R E S E A R C H W H I T E P A P E R

Healthcare Breach Survivability

A Statistical Analysis of Organizational Outcomes Following Cyber Incidents in Healthcare

Primary Study Dataset: 1,478 Breach Events Analyzed | January 2023 – February 2026

Excludes: Government Entities, Educational Institutions, Health Plans & Payors

Published March 2026

Cybantage

cybantage.com

by:

***Rod Andes**, CCISO, CCISP, CDORO, CISA …*

Executive Summary

Healthcare cybersecurity breaches have long been analyzed through the lens of patient privacy, regulatory compliance, and the number of records exposed. This research proposes a materially different and more consequential measure: whether the organization itself survives.

This whitepaper presents an analysis of 1,478 healthcare organizations — providers and business associates — that reported major breaches affecting protected health information (PHI) between January 1, 2023 and early 2026. This study dataset represents a carefully defined and intentionally bounded subset of a far larger breach universe, the full dimensions of which demand explicit acknowledgment at the outset.

The True Scale of the Breach Problem

In 2023 alone, the U.S. Department of Health and Human Services Office for Civil Rights (HHS/OCR) received approximately 320,000 complaints involving potential HIPAA violations and privacy breaches. In that same year, healthcare organizations reported approximately 36,000 individual breaches affecting fewer than 500 patient records — events that are required to be logged annually but do not trigger immediate public notification.

Our study dataset of 1,478 organizations represents major breach events — those affecting 500 or more individuals and subject to immediate HHS notification requirements — drawn specifically from healthcare providers and business associates. The following categories were intentionally excluded from this analysis:

- Health plans and payors, including commercial insurers, and pharmacy benefit managers
- Government-operated healthcare entities
- Educational institutions with affiliated healthcare operations
- Cases where the required organizational data was not accessible for analysis

Our 1,478-organization dataset represents the visible, data-accessible tip of a breach iceberg. The full healthcare breach universe in 2023 alone encompassed approximately 320,000 HHS complaints and 36,000 small-record breach events — neither of which is captured in our study population.

This context is critical for accurate interpretation. Our findings on organizational survival rates, breach characteristics, and closure patterns apply specifically to the studied population of

healthcare providers and business associates experiencing major breaches. The actual scope of healthcare cyber harm — including the tens of thousands of small breaches, the privacy complaints that never become formal breach notifications, and the impact on health plans and payors — is substantially larger than any single study dataset can capture.

Key Findings From the Study Dataset

Within the 1,478 organizations studied, the findings are consequential:

- Approximately 31.3% of studied organizations are no longer operating independently following their breach events — approximately 1 in 3 did not survive
- Organizations that closed had on average significantly smaller breaches (~40,000 individuals affected) than those that survived (~194,000), confirming that breach magnitude does not predict survival
- 83.1% of all breach events were Hacking or IT Incidents; 14.5% were Unauthorized Access events — together accounting for 97.6% of all incidents in the dataset
- Network servers (65.5%) and email systems (22.2%) account for nearly 88% of breach locations — both environments deeply dependent on identity and access management infrastructure
- Organizational scale is the strongest predictor of survivability in the regression model, with survival probability increasing sharply as employee count rises
- The data strongly supports a central hypothesis: modern healthcare breaches increasingly involve attackers logging into systems rather than breaking into them — exploiting identity and access management (IAM) failures rather than defeating technical defenses

These findings challenge conventional assumptions about healthcare cybersecurity risk. Breaches are often treated as technical events or compliance failures. The evidence suggests that breaches frequently act as organizational stress tests, exposing underlying weaknesses in governance, operational maturity, and financial resilience. Organizations most likely to fail are not those that suffered the largest breaches — they are the ones that lacked the structural capacity to absorb any significant breach at all.

This paper also introduces the Healthcare Breach Survivability Index (HBSI), a conceptual scoring model for estimating organizational survival probability based on structural characteristics including scale, governance maturity, identity management practices, financial resilience, and vendor ecosystem complexity.

Section 1: Introduction

1.1 The Evolving Healthcare Cybersecurity Landscape

Healthcare organizations occupy a uniquely dangerous position in the modern cybersecurity environment. They manage extraordinary volumes of sensitive personal data — medical histories, insurance records, financial information, and social identifiers — data that is both permanently valuable and effectively impossible to revoke once exposed. Unlike a compromised credit card number, a stolen medical record cannot be cancelled and reissued.

The digital transformation of healthcare over the past two decades has dramatically expanded the attack surface available to threat actors. Electronic health records, cloud-connected clinical systems, networked medical devices, remote access infrastructure, and sprawling vendor ecosystems have collectively created an environment of extraordinary complexity and exposure. Healthcare organizations now depend on interconnected systems that were frequently designed for clinical utility rather than security resilience.

Regulatory frameworks — most notably the Health Insurance Portability and Accountability Act (HIPAA) and its Security Rule — require healthcare organizations to report breaches affecting protected health information to the Department of Health and Human Services Office for Civil Rights. This reporting structure creates two distinct categories of breach events:

- Major breaches affecting 500 or more individuals, which must be reported to HHS and the media promptly and are listed on the public HHS breach notification portal
- Small breaches affecting fewer than 500 individuals, which must be documented internally and reported to HHS annually via a log submission

In 2023, HHS/OCR received approximately 320,000 total complaints — a figure that encompasses not only formal breach notifications but also privacy complaints, access complaints, and general HIPAA violation reports. In that same year, organizations submitted approximately 36,000 small-breach log entries covering incidents affecting fewer than 500 patients. Together, these figures illustrate the profound gap between the breach events that appear in public reporting and the full scope of healthcare privacy and security incidents occurring across the industry.

The public-facing breach notification portal — from which our study dataset is substantially derived — captures only a fraction of this activity: the major breach notifications from covered entities and business associates that meet the 500-individual threshold. Even within this more visible category, our study further scoped its analysis to exclude health plans and payors, government entities, and educational institutions, as discussed in detail in the Methodology section.

1.2 Why Survivability Matters

Most published analyses of healthcare breach data focus on familiar metrics: breach frequency, individuals affected, attack vectors, and regulatory penalties. These measures are useful for characterizing the threat landscape and evaluating compliance frameworks.

What they do not capture is what happens to the organization itself.

A cybersecurity breach is not only a privacy event. It triggers a cascade of secondary pressures — regulatory investigations, potential litigation, notification and remediation costs, operational disruption, reputational damage, and prolonged uncertainty about the organization's future. For many healthcare organizations, particularly smaller ones, these pressures combine to form something far more serious than a compliance problem. They can become an existential threat.

> ***"The breach does not create the failure. It reveals the weakness already present."***

This study asks a question that has received insufficient attention in both research and practice: What is the probability that a healthcare organization survives a cybersecurity breach? And what structural characteristics separate those that do from those that do not?

1.3 Research Objectives

This research was designed to achieve the following objectives:

- Accurately characterize the full scope of the healthcare breach problem, including the dimensions not captured in our study dataset
- Quantify the rate at which breached healthcare providers and business associates cease independent operations following a major incident
- Examine whether breach characteristics — type, size, location — correlate with organizational survival
- Identify structural organizational factors that appear to influence survivability
- Explore the role of identity and access management failures as a primary breach catalyst
- Introduce a conceptual framework for assessing organizational breach survivability
- Develop strategic implications for healthcare leaders, policymakers, and investors

Section 2: Research Methodology

2.1 Understanding the Full Breach Universe

Before describing the study dataset, it is essential to establish the broader context within which this research sits. Healthcare breach activity in the United States is reported through multiple channels, at different thresholds, and with varying levels of public visibility.

