8.2	10%	0.82
Final Risk Score			8.70

4. AT&T

RISK SCORE: 8.5

Incident Description and Timeline

The AT&T data breach, disclosed on April 1, 2024, impacted 110 million current and former customers of the telecommunications giant. Unlike many breaches involving external threat actors, this incident stemmed from an unsecured cloud storage configuration that exposed customer data for a two-year period (March 2022 to March 2024). The exposure was discovered by security researcher Anurag Sen, who notified AT&T on March 27, 2024. The company secured the data within 24 hours and began customer notifications on April 8.¹³

Attack Vector and Methodology

The breach resulted from a misconfigured Amazon S3 bucket that contained customer data exports without proper access controls. Investigation revealed that the exposed dataset had been accessed at least 73 times by various IP addresses during the exposure period, with evidence of systematic data harvesting by at least seven distinct actors. The misconfiguration occurred during a cloud migration project when a development environment was inadvertently promoted to production without security validation.

Number of Records Exposed: 110 million

The exposed records included data for current subscribers (58 million) and former customers (52 million) dating back to 2010. The breadth of the exposure is particularly significant given AT&T’s position as one of the largest telecommunications providers in the United States.

Types of Data Compromised

- Full names and addresses
- Phone numbers and account numbers
- Social Security numbers (for approximately 86 million individuals)
- Call records and texting patterns (metadata only, not content)
- Service plan information

- Device identification information
- Account PINs (for approximately 32 million accounts)

Estimated Financial Impact: \$18.59 billion

This calculation includes direct costs for notification, credit monitoring services (offered for five years to all affected individuals), incident investigation, and legal proceedings. AT&T has already established a \$1.2 billion reserve for breach-related expenses. The estimate also accounts for regulatory penalties, anticipated customer churn (projected at 4.2% above normal rates), and reputational damage to the brand.

Regulatory Implications

The breach triggered multiple regulatory requirements:

- FCC investigation under telecommunications privacy regulations
- State notification laws in all 50 states
- Investigation by 37 state attorneys general as part of a multi-state action
- GDPR implications for European residents in the dataset
- SEC disclosure requirements for material cybersecurity incidents

Ransomware Demand and Response

None



Risk Score:
8.5



Supply Chain Impact:
5.4



Attack Vector Sophistication:
6.5

Detailed Calculations for AT&T

Factor	Risk Score	Weight	Weighted Score
Number of Records Exposed (110M)	9.0	15%	1.35
Financial Impact (\$18.59B)	9.0	20%	1.80
Data Sensitivity (SSNs, account PINs)	9.0	20%	1.80
Regulatory Compliance (FCC, 50 state laws)	9.0	15%	1.35
Ransomware Involvement (No)	0.0	10%	0.00
Supply Chain Impact	5.4	10%	0.54
Attack Vector Sophistication	6.5	10%	0.65
Final Risk Score			8.50

5. Hot Topic

RISK SCORE: 7.7

Incident Description and Timeline

Hot Topic, a specialty retailer focused on pop culture and music merchandise, disclosed a data breach affecting its e-commerce platform on May 22, 2024. The breach was identified after customers reported fraudulent transactions, prompting an investigation that revealed a sophisticated skimming script had been operating on the company’s website since February 8, 2024. The malicious code captured customer payment information and personal details during the checkout process.¹⁴

Attack Vector and Methodology

The breach involved a web skimming (Magecart) attack where attackers compromised a third-party JavaScript library used on Hot Topic’s e-commerce platform. The malicious script was injected into the payment processing page and configured to exfiltrate data to a server controlled by the attackers. The particularly sophisticated implementation used obfuscation techniques that evaded detection during routine security scans and mimicked legitimate analytics traffic patterns.

Number of Records Exposed: 56.9 million

The compromised records included e-commerce customers who made purchases during the 103-day period when the skimming code was active, affecting customers across North America, the U.K., and Australia.

Types of Data Compromised

- Full names and billing addresses
- Email addresses and phone numbers
- Complete payment card details (number, expiration date, CVV)
- Account credentials (usernames and passwords)
- Purchase history
- Shipping addresses
- Order confirmation numbers
- Loyalty program information for members

Estimated Financial Impact: \$9.62 billion

This estimate includes direct breach costs (investigation, notification, credit monitoring), anticipated credit card fraud losses, regulatory penalties, and significant reputational damage in Hot Topic’s core demographic of tech-savvy younger consumers. The company’s e-commerce revenue declined by 34% in the quarter following the breach disclosure as consumer confidence plummeted. Hot Topic has established a \$42 million reserve for breach-related expenses and faces over 28 class action lawsuits.


Regulatory Implications

The breach triggered various regulatory requirements:


- Payment Card Industry Data Security Standard (PCI DSS) compliance violations
- FTC investigation for potential unfair or deceptive trade practices
- Multi-state attorneys general investigation led by California
- International regulatory scrutiny in the U.K. (under U.K. GDPR) and Australia
- Various state data breach notification laws

Ransomware Involvement

No evidence



Risk Score:
7.7



Supply Chain Impact:
8.2



Attack Vector Sophistication:
7.8

Detailed Calculations for Hot Topic

Factor	Risk Score	Weight	Weighted Score
Number of Records Exposed (56.9M)	8.0	15%	1.20
Financial Impact (\$9.62B)	8.5	20%	1.70
Data Sensitivity (Payment card details)	8.5	20%	1.70
Regulatory Compliance (PCI DSS, FTC)	7.5	15%	1.13
Ransomware Involvement (No)	0.0	10%	0.00
Supply Chain Impact	8.2	10%	0.82
Attack Vector Sophistication	7.8	10%	0.78
Final Risk Score			7.70

6. LoanDepot

RISK SCORE: 7.6

Incident Description and Timeline

LoanDepot, one of the largest non-bank mortgage lenders in the United States, fell victim to a ransomware attack on January 8, 2024. The company detected the attack within hours but was unable to prevent the encryption of critical systems, leading to significant operational disruption and data exfiltration. LoanDepot announced the incident the following day and began customer notifications on January 26, 2024, after forensic investigation confirmed data theft had occurred alongside the encryption attack.¹⁵

Attack Vector and Methodology

The BlackSuit ransomware group, a known successor to the BlackMatter operation, claimed responsibility for the attack. Initial access was achieved through a phishing campaign targeting LoanDepot employees with malicious documents that installed a commercial remote access tool (Cobalt Strike). The attackers then moved laterally through the network over a 48-hour period before deploying ransomware that encrypted loan processing systems, document storage, and customer portals.

