MACRO PRAXIS | Research Institute

Top 20 Breach Impact Analysis (as of 2025)

Analyzing $22.6B in Breach Costs to Identify a Strategic Detection Gap

Published by the MacroPraxis Research Institute: April 23, 2025

Author: Bobby Boughton, MacroPraxis Research Institute Fellow

---

Executive Summary

Cybersecurity leaders increasingly accept that breaches are inevitable. Yet the financial scale of those breaches remains underestimated due to the tendency to report only fines, settlements, or direct remediation costs. This paper revisits the top 20 cyberattacks from the past decade, assessing their **true financial impact**—including business disruption, customer churn, and regulatory fallout—and quantifies what the cost *could have been* had high-fidelity deception controls been in place. Deception technology, now validated by NSA and recognized by Gartner as a preemptive defense layer, offers a compelling risk-reduction tool that could have materially reduced or even neutralized many of these damages. As part of a modern Zero Trust and assume-breach architecture, deception has the potential to deliver the **highest return on investment of any cybersecurity control**. For CISOs seeking to align risk reduction with business resilience, deception provides a measurable and proactive path forward.

Section 1: Methodology

This report synthesizes breach cost data from a broad range of reputable sources, including SEC filings, earnings call transcripts, regulatory fines, class-action lawsuit settlements, and investigative journalism from outlets such as Reuters and The Wall Street Journal. In cases where full cost disclosures were unavailable, conservative estimates were derived using public statements, industry benchmarks, and comparative breach analogs.

We adopted a consistent definition of 'total cost' that includes direct response and remediation expenses, legal and regulatory liabilities, lost business, reputational harm, and operational disruption. Wherever possible, these values were validated against historical precedents or supported by third-party forensic analyses and insurance industry reporting.

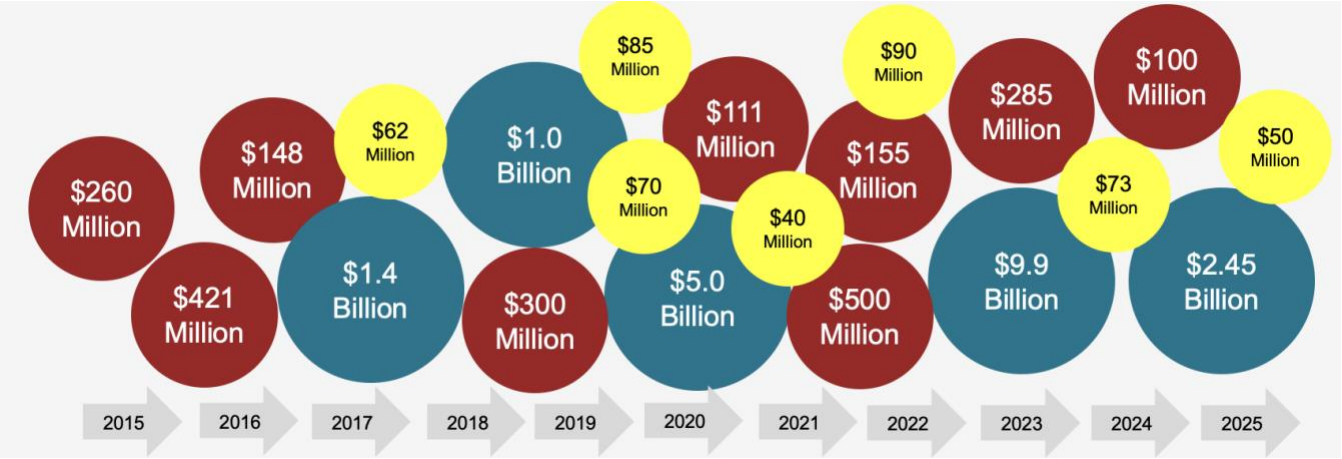
Breach impact figures are represented as minimum confirmed or best-available estimates, and all rankings reflect values known as of April 2025. The table also includes ≥ symbols to indicate conservative lower-bound estimates, recognizing that long-tail legal fees and reputational damage may continue to accrue for years following the initial incident.

We also considered the broader industry context for each breach, evaluating whether costs were borne solely by the breached organization or extended to customers, suppliers, and ecosystem partners. Where applicable—especially in software supply chain attacks and centralized healthcare clearinghouses—we incorporated downstream effects into the total cost estimate. This systems-level approach aims to reflect the true blast radius of each incident, rather than isolating the victim company's internal expenses.

Section 2: The Real Cost of Breach Events

Rank	Organization / Breach (Year)	Estimated Total Cost	Sector
1	MOVEit (Progress Software, 2023)	≥$9.9B	Software Supply Chain
2	SolarWinds Orion (2020)	≥$5.0B	Software Supply Chain
3	UnitedHealth – Change Healthcare (2024)	≥$2.45B	Healthcare
4	Equifax (2017)	≥$1.4B	Financial Services
5	Marriott / Starwood (2018)	≥$1.0B	Hospitality
6	T-Mobile US (2021–2023)	≥$500M	Telecom
7	U.S. Office of Personnel Management (2015)	≥$421M	Government
8	Capital One (2019)	≥$300M	Financial Services
9	First American Financial Corp. (2023)	≥$285M	Financial Services
10	Anthem (2015)	≥$260M	Healthcare
11	MGM Resorts (2023)	≥$155M	Hospitality
12	Uber (2016)	≥$148M	Mobility Tech
13	Colonial Pipeline (2021)	≥$111M	Energy Infrastructure
14	AT&T (2024)	≥$100M	Telecom
15	Optus (AU, 2022)	≥$90M	Telecom
16	JBS (2021)	≥$85M	Food Supply Chain
17	Caesars Entertainment (2023)	≥$73M	Hospitality
18	Kaseya VSA (2021)	≥$70M	Software Supply Chain
19	Latitude Financial (2023)	≥$50M	Financial Services
20	CNA Financial (2021)	≥$40M	Financial Services

Total estimated impact (top 20): $22.6 billion+ (conservative)



Section 2A: MOVEit Breach Case Study

The MOVEit Transfer breach of 2023 stands as one of the most damaging supply chain cyberattacks ever recorded, with estimated global costs of nearly $10 billion.