The most visible layer consists of major breach notifications submitted to HHS/OCR for incidents affecting 500 or more individuals. These notifications are published on the OCR breach portal and form the primary source of data for most healthcare breach research, including this study.

A less visible but numerically far larger layer consists of small breach events affecting fewer than 500 individuals. In 2023, approximately 36,000 such events were logged and reported to HHS on an annual basis. Because these events do not trigger immediate public notification, they are largely absent from public research and industry awareness — despite collectively representing an enormous volume of PHI exposure across the healthcare industry.

The broadest layer is the total HIPAA complaint and violation universe. In 2023, HHS/OCR received approximately 320,000 complaints — a figure encompassing formal breach notifications, patient privacy access complaints, and general HIPAA violation reports. This number reflects the true scope of privacy and security concerns across all healthcare entities subject to HIPAA regulation.

Layer	2023 Volume	Public Visibility	Included in This Study
Total HHS/OCR Complaints (all types)	~320,000	Internal/Aggregate	No
Small Breach Log Events (<500 individuals)	~36,000	Annual Aggregate	No
Major Breach Notifications (≥500 individuals)	~2,050 (2023–2026)	Public (OCR Portal)	Partial
This Study Dataset (providers & BAs only, data-accessible)	1,478 events (2023–2026)	Public (subset)	Yes

Table 1: The Healthcare Breach Reporting Hierarchy — Context for This Study

The table above illustrates the layered nature of healthcare breach reporting and the precise position of our study dataset within this broader hierarchy. Readers should interpret all findings in this paper with the understanding that they describe a specific, bounded population — not the full scope of healthcare breach activity.

2.2 Study Dataset Scope and Inclusions

The 1,478 organizations in the dataset were identified through public HHS/OCR breach notification records, supplemented with organizational profile data from commercial business intelligence sources to establish current operational status. The full HHS/OCR dataset for the same 2023–2026 period records 2,048 major breach notifications from healthcare providers and business associates — meaning the study dataset of 1,478 represents approximately 72% of the eligible universe. The remaining 28% (approximately 570 organizations) were excluded due to data accessibility constraints, as described in Section 2.3. These excluded organizations are likely disproportionately drawn from entities that dissolved rapidly after their breach, which means the 31.3% closure rate reported in this study should be understood as a conservative floor estimate.

Each record in the dataset includes the following variables:

- Organization classification (Healthcare Provider or Business Associate)
- Geographic information (city, state)
- Date of breach and date of HHS submission
- Type of breach (Hacking/IT Incident, Unauthorized Access/Disclosure, Theft, Loss, Improper Disposal)
- Location of breached information (Network Server, Email, Electronic Medical Record, Paper/Films, Laptop, Desktop Computer, Other)
- Number of individuals affected
- Organizational employee range (as a proxy for organizational scale)
- Whether a business associate was involved in the breach
- Current operational status (Open or Closed/Sold)

2.3 Explicit Exclusions and Their Significance

The following categories of healthcare entities were intentionally excluded from the study dataset, and each exclusion carries meaningful implications for interpretation:

Health Plans and Payors

Commercial health insurance carriers, Medicare Advantage plans, and pharmacy benefit managers were excluded from the dataset. This exclusion is analytically significant. Health plans often manage the largest patient data repositories in the healthcare ecosystem. Major breaches at health insurance organizations can affect tens of millions of individuals — far exceeding the scale of most provider-side events. Including health plans would have substantially altered the distribution of breach sizes and potentially the survival rate calculations, as large insurers operate with different financial profiles and resilience characteristics than clinical providers.

The exclusion means that our survivability findings apply specifically to the provider and business associate community. The breach dynamics — and survivability economics — of large health insurers are materially different from those of a community medical practice or a regional revenue cycle management firm.

Government Entities

Federal, state, and local government healthcare entities were excluded. Government-operated health organizations — including VA facilities, public health departments, and government-affiliated clinics — operate under different financial structures, accountability frameworks, and survival dynamics than private-sector healthcare organizations. A government entity that experiences a breach does not face the same market-driven closure risk as a private practice or commercial vendor. Including government entities would have artificially suppressed the closure rate findings.

Educational Institutions

Academic medical centers and university-affiliated healthcare entities were excluded for similar reasons. Academic institutions benefit from endowment resources, research funding, and institutional permanence that insulate them from the survivability pressures faced by commercial healthcare providers.

Data Accessibility Constraints

This exclusion creates a potential selection bias: organizations for which data was inaccessible may disproportionately include entities that dissolved quickly — meaning our 31.3% closure rate may underestimate the true failure rate among the studied population. Comparison with the full HHS/OCR dataset confirms the scale of this gap: 2,048 providers and business associates filed major breach notifications in the 2023–2026 period, versus 1,478 in this study, implying approximately 570 organizations (28%) could not be profiled for survivability status and are absent from our analysis.

2.4 Implications of Scope for Interpretation

The combination of these exclusions produces a dataset that is both more precisely defined and potentially more conservative in its findings than a fully comprehensive analysis would be. The 1,478 organizations studied represent a carefully bounded population: commercial healthcare providers and business associates that experienced major breaches affecting 500 or more individuals, for which sufficient organizational data was accessible.

The most important interpretive implication is this: our findings almost certainly understate the full scale of healthcare breach survivability risk. The 36,000 annual small-breach events in 2023

disproportionately affect smaller organizations — exactly the organizations our study shows are most vulnerable to post-breach closure. These small-breach organizations are invisible in our dataset, yet may represent some of the highest-risk entities in the healthcare ecosystem.

> ***The organizations most likely to fail after a breach — small independent practices and narrow-focus business associates — are also the organizations most likely to be absent from our study dataset, because their breaches fall below the 500-individual reporting threshold.***

2.5 Analytical Approach

The research employs both descriptive statistical analysis and logistic regression modeling. Descriptive analysis examines the distribution of breach types, locations, organizational sizes, and survival outcomes. Logistic regression models the probability of organizational survival as a function of structural and breach characteristics.

The dependent variable in the regression model is binary: organizational survival status (Open = 1, Closed = 0). Independent variables include breach type, breach location, individuals affected (log-transformed), employee range, and business associate involvement. The model achieved approximately 73% predictive accuracy on the study population.

Section 3: The Healthcare Breach Universe — What the Public Data Does Not Show

3.1 The Iceberg Structure of Healthcare Breach Reporting

To fully appreciate the significance of our study findings, it is necessary to understand the structure of healthcare breach reporting and the relationship between what is publicly visible and what actually occurs.

The HHS/OCR breach portal — commonly referred to as the 'Wall of Shame' — publishes major breach notifications affecting 500 or more individuals. This represents the visible surface of healthcare breach activity. Below this surface, two substantially larger bodies of breach data exist with far less public visibility.

The first is the annual small-breach log. HIPAA requires covered entities and business associates to maintain a log of all breaches affecting fewer than 500 individuals and to submit this log to HHS annually. In 2023, approximately 36,000 such events were reported. Each of these events represents a real exposure of patient health information — often involving a single misdirected email, an unauthorized access event by an employee, or a lost device containing patient data. Individually, these events are small. Collectively, they represent an enormous volume of privacy harm that never receives the public scrutiny reserved for major breach events.