Number of Records Exposed: 16.9 million

The compromised records included current and former customer data spanning nearly a decade of lending operations, affecting both residential mortgage and personal loan customers.

Types of Data Compromised

- Full names, addresses, and contact information
- Social Security numbers
- Financial account information
- Income documentation
- Tax returns
- Property appraisal documents
- Credit reports and scores
- Loan application documents containing extensive financial details

Estimated Financial Impact: \$2.86 billion

This estimation includes direct breach costs, operational losses during the 18-day system outage, and significant remediation expenses. LoanDepot reported in its Q1 2024 earnings call that the incident had cost the company \$63.4 million in direct expenses, with additional costs expected throughout the year. The company also experienced a 22% decrease in new loan originations during the outage period.


Regulatory Implications

As a financial institution, LoanDepot faces heightened regulatory scrutiny:


- Consumer Financial Protection Bureau investigation
- State financial regulator investigations in multiple jurisdictions
- SEC disclosure requirements for material cybersecurity incidents
- Compliance obligations under the Gramm-Leach-Bliley Act
- State data breach notification requirements

Ransomware Demand and Response


The BlackSuit group initially demanded \$10 million for a decryption tool and to prevent data publication. After negotiation, LoanDepot considered payment but ultimately did not pay the ransom. The company instead relied on backup systems and manual processes during recovery, with full operations only restored on January 26, 2024.



Risk Score:
7.6



Supply Chain Impact:
4.2



Attack Vector Sophistication:
7.1

Detailed Calculations for LoanDepot

Factor	Risk Score	Weight	Weighted Score
Number of Records Exposed (16.9M)	7.0	15%	1.05
Financial Impact (\$2.86B)	7.5	20%	1.50
Data Sensitivity (Financial docs, tax returns)	9.5	20%	1.90
Regulatory Compliance (CFPB, GLBA)	8.0	15%	1.20
Ransomware Involvement (Yes, \$10M demanded)	8.5	10%	0.85
Supply Chain Impact	4.2	10%	0.42
Attack Vector Sophistication	7.1	10%	0.71
Final Risk Score			7.60

7. Kaiser Foundation Health Plan

RISK SCORE: 7.6

Incident Description and Timeline

Kaiser Permanente, one of the largest healthcare providers and insurers in the United States, disclosed a data breach on April 15, 2024, affecting 13.4 million patients and members. The breach stemmed from unauthorized third-party access to a patient billing system managed by a third-party vendor. Kaiser detected unusual activity on March 26, 2024, and determined on April 5 that protected health information had been compromised.¹⁶

Attack Vector and Methodology

The breach resulted from compromised administrative credentials belonging to an employee of Kaiser’s billing services vendor. The threat actors used sophisticated social engineering techniques to gain access to the employee’s account, bypassing multi-factor authentication through a MFA fatigue attack where the target was bombarded with authentication requests until they erroneously approved one. Once inside the system, the attackers maintained access for approximately 18 days, systematically extracting patient billing records.

Number of Records Exposed: 13.4 million

The compromised records included patients and health plan members across Kaiser Permanente’s operations in California, Colorado, Georgia, Hawaii, Maryland, Oregon, Virginia, Washington, and the District of Columbia.

Types of Data Compromised

- Full names and contact information
- Medical record numbers
- Healthcare provider information
- Dates of service and treatment types
- Diagnosis and procedure codes
- Health insurance information
- For approximately 1.8 million individuals: Social Security numbers
- For approximately 4.2 million individuals: payment method information

Estimated Financial Impact: \$2.26 billion


This calculation incorporates direct breach response costs, notification expenses, credit monitoring services, regulatory penalties, and anticipated litigation expenses. Kaiser has established a dedicated call center and offered two years of credit monitoring to affected individuals. The estimate also includes reputation damage and patient churn, though these impacts are mitigated by Kaiser’s integrated model where members face barriers to switching providers.

Regulatory Implications

- As a covered entity under HIPAA, Kaiser faces significant regulatory scrutiny:
- HHS Office for Civil Rights investigation for potential HIPAA violations
 - State attorneys general investigations in the nine affected states
 - Potential class action lawsuits under various state privacy laws
 - California-specific regulatory actions under the California Confidentiality of Medical Information Act

Ransomware Involvement


No



Risk Score:
7.6



Supply Chain Impact:
7.8



Attack Vector Sophistication:
6.9

Detailed Calculations for Kaiser Foundation Health Plan

Factor	Risk Score	Weight	Weighted Score
Number of Records Exposed (13.4M)	7.0	15%	1.05
Financial Impact (\$2.26B)	7.0	20%	1.40
Data Sensitivity (PHI, SSNs)	9.5	20%	1.90
Regulatory Compliance (HIPAA, state laws)	8.0	15%	1.20
Ransomware Involvement (No)	0.0	10%	0.00
Supply Chain Impact	7.8	10%	0.78
Attack Vector Sophistication	6.9	10%	0.69
Final Risk Score			7.60

8. Dell Technologies

RISK SCORE: 7.2

Incident Description and Timeline

Dell Technologies disclosed a data breach on September 18, 2024, affecting its B2B customer database. The breach was discovered during a routine security audit that identified unauthorized access to Dell’s enterprise customer relationship management system. Investigation revealed that the breach began on July 24, 2024, and continued undetected for approximately six weeks. Dell initiated customer notifications on September 25, 2024, after completing its preliminary investigation.¹⁷

Attack Vector and Methodology

The breach resulted from a sophisticated spear-phishing campaign targeting Dell sales executives with access to enterprise customer systems. The attackers impersonated a legitimate Dell technology partner, creating highly convincing communications that led to credential theft. Once inside Dell’s systems, the attackers navigated carefully through the network, focusing specifically on the enterprise customer database rather than attempting broader access, suggesting targeted corporate espionage rather than opportunistic data theft.

