SEALD HEALTHCARE

The Breach Heard Around the World: Why CFOs, Not Just CISOs, Are Now Driving Healthcare Cybersecurity

February 2026

I started calling Change Healthcare "the breach heard ‘round the world" after the third CFO told me the same thing. Not a CISO. Not a security engineer. A CFO, and the message was identical every time: cybersecurity is now my number one concern because it brought our operations and cash flows to a halt for three months. I heard it shouted from the stage at prominent financial conferences like HFMA. I knew right then that healthcare needed a shift in how to protect PHI.

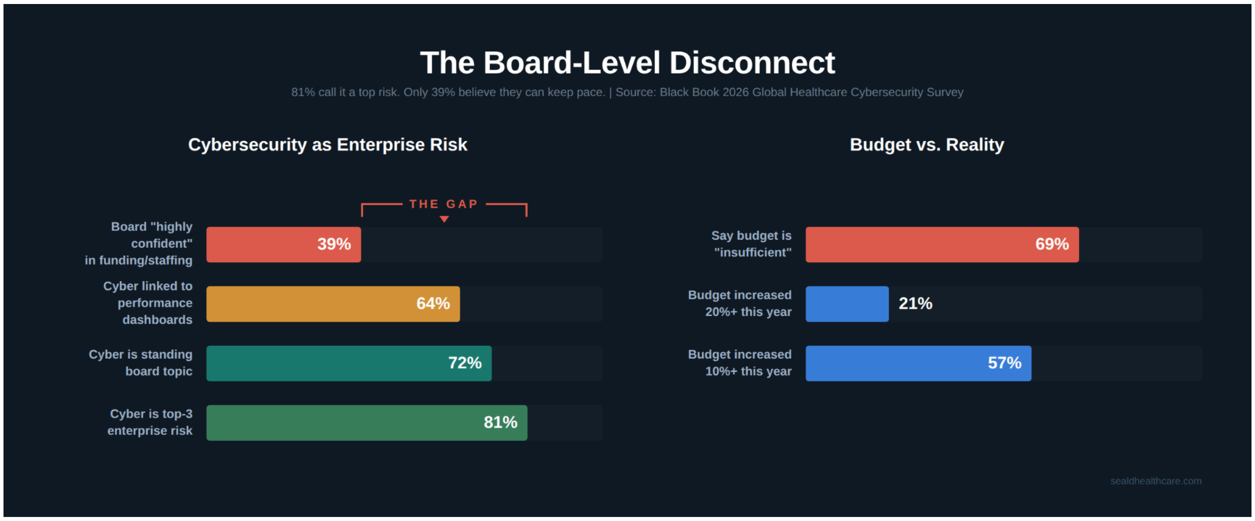
That is a sentence that would not have been spoken five years ago. Cybersecurity was IT's problem. It lived in a budget line somewhere between network infrastructure and help desk support. The board got an annual briefing. Maybe. If something went wrong, the CISO took the heat. The CFO worried about reimbursement rates and days in accounts receivable.

Change Healthcare changed all of that overnight.

When a single ransomware attack on one clearinghouse platform dropped claims processing by 70 to 90 percent across tens of thousands of providers, it stopped being an IT conversation. It became an existential business conversation. Pharmacies could not process prescriptions. Hospitals could not submit claims. Revenue cycles froze. Payroll became uncertain. And the estimated number of individuals affected reached into the hundreds of millions.

The Black Book Research 2026 State of Global Healthcare Cybersecurity survey confirms what those CFOs told me. The shift is real. It is measurable. And it is permanent.

Cybersecurity Is Now an Enterprise Risk



The Board-Level Disconnect

81% call it a top risk. Only 39% believe they can keep pace. | Source: Black Book 2026 Global Healthcare Cybersecurity Survey

Figure 1: The board-level disconnect between risk recognition and funding confidence (Black Book 2026)

Eighty-one percent of healthcare executives now say cybersecurity is a top-three enterprise risk. That is up from 65 percent just three years ago. Seventy-two percent report that cyber risk is a standing topic at every board meeting, not an annual strategy review item. Sixty-four percent have formally linked cybersecurity metrics to organizational performance dashboards.

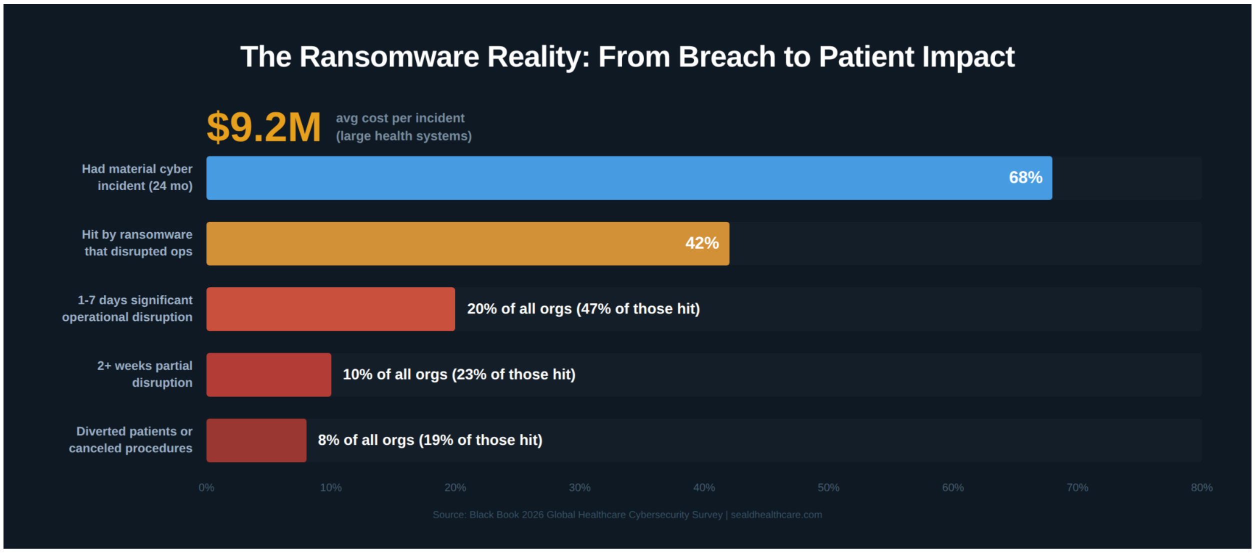
These numbers tell you that the awareness problem is solved. Boards get it. Executives get it. CFOs absolutely get it.