Key factors that contributed to the scale of damage:

- **Widespread Software Use**: MOVEit was embedded in thousands of enterprises and government agencies to transmit sensitive data like payroll, healthcare, and banking information.
- **Automated Exploitation**: The Cl0p ransomware group exploited a zero-day vulnerability to automate mass data exfiltration from over 2,600 known victim organizations.
- **High-Value Target Data**: Stolen datasets included social security numbers, bank accounts, health data, and other regulated fields triggering mandatory breach disclosures.
- **Ripple Effects Across Critical Infrastructure**: Affected institutions ranged from state governments to healthcare networks to multinational corporations, expanding the impact well beyond the software vendor.
- **Delayed and Staggered Disclosures**: Many victims only learned they were affected months later, prolonging incident response and increasing regulatory exposure.
- **Legal Fallout and Regulatory Probes**: Numerous class-action lawsuits and state attorney general investigations have followed, compounding direct response costs.

This breach illustrates the systemic risk of software supply chain vulnerabilities and the lack of early-warning systems in traditional prevention-first architectures. Had deception controls been embedded around data movement tools and exfiltration paths, many organizations could have contained the attack before sensitive data was accessed.

Section 2B: Change Healthcare Breach Case Study

In early 2024, Change Healthcare, a subsidiary of UnitedHealth Group, suffered one of the most disruptive cyberattacks in U.S. healthcare history, with a total estimated financial impact of **$2.45 billion**.

Key drivers of the breach's severity:

- **Healthcare Industry Interdependence**: Change Healthcare processes billions of healthcare transactions annually and acts as a clearinghouse for insurance claims, prescription management, and patient billing across the U.S.
- **Ransomware on Core Infrastructure**: The attack used ransomware to encrypt critical systems, halting claims processing, pharmacy transactions, and revenue cycles for thousands of hospitals, clinics, and pharmacies.
- **Widespread Economic Disruption**: Provider cash flow stalled across the country, prompting UnitedHealth to issue over **$3.3 billion in temporary advance payments** to affected medical groups.
- **Business Continuity Costs**: Systems had to be rebuilt, third-party claims routed manually, and services outsourced while internal networks were re-secured.

- **Regulatory Scrutiny and Lawsuits**: The attack has triggered federal and state investigations as well as lawsuits alleging negligence in Change Healthcare's cybersecurity posture.

This breach underscores the fragility of centralized infrastructure and the outsized cost of delayed detection. Had deception sensors surrounded high-value applications and data exchange endpoints, lateral movement could have been detected and interrupted before ransomware activation.

Section 2C: Insights from the IBM 2024 Data Breach Report

The 2024 IBM Cost of a Data Breach Report highlights the accelerating financial toll of cyber incidents. The **global average cost** of a data breach reached **$4.88 million**, while in the **United States**, the average soared to **$9.36 million**, the highest recorded in the study's history. These figures emphasize that breach recovery now impacts not only IT budgets but also business continuity, shareholder value, and regulatory standing.

One of the most critical findings was the influence of **detection speed**. Breaches with a dwell time (time to identify and contain) of under 200 days cost, on average, **$1.76 million less** than those that lingered beyond that threshold. Moreover, early detection technologies—such as AI-based detection, automation, and deception—showed the most significant ROI. Organizations leveraging such tools shortened their response cycles by nearly **80 days** compared to those relying on manual processes.

Additionally, IBM found that **supply chain attacks** were among the costliest, averaging **$4.91 million per incident**, due to the complexity of tracing the breach across interconnected partners. The MOVEit and SolarWinds breaches exemplify this trend. IBM's research strongly supports deception as a strategic complement to Zero Trust, allowing organizations to minimize breakout time and shift their posture from reactive forensics to proactive defense.

Section 3: What Could Have Been Prevented

In nearly every case, attackers gained a foothold and moved laterally toward high-value targets—privileged credentials, domain controllers, sensitive PII—often without detection for days, weeks, or months. Had deception technology been deployed at those junctures, the attackers would have tripped high-fidelity alerts long before exfiltration or ransomware detonation.

By embedding decoys at these finite attacker objectives, enterprises could have:

- Triggered early alerts
- Prevented lateral movement
- Contained dwell time
- Reduced breach costs by 90–100%

Section 4: Conclusion

The findings in this report make a compelling case for a shift in cybersecurity strategy—from attempting to perfectly prevent all intrusions to recognizing and preparing for inevitable breaches. Across more than $22.6 billion in analyzed damages, a recurring pattern emerges: organizations lacked early-warning systems that could have detected attacker movement before data was stolen or operations were halted.

Deception technology offers a fundamentally different posture—one that detects intrusions earlier, disrupts attacker objectives, and contains damage before it escalates. From ransomware outbreaks to supply chain compromises, our research shows that deception could have prevented or mitigated nearly every breach on our top 20 list.

As part of a modern Zero Trust and assume-breach architecture, deception has the potential to deliver the **highest return on investment of any cybersecurity control**. For CISOs seeking to align risk reduction with business resilience, deception provides a measurable and proactive path forward.

Sources: Reuters, WSJ, SEC Filings, IBM Cost of a Data Breach Report 2023, MacroPraxis Intelligence Network

The full Research Paper can be found here: https://macropraxis.org/published-research/top-20-breach-impact-analysis-as-of-2025