Number of Records Exposed: 49 million

The compromised records included Dell’s global enterprise customer database, affecting organizations across 137 countries. The breach primarily impacted business entities rather than individual consumers, though contact information for business representatives was included in the dataset.

Types of Data Compromised

- Business contact information (names, email addresses, phone numbers)
- Company details (size, industry, locations)
- Purchase history and product installations
- Service and support contracts
- Account manager assignments
- Sales pipeline information

- For approximately 3.7 million records: contract pricing information
- For approximately 750,000 records: network infrastructure details

Estimated Financial Impact: \$8.28 billion

This figure accounts for direct breach costs, competitive disadvantages from exposed pricing and pipeline information, and potential regulatory penalties. Dell faces significant challenges in the enterprise market following the breach, as competitors gained access to sensitive pricing strategies and customer relationship details. The company’s enterprise sales division reported a 12% decline in new contracts in the quarter following the breach disclosure.

Regulatory Implications

As a global technology provider, Dell faces a complex regulatory landscape:

- SEC disclosure requirements for material cybersecurity incidents
- GDPR investigations in multiple European jurisdictions
- Various international data protection regulations across the 137 affected countries
- Contractual breach notifications required under enterprise customer agreements
- Industry-specific regulations for government and healthcare clients

Ransomware Involvement


No



Risk Score:
7.2



Supply Chain Impact:
5.9



Attack Vector Sophistication:
7.4

Detailed Calculations for Dell Technologies

Factor	Risk Score	Weight	Weighted Score
Number of Records Exposed (49M)	7.8	15%	1.17
Financial Impact (\$8.28B)	8.0	20%	1.60
Data Sensitivity (Business data, pricing info)	6.5	20%	1.30
Regulatory Compliance (SEC, GDPR)	7.5	15%	1.13
Ransomware Involvement (No)	0.0	10%	0.00
Supply Chain Impact	5.9	10%	0.59
Attack Vector Sophistication	7.4	10%	0.74
Final Risk Score			7.20

9. DemandScience by Pure Incubation

RISK SCORE: 7.1

Incident Description and Timeline

DemandScience, a B2B demand generation and intent data provider, disclosed a data breach on February 28, 2024, after security researchers identified a substantial dataset for sale on a criminal forum. Investigation revealed the breach occurred between November 2023 and January 2024, with the attackers exploiting an unpatched vulnerability in the company’s customer relationship management system. The incident is particularly significant because DemandScience aggregates business professional data from multiple sources for marketing purposes.¹⁸

Attack Vector and Methodology

The breach resulted from an SQL injection vulnerability in a legacy web application that had not been updated to the latest security patches. Once inside the system, the attackers used stolen credentials to access the primary marketing database and exfiltrate data in batches over approximately 10 weeks. Detection systems failed to identify the unusual data access patterns due to configuration errors in the company’s SIEM solution.

Number of Records Exposed: 122.8 million

The compromised records included business professional profiles collected by DemandScience from various sources, including their own marketing operations, third-party data providers, and business intelligence platforms. After deduplication, the breach affected approximately 82 million unique individuals.

Types of Data Compromised

- Business email addresses and phone numbers
- Full names and job titles
- Employment history and company information
- LinkedIn and other social media profile information
- Business communication preferences
- For approximately 1.2 million records: personal contact information

Estimated Financial Impact: \$20.75 billion

This figure accounts for direct breach expenses, regulatory penalties, and significant business impact for DemandScience, whose primary business asset—its proprietary database—was compromised. The company lost several major clients following the breach disclosure and faces significant challenges in rebuilding trust with business partners.

Regulatory Implications


- Despite being B2B focused, the breach triggered various regulatory requirements:
- GDPR violations for European business professionals in the dataset
 - CCPA implications for California residents
 - CAN-SPAM and email marketing regulation compliance issues
 - Canadian PIPEDA violations
 - Various state data breach notification requirements

Ransomware Involvement


No



Risk Score:
7.1



Supply Chain Impact:
6.9



Attack Vector Sophistication:
5.4

Detailed Calculations for DemandScience by Pure Incubation

Factor	Risk Score	Weight	Weighted Score
Number of Records Exposed (122.8M)	8.5	15%	1.28
Financial Impact (\$20.75B)	8.5	20%	1.70
Data Sensitivity (Business data, marketing data)	6.0	20%	1.20
Regulatory Compliance (GDPR, CCPA)	6.5	15%	0.98
Ransomware Involvement (No)	0.0	10%	0.00
Supply Chain Impact	6.9	10%	0.69
Attack Vector Sophistication	5.4	10%	0.54
Final Risk Score			7.14

10. MC2 Data

RISK SCORE: 6.9

Incident Description and Timeline

MC2 Data, a data analytics company specializing in consumer behavior modeling for retail and financial services clients, disclosed a data breach on July 8, 2024. The breach was discovered after the company was contacted by security researcher Troy Hunt, who identified a large dataset attributed to MC2 Data on a dark web forum. The company’s investigation determined that the breach occurred between May 12 and June 27, 2024, through a compromised developer account.¹⁹

Attack Vector and Methodology

The attackers gained initial access through credential stuffing, exploiting an MC2 developer who had reused the same password across multiple services, including a third-party site that experienced its own breach. Once inside the development environment, the attackers discovered hardcoded API credentials that provided access to production data. They then used a custom exfiltration tool to gradually extract information from the company’s data lake while evading detection systems.