The full HHS/OCR dataset, spanning mandatory reporting since 2009, provides a cumulative perspective that contextualizes the annual figures described in this section. Across all entity types and all years through early 2026, healthcare organizations have reported breaches affecting a combined total of approximately **943.9 million individual records** — approaching one billion PHI exposures since the reporting framework was established. Of that cumulative total, approximately **542 million records** were exposed in the 2023–2026 period alone — meaning more than half of all healthcare PHI exposures in the history of mandatory reporting have occurred in just the last three years. These figures apply to major breach notifications only and exclude the tens of thousands of annual small-breach events, further confirming that the visible data represents only a fraction of actual healthcare privacy harm.

The second, even larger layer is the total HHS/OCR complaint volume. In 2023, HHS received approximately 320,000 complaints. This figure encompasses the full range of HIPAA-related concerns: privacy complaints about unauthorized disclosures, access complaints from patients denied their records, breach notifications at all scales, and general security rule violation reports. The 320,000 figure represents the outer boundary of healthcare privacy and security concerns reaching the federal regulator in a single year.

Reporting Category	Approx. 2023 Volume	Nature of Events
Total HHS/OCR Complaints	~320,000	All HIPAA privacy, security, and access complaints across all entity types
Small Breach Log Submissions (<500 individuals)	~36,000	Minor PHI exposure events; annual reporting, no immediate notification required
Major Breach Notifications (≥500 individuals, all entity types)	746	Large breaches triggering immediate notification to HHS, media, and affected individuals
This Study: Major breaches, providers & BAs only, 2023 portion	433	Subset of major breach notifications; excludes health plans, government, educational entities

Table 2: Healthcare Breach Reporting Layers and Study Dataset Position

3.2 What the Small-Breach Iceberg Tells Us

The 36,000 small breach events reported in 2023 carry a significance that extends well beyond their individual scale. These events disproportionately occur in exactly the organizations that our study identifies as most vulnerable to post-breach failure: small independent practices, community clinics, and narrow-focus business associates.

A small medical practice experiencing its third or fourth small breach event over a few years is accumulating regulatory exposure, compliance costs, and reputational damage in ways that may not be visible in any single reporting threshold — yet may collectively constitute a survivability risk equal to or greater than a single major breach event. The HIPAA reporting structure, which treats small breaches as an administrative logging requirement rather than an urgent public disclosure, may therefore systematically underrepresent the cumulative cyber harm being experienced by the most vulnerable segment of the healthcare provider population.

3.3 The Missing Health Plan Dimension

The exclusion of health plans and payors from our study dataset represents another dimension of the healthcare breach universe that deserves explicit attention. Commercial health insurers manage some of the largest repositories of protected health information in the entire healthcare ecosystem.

Major breach events at large health insurance organizations can affect tens of millions of individuals — a scale that dwarfs the typical provider-side incident. The financial and operational profiles of large commercial insurers are also materially different from those of clinical providers:

they have larger capital reserves, more sophisticated legal and regulatory relationships, and different competitive dynamics.

Mid-sized regional health plans, and specialty benefit managers face many of the same structural vulnerabilities as clinical providers — without the patient-relationship anchors that can help providers retain their communities even after a breach. The scale of this excluded sector is now quantifiable: the full HHS/OCR dataset records 903 health plan breach notifications across all years of mandatory reporting, with 241 occurring in the 2023–2026 period alone. Health plans accounted for 10.5% of all major breach notifications in that period, with 72% of their breaches classified as Hacking/IT Incidents — a distribution nearly identical to the provider and BA populations in this study. The survivability dynamics among mid-market health plans remain a significant research gap; the preliminary hypothesis that organizational resilience rather than breach magnitude determines survival is likely to hold across entity types.

A comprehensive extension of this research should include the health plan sector. The survivability dynamics among health plans may differ from providers in degree but not in kind. The preliminary hypothesis — that organizational resilience rather than breach magnitude determines survival — is likely to hold across entity types.

3.4 What This Means for Interpreting Our Findings

The study findings presented in subsequent sections should be read with two simultaneous understandings:

- Within our study population — commercial healthcare providers and business associates experiencing major breaches — the 31.3% closure rate is a well-supported and analytically robust finding
- Across the full healthcare breach universe, the actual scale of organizational harm from cyber incidents is almost certainly larger, affecting more organizations at smaller thresholds in ways that current public reporting structures do not capture

Together, these understandings support a conclusion that is more alarming than the study dataset alone would suggest: the 31.3% closure rate we document may represent a floor, not a ceiling, on the organizational survival risk that healthcare entities face from cybersecurity incidents.

Section 4: Key Statistical Findings From the Study Dataset

The following findings are derived from analysis of the 1,478-organization study dataset and describe outcomes within this specific, bounded population of commercial healthcare providers and business associates experiencing major breaches.

4.1 Organizational Survival Rates

The most consequential finding of this research is the proportion of breached healthcare organizations that ceased independent operations following their breach events.

Organizational Status	Count	Percentage of Study Dataset
Still Operating	1,016	68.7%
Closed or Sold	462	31.3%
Total	1,478	100%

Table 3: Organizational Outcomes — Healthcare Providers & Business Associates, Major Breaches, Jan 2023 – Feb 2026

Nearly one-third of organizations in the study dataset — 462 out of 1,478 — are no longer operating independently. This figure includes organizations that dissolved entirely, merged with larger health systems, or were acquired in transactions driven at least in part by breach-related distress.

> ***31.3% of studied healthcare providers and business associates experiencing major breaches did not survive as independent entities. This figure applies to the study population and likely understates the true closure rate across all breached healthcare organizations, particularly those experiencing small breaches below the 500-individual threshold.***

4.2 Breach Size vs. Organizational Survival

One of the most counterintuitive findings concerns the relationship between breach magnitude and organizational survival. Organizations that closed following a breach generally experienced smaller breaches than those that survived:

Status	Mean Individuals Affected	Median Individuals Affected
Closed / Sold	~40,371	~5,060
Still Operating	~193,814	~9,139

Table 4: Breach Size by Organizational Outcome

Organizations that closed experienced breaches averaging approximately 4.8 times smaller than those that remained open. This pattern confirms that breach magnitude is not the primary determinant of organizational survival. The capacity to survive a breach depends far more on the structural characteristics of the organization than on the size of the incident itself.

This finding has a particularly important implication when considered alongside the excluded small-breach population. If organizations in our study dataset — where breaches affected a minimum of 500 individuals — are closing at a 31.3% rate despite experiencing relatively large incidents, then the organizations experiencing the 36,000 annual small-breach events (which fall entirely below our study threshold) may face comparable or higher closure risk from incidents that are individually smaller but may be equally destabilizing given those organizations' limited resilience capacity.

4.3 Breach Type Distribution

Type of Breach	Count	Percentage
Hacking / IT Incident	1,228	83.1%
Unauthorized Access / Disclosure	214	14.5%
Theft	22	1.5%
Loss	7	0.5%
Improper Disposal	7	0.5%
Total	1,478	100%

Table 5: Breach Type Distribution Across Study Dataset

Hacking and IT incidents account for 83.1% of all breach events. Combined with unauthorized access events — which frequently involve credential misuse — digital intrusion methods account for 97.6% of all breach activity in the study population. Physical theft, loss, and improper disposal together represent less than 3%. The concentration of hacking in this dataset is itself noteworthy in historical context: the full HHS/OCR dataset spanning all years since 2009 shows hacking at

58.1% of all breach types, meaning the 83.1% rate in the 2023–2026 study period represents a dramatic acceleration — hacking as a share of all breach types has nearly doubled relative to the long-run baseline. This shift reinforces the central IAM hypothesis: the threat environment has fundamentally reoriented toward credential exploitation over the past several years.