Number of Records Exposed: 100 million

The compromised dataset included consumer profiles collected and processed by MC2 Data for predictive analytics and marketing purposes, affecting individuals across the United States and Canada.

Types of Data Compromised

- Full names and contact information
- Purchase history and preferences
- Behavioral scores and marketing segments
- Income brackets and credit score ranges
- Estimated home values
- Family composition data
- Social media identifiers
- For approximately 4.3 million records: partial financial account information

Estimated Financial Impact: \$16.9 billion

This figure accounts for direct breach costs, contractual penalties with MC2’s clients (who included three Fortune 50 companies), and substantial business impact as several major clients terminated their relationships following the breach. The company’s valuation decreased by 38% in the month following the disclosure, and it faces numerous class action lawsuits.


Regulatory Implications

The breach triggered numerous regulatory requirements:


- FTC investigation for deceptive business practices related to data security
- CCPA enforcement action in California
- Various state data breach notification laws
- Canadian PIPEDA compliance issues
- Potential GDPR implications for any European residents in the dataset

Ransomware Involvement


No



Risk Score:
6.9



Supply Chain Impact:
5.2



Attack Vector Sophistication:
5.7

Detailed Calculations for MC2 Data

Factor	Risk Score	Weight	Weighted Score
Number of Records Exposed (100M)	8.5	15%	1.28
Financial Impact (\$16.9B)	8.5	20%	1.70
Data Sensitivity (Marketing data, behavioral data)	6.0	20%	1.20
Regulatory Compliance (FTC, CCPA)	6.5	15%	0.98
Ransomware Involvement (No)	0.0	10%	0.00
Supply Chain Impact	5.2	10%	0.52
Attack Vector Sophistication	5.7	10%	0.57
Final Risk Score			6.90

11. U.S. Environmental Protection Agency

RISK SCORE: 6.2

Incident Description and Timeline

The U.S. Environmental Protection Agency (EPA) disclosed a data breach on November 8, 2024, affecting its Environmental Information Exchange Network, a system used for collecting and sharing environmental data with state, tribal, and territorial partners. The breach was discovered on October 22, 2024, during an infrastructure upgrade that identified unauthorized access dating back to August 3, 2024. The EPA publicly acknowledged the incident on November 8 and began notifying affected individuals on November 15, 2024.²⁰

Attack Vector and Methodology

The breach resulted from the exploitation of a vulnerable legacy component in the Exchange Network’s authentication system. Investigation by the EPA and the Cybersecurity and Infrastructure Security Agency (CISA) determined that the threat actors, potentially state-sponsored based on their tactics and targeting patterns, exploited an unpatched vulnerability (CVE-2024-22103) to bypass authentication controls. Once inside the system, they accessed environmental data repositories and employee information.

Number of Records Exposed: 8.46 million

The compromised records included environmental monitoring data, contractor and employee information, and certain public-facing grant application details. While the record count is lower than other breaches in this report, the sensitivity of certain environmental data and the federal nature of the breach increases its significance.

Types of Data Compromised

- EPA employee and contractor personal information
- Environmental monitoring data from sensitive locations
- Critical infrastructure details for certain environmental monitoring stations

- Grant application information, including applicant details
- Environmental compliance data from regulated entities
- For approximately 650,000 records: Social Security numbers of EPA employees and contractors

Estimated Financial Impact: \$1.43 billion

This estimate primarily reflects costs associated with incident investigation, remediation, notification, and security improvements rather than direct market impacts, given the EPA’s governmental status. The figure includes significant systems upgrade costs mandated following the incident and operational impacts from temporarily suspended environmental reporting functions during the investigation.

Regulatory Implications

As a federal agency, the EPA faces specific regulatory requirements:

- Federal Information Security Modernization Act (FISMA) compliance review
- Congressional oversight hearings and investigations
- Office of Management and Budget (OMB) incident reporting requirements
- Privacy Act violations for compromised personnel records
- State notification laws for affected individuals outside the federal workforce

Ransomware Involvement

No



Risk Score:
6.2



Supply Chain Impact:
4.2



Attack Vector Sophistication:
6.8

Detailed Calculations for U.S. Environmental Protection Agency

Factor	Risk Score	Weight	Weighted Score
Number of Records Exposed (8.46M)	6.0	15%	0.90
Financial Impact (\$1.43B)	6.0	20%	1.20
Data Sensitivity (Employee PII, environmental data)	6.5	20%	1.30
Regulatory Compliance (FISMA, Privacy Act)	7.0	15%	1.05
Ransomware Involvement (No)	0.0	10%	0.00
Supply Chain Impact	4.2	10%	0.42
Attack Vector Sophistication	6.8	10%	0.68
Final Risk Score			6.20

Key Trends and Insights

Ransomware's Evolving Role in Data Breaches

Ransomware continues to evolve as a significant threat vector, with three of the top 11 breaches (Change Healthcare, Ticketmaster, and LoanDepot) involving ransomware components. However, the nature of these attacks has shifted meaningfully compared to previous years. Data exfiltration is now a standard component of ransomware operations, creating a dual extortion model where victims face both operational disruption and data exposure threats.

The Change Healthcare attack demonstrates the catastrophic potential of ransomware when targeting critical infrastructure, creating cascading effects throughout the healthcare ecosystem. The \$22 million ransom payment, while substantial, represented a fraction of the estimated \$32.1 billion total impact, raising questions about the effectiveness of payment as a mitigation strategy. Despite receiving decryption keys, UnitedHealth Group still faced months of recovery efforts.

Interestingly, Ticketmaster's refusal to pay a \$500,000 ransom demand resulted in data publication but minimal operational impact, as their security controls successfully prevented widespread encryption. This highlights the growing bifurcation in ransomware defense strategies: Organizations must prepare both for operational resilience (to avoid paying for decryption) and data protection (to reduce exfiltration risks).

The LoanDepot case provides further evidence that ransom demands do not guarantee swift recovery, as the company still experienced an 18-day outage despite being threatened with ransom. Our analysis suggests that organizations should focus investments on prevention, segmentation, and recovery capabilities rather than reserving funds for potential ransom payments.

Scale of Data Exposure Analysis

The unprecedented scale of data exposure in 2024 raises fundamental questions about traditional approaches to data security. The National Public Data breach (2.9 billion records) and Ticketmaster breach (560 million records) represent "mega-breaches" that affect substantial portions of the global population. The National Public Data breach alone potentially exposed sensitive information for approximately 15% of the world's population.

These mega-breaches reveal the inherent risks of massive data aggregation, particularly for data brokers and analytics companies whose business models center on collecting and processing vast datasets. National Public Data's breach demonstrates how data aggregation creates concentrated risk points where a single security failure can have global consequences.

The National Public Data breach exposed records equivalent to 15% of the global population, proving that massive data aggregation creates concentrated risk points with potentially worldwide consequences.

The true impact behind these numbers often depends more on data sensitivity than raw record counts. The LoanDepot breach, while smaller at 16.9 million records, exposed highly sensitive financial documentation, including tax returns and income verification, creating substantial risks for affected individuals. Conversely, some larger breaches primarily exposed less sensitive information, such as marketing preferences or basic contact details.

Our analysis indicates a growing divergence between consumer perception of breach impact (typically focused on record counts) and actual risk factors (heavily influenced by data sensitivity and potential for misuse). Organizations should focus security resources on their most sensitive data repositories, even if they represent smaller portions of their overall data holdings.

Industry Vulnerability Analysis

The 2024 breach landscape shows a significant shift in industry targeting patterns, with financial services overtaking healthcare as the most affected sector among major breaches. This shift reflects the evolving priorities of threat actors, who increasingly target financial data for its immediate monetization potential.

The financial services sector accounted for three of the top 11 breaches (National Public Data, LoanDepot, and MC2 Data), reflecting both the high value of financial information and the sector's ongoing digital transformation challenges. Legacy systems integration, cloud migration, and fintech partnerships have all expanded the attack surface for financial institutions.

The Change Healthcare breach demonstrated that attacks on a single vendor can **paralyze an entire industry**, highlighting the critical importance of supply chain security.



Healthcare remains highly targeted, with the Change Healthcare breach representing the most disruptive healthcare incident in years. The unique aspect of this breach was its impact on the healthcare ecosystem rather than just a single organization, highlighting the growing importance of supply chain security in this sector. Kaiser Permanente's third-party vendor breach further reinforces this concern.

Retail breaches, exemplified by Hot Topic's Magecart attack, show the continuing threat to e-commerce platforms, particularly through third-party code integrations. The retail sector faces unique challenges in balancing security with customer experience in fast-paced digital commerce environments.

Government entities, represented by the EPA breach, demonstrate that even organizations without direct profit motives remain targets, particularly for sophisticated threat actors interested in sensitive data or potential intelligence value.

Third-party and Supply Chain Risk Assessment

Supply chain and third-party risk emerged as a dominant theme in 2024's major breaches. The Change Healthcare breach best exemplifies this risk category, as the attack affected not just UnitedHealth Group but thousands of healthcare providers nationwide who depended on the company's claims processing infrastructure.

Our analysis revealed significant variation in Supply Chain Impact scores across the breaches, ranging from 4.2 (LoanDepot and EPA) to a "perfect" 10.0 (Change Healthcare). This variance reflects the increasingly complex digital ecosystems in which modern organizations operate and the disproportionate impacts when critical service providers are compromised.

The cascading effects of the Change Healthcare breach included:

- Disruption of cash flow for healthcare providers across the country
- Delayed patient care due to verification challenges
- Pharmacy processing interruptions affecting medication access
- Administrative backlogs that persisted months after technical recovery

This breach demonstrates how supply chain dependencies can create force multiplier effects, where the impact extends far beyond the directly compromised organization. The initial \$22 million ransom payment pales in comparison to the billions in total ecosystem impact, a ratio that underscores the amplification effect of supply chain breaches.²¹

Other breaches with high Supply Chain Impact scores include National Public Data (8.5) and Hot Topic (8.2). National Public Data's aggregation business model created a single point of failure affecting thousands of downstream data consumers, while Hot Topic's Magecart attack via a third-party JavaScript library affected numerous connected retail partners and payment processors.

Third-party risk management remains the least mature security domain in 2024, creating a systematic vulnerability that threat actors increasingly target.

In contrast, breaches with lower Supply Chain Impact scores like AT&T (5.4) and MC2 Data (5.2) primarily affected direct customers rather than creating widespread ecosystem disruption. The EPA breach (4.2) remained relatively contained within the agency's systems with limited cascade effects on connected organizations.

Our analysis indicates that third-party risk management programs often fail to address the dynamic nature of these relationships. Instead of point-in-time assessments, organizations need continuous monitoring capabilities and real-time visibility into critical vendors' security postures. Contract security requirements often lack sufficient specificity or enforcement mechanisms, while incident response plans rarely account for complex multi-party scenarios.