It is worth noting that the breach type distribution in the small-breach population may differ somewhat from these proportions. Small breaches are more likely to involve misdirected emails, inadvertent disclosures, or employee snooping — though credential-based attacks have become increasingly prevalent across all breach size categories.

4.4 Location of Breached Information

Location of Breached Information	Count	% of Dataset
Network Server	968	65.5%
Email	328	22.2%
Paper / Films	62	4.2%
Electronic Medical Record (EMR)	48	3.2%
Laptop	12	0.8%
Desktop Computer	10	0.7%
Other / Multiple Systems	50	3.4%

Table 6: Location of Breached Information

Network servers and email systems together account for approximately 87.7% of all breach locations. Both environments are deeply dependent on identity and access management infrastructure. The dominance of these two systems strongly suggests that many healthcare breaches occur at the identity layer — through compromised credentials rather than technical exploit.

4.5 Business Associate Involvement

Business Associate Involved	Count	Percentage
No Business Associate	1,020	69.0%
Business Associate Involved	458	31.0%

Table 7: Business Associate Involvement in Breach Events

Approximately 31% of breaches in the study dataset involved a business associate. Interestingly, organizations with business associate involvement showed slightly higher survival rates — likely reflecting a selection effect where organizations that maintain formal vendor relationships with business associate agreements tend to demonstrate greater overall governance maturity.

4.6 Geographic and Industry Distribution

Breach events in the full HHS/OCR dataset for 2023–2026 are concentrated in states with the largest healthcare provider populations: California (197 events), Texas (160), New York (149), Florida (119), and Illinois (96). Note that state rankings from the study subset differ slightly from the full HHS dataset because the study subset excludes health plans, government, and educational entities; the full-dataset rankings above reflect all entity types. By industry category within the study subset, Hospital and Health Care entities account for 839 organizations (56.8%), followed by Health, Wellness and Fitness (102, 6.9%), Mental Health Care (34, 2.3%), Insurance (26, 1.8%), and a range of healthcare technology and administrative service firms.

4.7 Temporal Trends

Year	Study Dataset Events	Year-over-Year Change
2023	433	Baseline
2024	464	+7.2%
2025	523	+12.7%
2026 (partial)	83	N/A (partial year)

Table 8: Breach Events in Study Dataset by Year (Providers & BAs Only)

The year-over-year increase within the study dataset — from 433 events in 2023 to 523 in 2025, a 20.8% increase — reflects continued growth in the provider and business associate study population. Context from the full HHS/OCR dataset (all entity types) adds important nuance: macro-level major breach notifications plateaued in the 730–750 range annually from 2022 through 2025, suggesting that the broader breach environment may be stabilizing in volume even as the study subset continues to grow. This does not diminish the threat; rather, it signals that growth is concentrated in specific entity categories. The upward trajectory within providers and business associates, when considered alongside the approximately 320,000 HHS complaints received in 2023 alone, confirms that major breach pressure on clinical and vendor organizations remains acute and unresolved.

Section 5: Regression Modeling of Organizational Survivability

5.1 Logistic Regression Overview

To examine whether breach and organizational characteristics can predict survivability within the study population, a logistic regression model was applied to the dataset. Logistic regression estimates the probability of a binary outcome — in this case, whether an organization remains operational (1) or closes/is sold (0) following a breach.

The model incorporates breach type, breach location, individuals affected (log-transformed), employee range, and business associate involvement as independent variables. It achieved approximately 73% predictive accuracy on the study dataset. This level of accuracy indicates meaningful statistical associations between observable characteristics and survivability outcomes, while also confirming that significant unexplained variance remains — variance that likely resides in unobserved organizational variables such as financial health, governance maturity, and security program sophistication.

5.2 Organizational Scale as the Dominant Predictor

Among the variables tested, organizational scale — as measured by employee range — demonstrates the most consistent and robust association with survival probability. Larger organizations across every breach type and location category show materially higher survival rates:

Employee Range	Count in Dataset	Approx. Survival Rate	Risk Level
1 – 10 employees	139	~56%	Very High Closure Risk
11 – 50 employees	257	~58%	Very High Closure Risk
51 – 250 employees	435	~68%	Elevated Closure Risk
251 – 1,000 employees	282	~75%	Moderate Risk
1,000 – 5,000 employees	159	~85%	Low Risk
5,000 – 10,000 employees	44	~88%	Very Low Risk
10,000+ employees	55+	~90%+	Minimal Closure Risk

Table 9: Employee Range vs. Estimated Survival Rate — Study Dataset

The survival probability gradient across employee ranges is striking: the difference between organizations with 1-10 employees (~56% survival) and those with 10,000+ employees (~90%+) is approximately 34 percentage points. This differential is not primarily a function of the types of breaches experienced — it reflects the structural capacity of the organization to absorb and recover from breach consequences.

This finding becomes even more significant when considered alongside the excluded small-breach population. Organizations experiencing 36,000 annual small-breach events are disproportionately small entities — and if our study shows that small organizations in the major-breach population face 44% closure rates, the survival dynamics for the small-breach population may be at least as severe.

5.3 The Primacy of Structure Over Breach Characteristics

The regression analysis confirms that breach characteristics themselves — size, type, and location — are not strong predictors of organizational closure on their own. Neither breach magnitude nor attack method reliably differentiates organizations that survive from those that do not.

> ***The breach is not the cause of organizational failure. The breach is the event that reveals whether an organization had the resilience to survive disruption in the first place.***

This finding has a profound practical implication. Security programs that focus exclusively on breach prevention — without also building organizational resilience — are addressing only half the problem. An organization that cannot survive a breach it could not prevent has not adequately managed its enterprise risk.

5.4 Business Associate Involvement and the Governance Signal

Business associate involvement shows a slight positive association with organizational survival in the regression model. This counterintuitive finding — that organizations whose breaches involved a third party are marginally more likely to survive — is most plausibly explained as a governance maturity signal. Organizations that maintain formal vendor relationships with executed business associate agreements tend to be more operationally mature overall. The vendor relationship proxies for broader governance sophistication that contributes to resilience.

Section 6: Identity and Access Management as a Breach Catalyst

6.1 The 'Logging In' Hypothesis

The concentration of breach events in email systems and network servers — two environments that are fundamentally structured around identity and authentication — leads to a central hypothesis: many modern healthcare breaches do not involve attackers defeating technical defenses through sophisticated exploit code. Instead, they involve attackers obtaining valid credentials and operating within systems as though they were legitimate users.

> ***Modern healthcare attacks are not breaking in. They are logging in.***

This hypothesis is consistent with the broader trajectory of cybersecurity threat intelligence across industries. Credential compromise — through phishing, password reuse, credential stuffing, MFA bypass, and OAuth token abuse — has become one of the dominant initial access vectors for threat actors. Healthcare environments are particularly susceptible because of structural tensions between clinical workflow demands and strict access control practices.

The IAM hypothesis also provides a compelling explanation for a pattern that appears across both the major-breach population in our study and the broader small-breach universe: the consistency of attack pathways. If attackers were exploiting unique technical vulnerabilities in each organization, we would expect greater diversity in breach locations and types. Instead, the remarkable concentration in email and server environments — repeated year after year across thousands of distinct organizations — suggests systematic exploitation of consistent identity weaknesses across the healthcare sector.