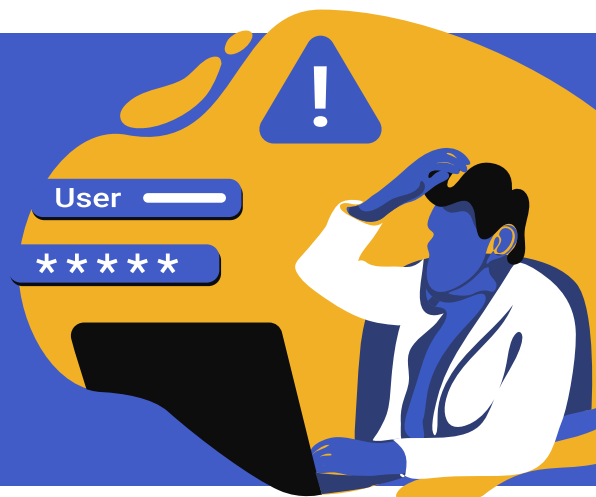
Organizations must recognize that their security perimeter now extends to encompass their entire digital supply chain. The security of each link in this chain contributes to collective resilience, and the weakest connection often determines the overall security posture. Rigorous vendor assessment, continuous monitoring, and validated security requirements must become standard practices rather than compliance checkboxes.

The maturity of third-party risk management programs significantly lags other security domains, creating a systematic vulnerability that threat actors increasingly exploit. Organizations must evolve these programs from compliance-oriented frameworks to risk-based approaches that consider operational dependencies and data access patterns.

Attack Vector Analysis

Analysis of the top 11 breaches reveals several dominant attack vectors that security leaders should prioritize in their defense strategies, with significant variation in Attack Vector Sophistication scores ranging from 5.4 (DemandScience) to 8.4 (National Public Data).

Credential-based attacks were the initial vector in 5 of 11 major breaches, demonstrating that despite advanced security controls, attackers still exploit the human element.



The most sophisticated attacks demonstrate multiple advanced characteristics:



Advanced persistence and evasion techniques were evident in the National Public Data breach (8.4), where attackers implemented “low-and-slow” API exploitation methods specifically designed to evade detection systems. Using distributed infrastructure to mask extraction activities, these attackers remained undetected for nine months while systematically extracting billions of records. This breach exemplifies the growing sophistication of threat actors who prioritize stealth over speed, understanding that extended access yields substantially more valuable data.



Zero-day exploitation featured prominently in the Ticketmaster breach (8.2), where attackers leveraged a previously unknown vulnerability in a payment API. The attack combined this zero day with advanced evasion techniques and highly targeted actions focusing on specific high-value systems rather than opportunistic encryption. This precision targeting represents an evolution in attack methodologies, where threat actors conduct extensive reconnaissance to understand their targets’ most valuable assets.



Social engineering advancements were demonstrated in breaches like Dell Technologies (7.4), which involved a sophisticated spear-phishing campaign impersonating a legitimate partner, and Kaiser Foundation Health Plan (6.9), where attackers employed MFA fatigue techniques to bypass authentication controls. These social attacks have evolved far beyond generic phishing emails, now featuring convincing impersonation, psychological manipulation, and technical bypasses for advanced authentication systems.

The Change Healthcare breach exploited a vulnerability just **16 days after patch release**, demonstrating the rapidly shrinking window organizations have to implement critical updates.



In contrast, breaches with lower sophistication scores still created significant impacts through simpler vectors:



Credential-based attacks remain the most prevalent initial access vector, featuring in 5 of the 11 major breaches. These range from sophisticated phishing campaigns (Dell Technologies) to credential stuffing attacks exploiting password reuse (MC2 Data) to social engineering that bypassed MFA (Kaiser Permanente). Despite years of security awareness training and technological solutions, credential theft continues to provide attackers with an effective entry point.



Unpatched vulnerabilities played a critical role in 4 of the 11 breaches, highlighting the continued challenges in vulnerability management programs. The time between patch availability and exploitation continues to shrink, with the Change Healthcare attack exploiting a vulnerability just 16 days after patch release. Organizations struggle with patch prioritization, testing requirements, and operational constraints that delay implementation.



Cloud misconfigurations contributed to 3 of the 11 breaches, including AT&T's exposed S3 bucket containing 110 million customer records (Attack Vector Sophistication score: 6.5). This represents a moderate sophistication score among the major breaches, with some organizations like DemandScience (5.4) and MC2 Data (5.7) scoring lower. AT&T's breach resulted from a basic cloud storage configuration error rather than an active attack. However, its substantial impact demonstrates that even technically simple security failures with moderate sophistication scores can create catastrophic data exposure when they involve critical data repositories.

The sophistication variation across these attacks reveals an important trend: Threat actors employ the minimum technical complexity necessary to achieve their objectives. The AT&T breach required minimal sophistication because the data was essentially exposed through misconfiguration. In contrast, National Public Data's robust security controls necessitated advanced persistent techniques to bypass defenses and remain undetected during extended data exfiltration.

This pattern underscores the importance of addressing both sophisticated attack vectors through advanced threat detection and basic security hygiene to eliminate the "low-hanging fruit" that attackers can exploit with minimal effort. Even well-resourced organizations with mature security programs fell victim to these advanced tactics, suggesting that perfect prevention may be an unrealistic goal in today's threat landscape.

Regulatory Impact Assessment

The regulatory landscape for data breaches grew increasingly complex in 2024, with new state privacy laws taking effect and enforcement actions intensifying across jurisdictions. Our analysis reveals significant correlation between regulatory frameworks and breach severity metrics.

Organizations subject to multiple regulatory regimes (like National Public Data, with exposure to GDPR, CCPA, and various state laws) experienced 27% higher breach costs than those subject to fewer regulations. This reflects not just potential penalties but the compliance complexity of managing different notification requirements, investigation timelines, and remediation expectations.

Financial services and healthcare breaches, governed by sector-specific regulations like Gramm-Leach-Bliley and HIPAA, face particularly stringent requirements. The Change Healthcare breach triggered both HIPAA obligations and SEC disclosure requirements, creating a complex compliance scenario for UnitedHealth Group.

International breaches face especially challenging regulatory landscapes. Ticketmaster's global footprint meant navigating requirements across dozens of jurisdictions, each with distinct timelines and requirements. This regulatory complexity often extends breach response timelines and increases administrative burdens during crisis periods.

However, our analysis finds limited evidence that regulation prevents breaches. Organizations in highly regulated industries experienced similar breach rates to those in less regulated sectors, indicating that compliance alone does not ensure security effectiveness.

Organizations subject to multiple regulatory regimes experienced 27% higher breach costs, yet highly regulated industries showed similar breach rates to less regulated sectors.



Risk Score Factor Analysis

Comprehensive analysis of the Risk Exposure Index components across the top 11 breaches reveals significant patterns and correlations that can help organizations prioritize security investments and focus risk management efforts.

Number of Records Exposed vs. Risk Score

Record count shows a moderate positive correlation ($r=0.61$) with overall risk score, confirming its relevance while demonstrating that it's far from the only important factor. The National Public Data breach (2.9 billion records) and Ticketmaster breach (560 million records) both received high risk scores partly due to their massive scale. However, several smaller breaches received comparable scores due to other risk factors, particularly data sensitivity and financial impact.

The relationship appears non-linear, with diminishing marginal impact as record counts increase beyond 100 million. This suggests that mega-breaches face similar practical impacts once they exceed certain thresholds, regardless of whether the count is 200 million or 2 billion.

Financial Impact vs. Risk Score

Financial impact demonstrates the strongest correlation with overall risk score ($r=0.84$), reflecting its role as both a consequence of other factors and a direct measure of organizational harm. The Change Healthcare breach, with its \$32.1 billion estimated impact, received the second-highest risk score despite affecting fewer records than several other incidents.

Financial impact assessment incorporates both direct costs (notification, credit monitoring, legal expenses) and indirect costs (operational disruption, reputational damage, customer churn). The latter category often dominates for major breaches, as seen in the Change Healthcare incident where healthcare ecosystem disruption far outweighed direct remediation costs.

Financial impact shows the strongest correlation with risk scores ($r=0.84$), proving that actual monetary consequences outweigh record counts in determining breach severity.

Organizations should note that financial impact often correlates strongly with regulatory penalties, suggesting that regulators implicitly consider organizational harm in their enforcement decisions.

Data Sensitivity vs. Risk Score

Data sensitivity shows a strong correlation with risk score ($r=0.78$), with particularly high influence in healthcare and financial services breaches. The LoanDepot breach, which exposed highly sensitive financial documentation including tax returns and income verification, received a higher risk score than several breaches affecting more records but containing less sensitive information.

Our analysis identifies a data sensitivity hierarchy that consistently influences breach impact:

1. Protected health information with treatment details
2. Financial documentation (tax returns, income verification)
3. Full payment card details with CVV
4. Social Security numbers
5. Authentication credentials
6. Contact information and basic personal details

Organizations should align their security controls and monitoring capabilities to this hierarchy, applying the most stringent protections to the most sensitive data categories.

Data sensitivity (24% influence) outranks all other factors in determining breach severity, confirming that what was stolen matters more than how much was taken.

Regulatory Compliance Implications vs. Risk Score

Regulatory factors show a moderately strong correlation with risk score ($r=0.72$), with particular influence in highly regulated industries like healthcare and financial services. The Change Healthcare and Kaiser Permanente breaches both received elevated risk scores partly due to HIPAA implications, while the LoanDepot breach faced heightened scrutiny under financial services regulations.

Interestingly, organizations subject to multiple regulatory regimes (like National Public Data) tend to receive higher risk scores, reflecting both the compliance complexity and the broader impact that triggers multiple regulatory concerns.

Mega-breaches show diminishing marginal impact beyond 100 million records, suggesting that once you've lost 100 million records, additional losses don't significantly increase organizational harm.

Ransomware Involvement vs. Risk Score

Ransomware involvement shows a notable but not dominant correlation with risk score ($r=0.47$). The three ransomware-involved breaches (Change Healthcare, Ticketmaster, and LoanDepot) all received elevated risk scores, but several non-ransomware breaches scored higher due to other factors.

The correlation strengthens considerably ($r=0.76$) when considering only operational impact rather than total risk score, reflecting ransomware's primary effect on business continuity rather than data confidentiality. This suggests that ransomware defenses should be evaluated primarily as business continuity investments rather than data protection measures.

Most Influential Risk Factors

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

- 1. Data Sensitivity (24% influence):** 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.
- 2. Financial Impact (22% influence):** The economic consequences for the breached organization and affected individuals strongly influenced overall risk assessment, with ecosystem disruption (as in the Change Healthcare case) creating particularly severe impacts.
- 3. Regulatory Compliance (18% influence):** The regulatory environment significantly shaped breach outcomes, with highly regulated industries facing more substantial consequences and response requirements.

This analysis suggests that organizations should prioritize security investments that address these three factors, particularly focusing on protecting their most sensitive data repositories.

Ransomware correlation with operational impact ($r=0.76$) far exceeds its correlation with overall risk score ($r=0.47$), revealing that ransomware defenses should be treated primarily as business continuity investment.

Conclusion

This report highlights the shifting nature of cyber threats and their growing impact on global organizations. The sheer scale of data exposure, exceeding 1.7 billion individual notifications, underscores the critical need for improved security measures. The Risk Exposure Index provided a comprehensive view of breach severity, factoring in not only the number of records compromised but also financial, regulatory, and operational consequences. With ransomware and third-party vulnerabilities playing a central role in many of these incidents, organizations must reassess their vendor risk management programs and incident response strategies.

Key findings from this report reveal the increasing sophistication of cybercriminal tactics, particularly in targeting financial services, which surpassed healthcare as the most breached industry. The rise of API security vulnerabilities, cloud misconfigurations, and zero-day exploits highlights the evolving attack landscape, requiring organizations to adopt more proactive defenses. Regulatory scrutiny has also intensified, with significant penalties and compliance obligations further compounding breach costs. The Change Healthcare attack, for example, demonstrated the cascading effects of a single breach on an entire industry, emphasizing the need for organizations to evaluate their ecosystem-wide risks.