6.2 Healthcare IAM Vulnerabilities

Healthcare organizations face identity and access management challenges that are structurally distinct from many other industries. The clinical care environment places an enormous premium on speed and clinician convenience — priorities that frequently conflict with strict access control enforcement:

- Shared workstation accounts used across clinical staff shifts, eliminating individual accountability
- Generic or role-based credentials for high-use clinical systems with broad access privileges

- Weak or inconsistent multi-factor authentication enforcement, particularly for legacy clinical applications
- Inadequate lifecycle management — former employees, contractors, and vendor accounts retaining active credentials after departure
- Complex Active Directory environments with inconsistent privileged access controls
- Third-party vendor accounts with persistent access to internal systems between engagements
- Remote access infrastructure (VPN, RDP) with insufficient authentication controls

These conditions create environments where credential misuse is often easier than technical exploitation. Once a threat actor possesses a valid credential — whether obtained through phishing, credential harvesting, or password reuse from previously compromised databases — they can frequently access sensitive systems with minimal resistance.

6.3 Email as an Identity Attack Vector

Email systems account for 22.2% of breach locations in the study dataset. Email breaches in healthcare typically occur through: phishing campaigns that capture email credentials or linked system access; business email compromise attacks that hijack administrative accounts; OAuth token abuse providing persistent access; and account takeover through password reuse. In each scenario, the attacker authenticates as a legitimate user — not a technical intruder.

This pattern is likely even more prevalent in the small-breach population excluded from our study. Many of the 36,000 annual small-breach events in 2023 involve exactly this type of incident: a single compromised email account used to access a limited number of patient records. The IAM failure is identical to what occurs in major breach events — the difference is typically the scope of what the attacker chooses to access or exfiltrate, not the nature of the initial compromise.

6.4 Network Server Breaches and Credential Pathways

Network server breaches, constituting 65.5% of breach locations in the study dataset, typically begin with the same fundamental vulnerability: identity compromise. Common pathways include compromised VPN credentials providing remote access to internal infrastructure; stolen domain credentials enabling lateral movement through Active Directory; compromised administrator accounts providing elevated access to servers and databases; and exposed RDP services with weak authentication controls.

Once a threat actor establishes a foothold through compromised credentials, ransomware deployment or data exfiltration typically proceeds through legitimate authentication mechanisms rather than technical bypasses. The attack unfolds inside the security perimeter, not against it.

6.5 The Governance Dimension of IAM Failure

The most important dimension of the IAM problem is not technical but organizational. Many healthcare organizations possess the technical capability to implement strong identity controls. The failure is frequently one of governance: the organizational willingness to prioritize security over operational convenience.

Clinical leadership may resist MFA enforcement because it slows workflows. Operations teams may tolerate shared accounts because individual provisioning requires more administrative effort. IT departments may lack the authority to enforce least-privilege policies that clinical staff find restrictive.

This governance dimension means that IAM improvements require more than a technology investment. They require executive sponsorship, clinical buy-in, and clear policies that establish security as an organizational priority — not a negotiable tradeoff against convenience. Organizations that treat IAM governance as an executive priority rather than an IT housekeeping task demonstrate substantially stronger breach resilience. Our data, while not capturing this variable directly, supports this interpretation through the strong correlation between organizational maturity and survival outcomes.

Section 7: Organizational Resilience Thresholds

7.1 Three Resilience Tiers

The dataset strongly suggests that healthcare organizations cluster into distinct resilience categories that determine whether a breach represents a manageable disruption, a serious crisis, or an existential threat.

Tier 1: Fragile Organizations

These organizations typically operate with fewer than 50 employees, thin financial margins, and minimal internal security infrastructure. Technology is managed by external providers of varying capability. Security programs, to the extent they exist, are compliance-oriented rather than operationally mature.

When a breach occurs, resulting costs — legal fees, notification expenses, regulatory investigations, and operational disruption — may collectively exceed the organization's financial capacity to absorb them. The breach frequently becomes the precipitating event in a sequence that ends in dissolution, sale, or merger. Fragile organizations represent the largest segment of closure cases in the study dataset, with closure rates approaching 42-44% for organizations with fewer than 50 employees.

Critically, this tier also represents a population that is substantially under-studied. The 36,000 annual small-breach events are disproportionately concentrated among fragile organizations — meaning that even our documented closure rates for this tier likely represent only a portion of the true post-breach failure rate across all small healthcare providers.

Tier 2: Operationally Stable Organizations

Tier 2 organizations possess sufficient operational and financial infrastructure to survive breach events, though they may experience significant disruption. They have dedicated IT staff, basic security programs, and access to legal and regulatory resources. They may have cyber insurance that partially offsets response costs. These organizations survive their breach events but may emerge with weakened competitive positions, reduced patient trust, or ongoing regulatory scrutiny.

Tier 3: Resilient Organizations

Tier 3 organizations demonstrate mature security governance, dedicated security leadership, strong identity and access management controls, and the financial resilience to absorb incident response costs without existential impact. These organizations have formal incident response

plans, threat detection capabilities, and established relationships with cybersecurity counsel and forensic response providers. For them, breach events become operationally significant disruptions rather than organizational crises.

7.2 The Resilience Threshold

A meaningful resilience threshold appears in the data at approximately the 1,000-employee level, where survival rates begin to exceed 85% and increase significantly from that point. Below this threshold, organizations face materially elevated closure risk.

The threshold concept has critical practical implications. For smaller healthcare organizations, the question is not merely how to prevent a breach, but how to build sufficient organizational infrastructure to survive one — because the probability of experiencing a breach, given the current threat environment, cannot be reduced to zero through any defensive investment alone.

7.3 Cybersecurity as a Healthcare Consolidation Force

When smaller organizations fail at significantly higher rates following breaches and are subsequently acquired by larger health systems or absorbed by private equity platforms, cybersecurity pressure becomes an accelerant of market consolidation. This effect is structural and ongoing. As breach rates increase year over year, smaller healthcare organizations face persistent, elevated existential risk that larger competitors do not.

When the scale of the full breach universe is considered — including the 36,000 annual small-breach events concentrated among smaller providers — the consolidation pressure is even more significant than the study dataset alone suggests. Cybersecurity is not only a patient safety and privacy issue. Through its differential impact on organizational survival, it is functioning as a structural economic force within healthcare markets, one that has received insufficient regulatory and policy attention.

Section 8: Structural Risk Categories in Healthcare

8.1 Three Organizational Profiles Most Vulnerable to Post-Breach Failure

When the dataset is segmented by organizational characteristics, three distinct profiles emerge among organizations with the highest closure rates. Understanding these profiles is essential for identifying where targeted intervention — from the organizations themselves, regulators, or the broader ecosystem — is most needed.

Profile 1: Small Independent Clinical Practices

The largest single category of post-breach closures consists of small independent clinical practices: physician-owned specialty clinics, behavioral health providers, dental practices, physical therapy clinics, imaging centers, and small surgical groups. These organizations are structurally vulnerable for interconnected reasons:

- No internal security leadership — few small practices can afford a dedicated security professional
- Outsourced technology managed by small MSPs whose cybersecurity expertise varies widely
- Security policies that exist as compliance documentation but lack operational enforcement
- Minimal or absent cyber insurance coverage
- Extremely thin operating margins that leave no financial buffer for breach-related costs

This profile is particularly important when considered alongside the small-breach data. The 36,000 annual small-breach events include an enormous number of these organizations — practices that may be accumulating regulatory exposure, compliance costs, and notification obligations from multiple small events that individually fall below the public reporting threshold but collectively represent significant organizational strain.

Profile 2: Healthcare Business Associates With Narrow Service Models

Revenue cycle management firms, medical transcription services, billing processors, and niche healthcare software vendors represent a distinct vulnerability category. These organizations depend entirely on the trust of their healthcare clients. When a breach occurs, client contracts are terminated, competitors fill the gap, and litigation risk escalates — destroying the core commercial asset that the business model is built upon. Unlike clinical providers that retain patient relationships even after a breach, a business associate's commercial position can be destroyed almost immediately.

> **Case Illustration: Change Healthcare (2024).** The full HHS/OCR dataset reveals that the single largest healthcare breach ever recorded involved Change Healthcare, Inc. — a Business Associate — which reported 192.7 million individuals affected in July 2024. This figure exceeds the Anthem breach (78.8 million, 2015) by more than 2.4 times and represents approximately 57% of the U.S. population. Change Healthcare provides payment processing, claims clearinghouse, and revenue cycle services to thousands of healthcare organizations, illustrating precisely the systemic vulnerability of narrow-model BAs described in this profile: a single point of credential compromise in a deeply interconnected vendor cascaded into the largest known PHI exposure in history. The organizational and operational consequences — including UnitedHealth Group absorbing billions in losses and congressional scrutiny — underscore that BA survivability risk operates at a scale that can threaten the broader healthcare market, not merely individual organizations.

Profile 3: Rapidly Scaling Healthcare Platforms With Immature Security Programs

Rapidly expanding healthcare platforms — PE-backed consolidation groups, multi-site urgent care networks, telehealth companies — face a specific structural risk: security maturity rarely scales at the same pace as the business. Growth through acquisition creates fragmented IT infrastructure, inconsistent access controls, and identity environments with thousands of accounts across multiple systems. When a breach occurs in these environments, the fragmentation amplifies both incident scope and response difficulty — triggering regulatory scrutiny and investor concern simultaneously.

8.2 The Common Thread

Organization Type	Core Structural Weakness	Population Captured in This Study
Small independent practices	No security leadership; no financial buffer	Partial — major breaches only; small breaches excluded
Business associates (narrow model)	Trust-dependent revenue; no patient relationship anchor	Yes — fully represented in study dataset
Rapidly scaling PE platforms	Growth outpacing governance and security maturity	Partial — larger platforms represented; smaller roll-ups may be excluded

Table 10: Structural Risk Profiles and Study Dataset Coverage

The table above reinforces a critical point: our study dataset most fully captures the business associate population, while the small independent practice population is substantially represented only through its major breach events. The full extent of failure risk among small practices — including those experiencing the 36,000 annual small-breach events — is not captured in our 31.3% closure rate.

Section 9: Structural Insights Beyond the Visible Data

9.1 Compliance Is Not Operational Security

Most organizations in our study dataset almost certainly had HIPAA compliance programs in place at the time of their breach. They conducted required risk assessments, maintained written policies, completed workforce training, and managed vendor agreements.

They were breached anyway.

The continued frequency of breaches across organizations of all sizes, in a heavily regulated industry, across a sector experiencing approximately 320,000 HHS complaints in a single year, strongly suggests a fundamental gap between compliance and operational security capability. HIPAA's Security Rule defines what healthcare organizations should have — policies, procedures, access controls, audit mechanisms. It does not effectively measure whether those controls actually work against real adversaries.

> ***Compliance programs measure the presence of governance processes. Operational security measures whether those processes work. The 320,000 annual HHS complaints and 36,000 small-breach events confirm that governance documentation alone is not protecting patients or organizations.***

9.2 The Survivorship Bias Problem — Amplified by Scope

The survivorship bias concern inherent in any breach survivability study is amplified in this research by the scope exclusions. Our dataset captures organizations that reported major breaches and for which organizational status could be subsequently verified. Organizations that failed most rapidly may disappear before data collection is possible.

More significantly, the 36,000 annual small-breach events are essentially invisible in our analysis. If a small practice experiences a minor breach, closes within a few months under combined financial and regulatory pressure, and submits its annual small-breach log before dissolution, it does not appear in our dataset at all. The 31.3% closure rate we report may therefore meaningfully underestimate the true post-breach failure rate across the full healthcare provider population.

9.3 The Healthcare Technology Monoculture

The consistent concentration of breaches in the same technical environments — network servers and email systems — repeated year after year across thousands of distinct organizations, suggests a structural pattern: technological monoculture. Healthcare organizations, particularly smaller providers, frequently share common EHR platforms, cloud service providers, email environments, and remote access architectures.

This convergence creates conditions in which attack techniques developed against one organization can be rapidly deployed against many others. The remarkable consistency of breach locations across the study dataset — and almost certainly across the much larger small-breach population as well — suggests that healthcare organizations are not each facing unique adversaries. They are facing the same attack playbooks, applied repeatedly against the same systemic weaknesses.

9.4 Breach Magnitude as a Misleading Metric

The industry standard for measuring breach severity — number of individuals affected — is a poor proxy for the variable that actually matters: organizational impact. Two breaches affecting the same number of individuals can have dramatically different operational consequences depending on whether the incident involved ransomware encrypting clinical systems versus an email account compromise exposing a limited record set.

This metric problem is particularly pronounced when considering the boundary between major and small breaches. A breach affecting 499 individuals is classified as a small breach requiring only annual log reporting; a breach affecting 501 individuals is a major breach requiring immediate notification and public disclosure. The operational and survivability impact on the affected organization may be nearly identical — yet the reporting framework treats them as categorically different.

Future research should attempt to develop multi-dimensional severity measures that incorporate operational downtime, clinical service disruption, time to recovery, financial cost, and organizational outcome alongside record count.

Section 10: The Healthcare Breach Survivability Index (HBSI)

10.1 Conceptual Framework

Drawing on the research findings, this paper proposes the Healthcare Breach Survivability Index (HBSI) — a scoring model for estimating the probability that a healthcare organization will survive a major cybersecurity breach based on assessable structural characteristics.

The HBSI is designed to be practical: it incorporates variables that can be evaluated through organizational assessment without requiring access to internal financial records that may not be publicly available. The goal is to produce a score that is both meaningful and actionable — providing healthcare leaders with a structured framework for evaluating and improving organizational resilience. The model applies across the full spectrum of healthcare entities, from small independent practices experiencing small breaches to large systems managing major incidents.

10.2 HBSI Scoring Variables

HBSI Variable	Weight	Rationale
Organizational Scale	25%	Strongest predictor in regression analysis; larger organizations have greater financial and operational resilience capacity
Identity Governance Maturity	20%	Primary breach vector; IAM discipline directly determines breach probability and lateral movement exposure
Operational Resilience	15%	Incident response capability; business continuity planning; recovery infrastructure readiness
Financial Stability	15%	Capacity to absorb legal, regulatory, and remediation costs without triggering organizational failure
Vendor Ecosystem Maturity	10%	Quality of third-party oversight; BA agreement governance; vendor security requirement enforcement
Incident Response Capability	10%	Formal IR planning; tabletop exercises; forensic response partnerships; detection speed
Infrastructure Complexity	5%	Attack surface management; legacy system exposure; integration governance maturity

Table 11: HBSI Variable Weights and Rationale

10.3 HBSI Score Interpretation

Score Range	Risk Level	Interpretation
0 – 40	Critical Risk	High probability of organizational failure following any significant breach. Immediate resilience investment required.
41 – 65	Elevated Risk	Significant closure risk. Structural gaps exist that may overwhelm capacity if a breach occurs.
66 – 80	Moderate Risk	Organization likely survives a breach but faces meaningful disruption and potential long-term impairment.
81 – 90	Stable	Organization has substantial resilience capacity. Breaches are survivable with well-managed response.
91 – 100	Resilient	Mature resilience infrastructure. Breaches are operationally significant but not existential.