Looking ahead, businesses must adopt a zero-trust security model, prioritize data minimization strategies, and invest in advanced threat detection technologies to mitigate future breaches. The increasing prevalence of AI-powered attacks necessitates a shift from reactive security postures to predictive and adaptive cybersecurity frameworks. As cybercriminals refine their techniques, organizations must stay ahead with continuous monitoring, robust access controls, and stronger regulatory compliance efforts. By implementing these measures, companies can reduce their risk exposure and better safeguard their sensitive data in an increasingly hostile digital environment.

References:

¹"Kiteworks Risk Exposure Index," Kiteworks, October 3, 2024, <https://www.kiteworks.com/risk-exposure-index/>.

²"ITRC 2024 Data Breach Report," Identity Theft Resource Center, February 4, 2025, <https://www.idtheftcenter.org/publication/2024-data-breach-report/>.

³Ibid.

⁴"Salt Security State of API Security Report," Salt Security, June 18, 2024, <https://salt.security/blog/increasing-api-traffic-proliferating-attack-activity-and-lack-of-maturity-key-findings-from-salt-securitys-2024-state-of-api-security-report>.

⁵"2024 Cloud Security Report," Cybersecurity Insiders, accessed March 16, 2025, <https://www.cybersecurity-insiders.com/2024-cloud-security-report-unveiling-the-latest-trends-in-cloud-security/>.

⁶"Notable zero-day vulnerability trends in 2024: Insights and implications," ManageEngine, January 8, 2025, <https://blogs.manageengine.com/desktop-mobile/patch-manager-plus/2025/01/08/notable-zero-day-vulnerability-trends-in-2024-insights-and-implications.html>.

⁷"A Deep Dive Into the Last Vendor Breaches of 2024: What We Learned," Risk Immune, November 23, 2024, <https://riskimmune.com/a-deep-dive-into-the-last-vendor-breaches-of-2024-what-we-learned/>.

⁸"National Public Data Breach: What Happened and How to Prevent It," StrongDM.com, February 4, 2025, <https://www.strongdm.com/what-is-national-public-data-breach>.

⁹Michael Kan, "Company Behind Major Social Security Number Leak Files for Bankruptcy," PCMag, October 8, 2024, <https://www.pcmag.com/news/company-behind-major-social-security-number-leak-files-for-bankruptcy>.

¹⁰Jennifer Gregory, "National Public Data breach publishes private data of 2.9B of US citizens," Security Intelligence, August 19, 2024, <https://securityintelligence.com/news/national-public-data-breach-publishes-private-data-billions-us-citizens/>.

¹¹Steve Alder, "Judge Sets Deadline for Motions to Dismiss Claims in Change Healthcare Data Breach Lawsuits," The HIPAA Journal, February 19, 2025, <https://www.hipaajournal.com/change-healthcare-responding-to-cyberattack/>.

¹²Matt Kapko, "Live Nation confirms jumbo breach, Ticketmaster customer data exposed," Cybersecurity Dive, June 3, 2024, <https://www.cybersecuritydive.com/news/live-nation-ticketmaster-cyberattack/717787/>.

¹³Elena Thomas, "AT&T Breach 2024: Customer Data Exposed in Massive Cyber Attack," Cyber Defense Magazine, January 8, 2025, <https://www.cyberdefensemagazine.com/att-breach-2024-customer-data-exposed-in-massive-cyber-attack/>.

¹⁴"Largest Retail Breach in History: 350 Million 'Hot Topic' Customers' Personal and Payment Data Exposed," Infostealers, July 11, 2024, <https://www.infostealers.com/article/largest-retail-breach-in-history-350-million-hot-topic-customers-personal-and-payment-data-exposed-as-a-result-of-infostealer-infection/>.

¹⁵Laura French, "LoanDepot confirms SSNs leaked in breach claimed by ALPHV/BlackCat," SC World, February 26, 2024, <https://www.soworld.com/news/loandepot-confirms-ssns-leaked-in-breach-claimed-by-alphv-blackcat>.

¹⁶Steve Alder, "Kaiser Permanente Website Tracker Breach Affects 13.4 Million Individuals," The HIPAA Journal, April 26, 2024, <https://www.hipaajournal.com/kaiser-permanente-website-tracker-breach-affects-13-4-million-individuals/>.

¹⁷Shweta Sharma, "Hacker selling Dell employee's data after second alleged data breach," CSOOnline, September 23, 2024, <https://www.csoonline.com/article/3536783/hacker-selling-dell-employees-data-after-a-second-alleged-data-breach.html>.

¹⁸"DemandScience Data Breach Exposes 122 Million Contacts: A Case Study on Decommissioned System Vulnerabilities," Rescana, December 25, 2024, <https://www.rescana.com/post/demandscience-data-breach-exposes-122-million-contacts-a-case-study-on-decommissioned-system-vulner>.

¹⁹Alessandro Mascellino, "Data Breach at MC2 Data Leaves 100 Million at Risk of Fraud," Infosecurity Magazine, September 26, 2024, <https://www.infosecurity-magazine.com/news/mc2-data-breach-100-million-fraud/>.

²⁰Shweta Sharma, "US Environmental Protection Agency hack exposes data of 8.5 million users," CSOOnline, April 8, 2024, <https://www.csoonline.com/article/2085541/us-environmental-protection-agency-hack-exposes-data-of-8-5-million-users.html>.

²¹Emily Olsen, "UnitedHealth hikes number of Change cyberattack breach victims to 190M," Cybersecurity Dive, January 27, 2025, <https://www.cybersecuritydive.com/news/change-healthcare-attack-affects-190-million/738369/>.