Table 12: HBSI Score Interpretation

10.4 HBSI Applications

The HBSI framework has several practical applications:

- Board-level risk assessment: HBSI scoring provides boards with a structured basis for evaluating cybersecurity risk in terms of organizational survivability rather than purely technical metrics
- Cyber insurance underwriting: insurers can use HBSI-style assessments to more accurately price coverage and structure incident response support, particularly for the small-organization segment most at risk
- Merger and acquisition due diligence: investors and acquirers can use HBSI assessments to evaluate cyber resilience in healthcare transactions
- Regulatory risk assessment: regulators can use survivability frameworks to identify market segments at greatest risk of breach-driven consolidation
- Small provider support programs: policymakers can use HBSI-type assessments to target technical assistance and shared security infrastructure toward organizations most likely to fall below the resilience threshold

Section 11: Strategic and Policy Implications

11.1 For Healthcare Boards and Executive Leaders

The evidence that approximately one in three major-breach organizations studied did not survive as independent entities — combined with the context of 320,000 annual HHS complaints and 36,000 annual small-breach events — constitutes a board-level governance reality, not merely an IT risk metric.

Healthcare boards that have not established a structured, ongoing process for evaluating cybersecurity resilience — not just compliance status — are operating with an incomplete understanding of their enterprise risk profile. Recommended governance shifts include:

- Cybersecurity should appear on board agendas as an organizational survivability dimension alongside financial, operational, and reputational risk
- Executive accountability for security resilience — including identity governance — should be clearly defined and reported on regularly
- Boards should evaluate not only whether the organization has experienced a breach, but whether it is structurally prepared to survive one
- Investment in resilience should be framed as an enterprise survival investment, not solely a compliance or prevention cost

11.2 For Smaller Healthcare Organizations

For smaller healthcare organizations — physician practices, independent clinics, small behavioral health providers — the research findings are sobering. The closure rate among organizations with fewer than 50 employees approaches 42-44% in the major-breach study population. Given that these organizations also disproportionately populate the 36,000 annual small-breach category, the cumulative cyber risk exposure is significant.

Achievable steps for smaller organizations include:

- Obtain adequate cyber insurance with incident response services included — even basic coverage can be the difference between managed recovery and organizational failure
- Prioritize identity governance: implement multi-factor authentication, enforce least-privilege access, and manage credential hygiene consistently — these are the controls that address the primary attack vector
- Develop a basic incident response plan before a breach occurs — including relationships with legal counsel and a forensic response provider
- Consider managed security service partnerships that provide security monitoring and identity management capabilities without requiring internal staffing

11.3 For Regulators and Policymakers

The current regulatory framework for healthcare cybersecurity focuses primarily on privacy protection and breach notification. The research — particularly when the full breach universe is considered — suggests that policymakers should consider a broader mandate that accounts for organizational survivability and market stability:

- Minimum operational resilience standards: beyond compliance documentation, consider standards requiring demonstrated security capability, particularly for organizations serving vulnerable populations
- Small provider support infrastructure: the concentration of small-breach events among small providers suggests a need for shared security resources — shared security operations centers, subsidized identity management tools, or federal technical assistance programs
- Market consolidation monitoring: regulators should track whether cybersecurity-driven consolidation is reducing healthcare access in specific communities as smaller providers are absorbed or dissolved
- Reporting framework modernization: annual small-breach log reporting may be insufficient to identify emerging survivability risks among the most vulnerable provider segment — more frequent small-breach notification thresholds or aggregate analysis programs could improve early warning capabilities

11.4 For Cyber Insurers

Cyber insurers have direct financial exposure to the survivability dynamics documented in this research. Organizational scale should be a primary underwriting variable — the data confirms that smaller organizations face materially higher closure risk, implying different claims profiles and support needs. Pre-breach resilience assessments incorporating HBSI-style elements could improve both pricing accuracy and loss prevention. Insurers should also analyze whether their small-provider book of business adequately reflects the cumulative risk exposure from repeated small-breach events that precede major incidents.

Section 12: Future Research Directions

12.1 Expanding to the Full Breach Universe

The most important extension of this research would incorporate the full healthcare breach universe — including small-breach events, health plan and payor entities, and government and educational healthcare organizations. Each of these populations likely exhibits distinct survivability dynamics, and including them would substantially improve the completeness of the healthcare breach survivability picture.

Small-breach survivability analysis in particular represents a significant research gap. The 36,000 annual small-breach events represent a large, vulnerable population about which essentially nothing is known from a survivability perspective. A study that tracks the three- to five-year organizational fate of entities reporting repeated small breaches would likely reveal closure rates equal to or higher than those documented in this study.

12.2 Building a Validated Predictive Model

The ultimate objective toward which this research points is a validated, prospective Healthcare Breach Survivability Index — one that can estimate organizational closure probability before a breach occurs and guide targeted resilience investments. This will require incorporating variables not currently available in public breach datasets: financial health indicators, cybersecurity governance maturity assessments, cyber insurance coverage details, incident detection and response timelines, and identity governance maturity measures. Partnership between researchers, healthcare organizations, and potentially regulators will be necessary to develop the longitudinal dataset required.

12.3 Quantifying the Consolidation Effect

The data suggests that cybersecurity pressure is accelerating healthcare market consolidation. Future research should attempt to quantify this effect: to what extent are post-breach acquisitions driving consolidation in specific healthcare market segments, and what are the downstream effects on healthcare access, competition, and patient outcomes? This question bridges healthcare cybersecurity research and health economics in ways that neither field has yet adequately addressed.

Section 13: Conclusion

This research set out to answer a question that has received insufficient attention: what happens to healthcare organizations after they experience a cybersecurity breach?

The answer, as documented across 1,478 healthcare providers and business associates experiencing major breaches between January 2023 and early 2026, is both clear and consequential: approximately one in three did not survive as independent entities. The closure rate of 31.3% documented in our study population represents a material survivability risk that the healthcare industry has not yet fully reckoned with.

But the full picture is larger and more alarming than even this finding suggests. Our study dataset represents the data-accessible portion of the major-breach population, limited to commercial providers and business associates. Set against the backdrop of approximately 320,000 HHS complaints and 36,000 small-breach events in a single year — events involving organizations that are largely invisible in our dataset yet disproportionately drawn from the most vulnerable segments of the healthcare provider community — the 31.3% closure rate is almost certainly a conservative floor on the true organizational harm that healthcare cybersecurity incidents are causing.

> ***The healthcare breach crisis is not only a privacy problem. It is a survivability problem — and its full scale is substantially larger than public reporting structures currently reveal.***

Within our study population, the data yields a finding that challenges conventional assumptions about cyber risk: organizations that closed had, on average, smaller breaches than those that survived. Breach magnitude does not predict survival. What predicts survival is organizational resilience — the structural capacity to absorb and recover from the compounding pressures a breach triggers.

The concentration of breach activity in email systems and network servers — environments structured around identity and authentication — supports a hypothesis with significant strategic implications: modern healthcare attacks are not primarily breaking into systems. They are logging in. Identity governance and access control discipline are not supplementary security measures. They are the primary lever for reducing both breach probability and organizational closure risk.

The Healthcare Breach Survivability Index introduced in this paper offers a framework for structured resilience assessment — one that moves beyond compliance documentation toward

operational preparedness. Future research should refine and validate this model, expand it to cover the full breach universe, and develop its potential as a predictive tool for healthcare leaders, regulators, and investors.

The fundamental reframing that this research demands is this: healthcare cybersecurity breaches are not primarily IT incidents or compliance failures. They are organizational stress tests. The organizations that invest in resilience — not just prevention, not just compliance — are the ones that will continue to serve their patients and communities when the inevitable breach occurs.

The question for every healthcare leader is no longer whether their organization will face a cyber incident. The 320,000 annual complaints, the 36,000 annual small-breach events, and the sustained volume of major breach notifications — totaling nearly one billion individual records exposed across all healthcare entities since mandatory reporting began in 2009 — have answered that question. The question is whether their organization is built to survive one.

About Cybantage

Cybantage works with healthcare providers, business associates, financial services firms and technology organizations to align governance assurance with operational resilience. Our work spans HITRUST interpretation and implementation, SOC 2 scope analysis, identity architecture validation, adversarial modeling, and board-level security reporting for regulated and adjacent industries.

cybantage.com

Appendix A: Summary Statistical Tables

A.1 Study Dataset Summary

Metric	Value
Total organizations in study dataset	1,478
Study period	January 2023 – March 2026
Entity types studied	Healthcare Providers and Business Associates only
Excluded entity types	Health Plans/Payors, Government Entities, Educational Institutions
Organizations still operating	1,016 (68.7%)
Organizations closed / sold	462 (31.3%)
Mean individuals affected (all)	~145,850
Median individuals affected (all)	~7,190
Mean individuals affected (closed organizations)	~40,371
Mean individuals affected (operating organizations)	~193,814
Hacking / IT Incidents (% of dataset)	1,228 (83.1%)
Network Server breach location (% of dataset)	968 (65.5%)
Email breach location (% of dataset)	328 (22.2%)
Business Associate involvement (% of dataset)	458 (31.0%)

A.2 Broader Healthcare Breach Universe (2023 Reference)

Data Point	Approx. Value	Source / Notes
Total HHS/OCR Complaints Received (2023)	~320,000	HHS Office for Civil Rights annual data
Small Breach Log Submissions (<500 individuals, 2023)	~36,000	HHS annual small breach log reporting aggregate
Major Breach Events in Study Dataset (2023 portion)	433	This study — providers and BAs only
Year-over-Year Major Breach Growth (2023–2025)	+20.8%	Study dataset analysis

A.3 Breach Events by Year (Study Dataset)

Year	Events in Study Dataset	Year-over-Year Change
2023	433	Baseline
2024	464	+7.2%
2025	523	+12.7%
2026 (partial)	58	N/A

A.4 Top 10 States by Breach Frequency

State	Breach Events (Study Dataset)
California	197
New York	149
Texas	160
Florida	119
Illinois	96
Pennsylvania	92
Massachusetts	58
Ohio	78
Georgia	57
Michigan	59

A.5 Industry Distribution (Study Dataset)

Industry Category	Organizations	% of Study Dataset
Hospital & Health Care	839	56.8%
Health, Wellness and Fitness	102	6.9%
Mental Health Care	34	2.3%
Individual & Family Services	28	1.9%
Insurance (BAs)	26	1.8%
Consumer Services	26	1.8%

Industry Category	Organizations	% of Study Dataset
Medical Devices	22	1.5%
Alternative Medicine	20	1.4%
Information Technology & Services	19	1.3%
Computer Software	17	1.2%
Other / Not Classified	345	23.3%

A.6 Full HHS/OCR Historical Breach Volume (All Entity Types, 2018–2026)

Year	Major Breach Notifications (All Entities)	Year-over-Year Change
2018	369	-
2019	511	+38.5%
2020	663	+29.7%
2021	715	+7.8%
2022	719	+0.6%
2023	746	+3.8%
2024	742	-0.5%
2025	732	-1.3%
2026 (partial)	77	N/A

Table A.6: Full HHS/OCR Major Breach Notifications by Year, All Entity Types. Source: HHS/OCR Breach Reporting Portal. Note plateau in 2022–2025 following rapid growth in 2019–2020.

Appendix B: HBSI Quick Self-Assessment

The following self-assessment allows healthcare organizations to develop a preliminary HBSI score. Each question should be answered based on honest organizational assessment. Scores are illustrative and intended to identify relative risk areas rather than serve as a definitive security audit. This tool is applicable to organizations of all sizes, including those primarily at risk from small-breach events.

Domain	Question	Scoring Guidance
Organizational Scale	What is your organization's approximate employee count?	1–50: 0 pts | 51–250: 5 pts | 251–1K: 10 pts | 1K+: 20 pts
Identity Governance	Is multi-factor authentication enforced for all remote access and email?	No: 0 pts | Partial: 5 pts | Yes, universally enforced: 15 pts
Identity Governance	Are access rights reviewed and revoked on a regular schedule?	No formal process: 0 pts | Annual review: 5 pts | Quarterly or more: 10 pts
Operational Resilience	Does your organization have a documented and tested incident response plan?	No plan: 0 pts | Documented but untested: 5 pts | Tested annually: 10 pts
Financial Stability	Does your organization have cyber insurance with incident response services included?	No coverage: 0 pts | Basic coverage only: 5 pts | Comprehensive with IR services: 10 pts
Security Leadership	Does your organization have dedicated security leadership (CISO, Security Director)?	None: 0 pts | Part-time or shared: 5 pts | Dedicated full-time: 10 pts
Vendor Oversight	Are all business associates subject to formal security assessments beyond BAA execution?	No: 0 pts | BAAs only: 3 pts | BAAs plus security assessments: 7 pts
Infrastructure	Is sensitive data access monitored and logged with real-time alerting capability?	No: 0 pts | Partial monitoring: 3 pts | Comprehensive coverage: 8 pts

Maximum possible score: 90 points. Interpret results using the HBSI Score Interpretation table in Section 10.3. Organizations scoring below 40 should treat cybersecurity resilience as an immediate organizational priority.

Appendix C: Glossary of Terms

Term	Definition
Business Associate (BA)	An organization that creates, receives, maintains, or transmits protected health information on behalf of a covered entity under HIPAA.
Covered Entity	A healthcare provider, health plan, or healthcare clearinghouse that transmits health information in electronic form under HIPAA.
HBSI	Healthcare Breach Survivability Index: a proposed scoring model for estimating the probability that a healthcare organization survives a major cyber incident.
HIPAA	Health Insurance Portability and Accountability Act: U.S. federal legislation governing the privacy and security of protected health information.
HHS/OCR	U.S. Department of Health and Human Services, Office for Civil Rights: the division responsible for HIPAA enforcement and maintenance of the public breach notification portal.
IAM	Identity and Access Management: the frameworks, processes, and technologies used to manage digital identities and control access to systems and data.
Major Breach	A PHI breach affecting 500 or more individuals, requiring immediate notification to HHS/OCR, the media, and affected individuals under HIPAA.
MFA	Multi-Factor Authentication: a security control requiring users to verify identity through multiple independent mechanisms before gaining access.
PHI	Protected Health Information: individually identifiable health information created or maintained by covered entities and business associates.
Ransomware	Malicious software that encrypts an organization's systems or data and demands payment in exchange for restoration of access.
Resilience Threshold	The organizational scale and maturity level at which survivability probability following a breach increases substantially.
Small Breach	A PHI breach affecting fewer than 500 individuals; organizations are required to log these events and report them to HHS annually.

Healthcare Breach Survivability

A Statistical Analysis of Organizational Outcomes Following Cyber Incidents in Healthcare

Published March 2026 | Cybantage | cybantage.com

Study Population: Healthcare Providers and Business Associates | Excludes Health Plans, Government, and Educational Entities