But here is where the data turns alarming.

Only 39 percent of those same boards say they are "highly confident" that their organization's cybersecurity program is adequately funded and staffed to keep pace with threats. That is a 42-point gap between recognizing the risk and believing you can actually manage it. Eighty-one percent call it a top risk. Thirty-nine percent believe they are equipped to handle it.

That gap is where breaches live.

The Ransomware Reality



The Ransomware Reality: From Breach to Patient Impact

Source: Black Book 2026 Global Healthcare Cybersecurity Survey | sealdhealthcare.com

Figure 2: Ransomware impact cascade across healthcare organizations (Black Book 2026)

The scale of what healthcare organizations are facing is staggering. According to Black Book's survey, 68 percent of healthcare organizations experienced at least one material cybersecurity incident in the past 24 months. That is not a phishing email that got caught by a filter. That is a breach, a ransomware event, or a significant outage that disrupted operations.

Forty-two percent report at least one successful ransomware attack that disrupted clinical, claims, or business operations. Of those hit by ransomware, 47 percent experienced one to seven days of significant operational disruption. Twenty-three percent reported more than two weeks of at least partial disruption. Nineteen percent had to divert patients or cancel planned procedures as a direct result.

The average all-in financial impact per major incident is $9.2 million for large health systems and payers. That includes downtime, overtime, recovery costs, lost revenue, and regulatory and legal expenses. These are not projections. These are reported outcomes from the last two years.

Budgets Are Rising. They Are Still Not Enough.

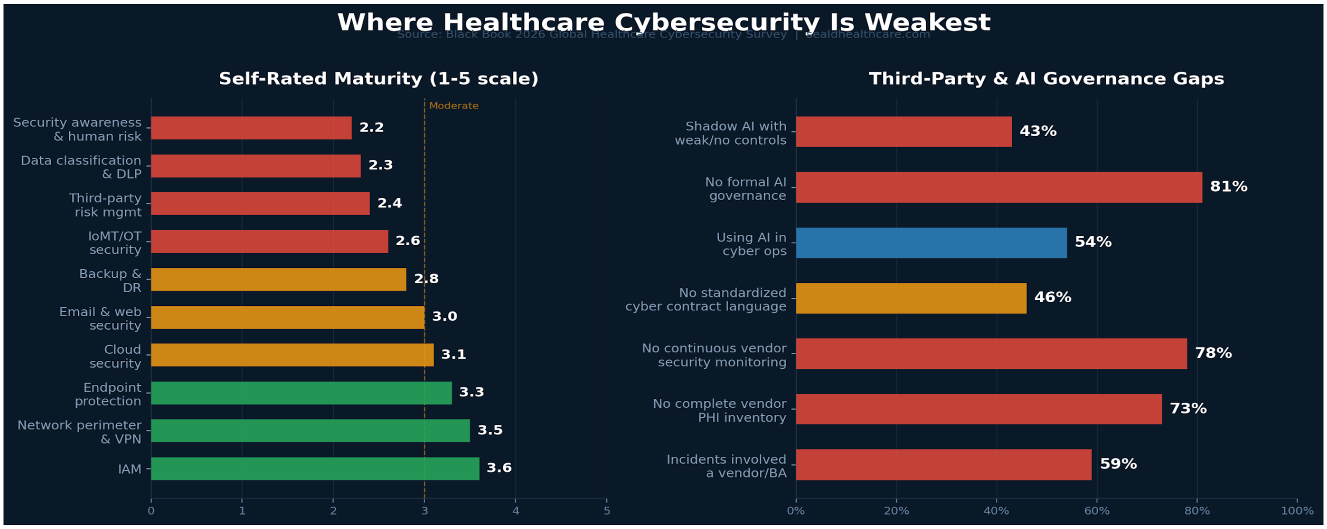
Healthcare organizations are spending more on cybersecurity than ever before. Fifty-seven percent increased their cybersecurity budgets by 10 percent or more in the past year. Twenty-one percent increased by 20 percent or more. Cybersecurity now consumes 6 to 8 percent of total IT spend, up from 4 to 5 percent three years ago.

Despite all of that, 69 percent of respondents say their current budget is insufficient for the level of risk they face. They cite legacy system dependencies, IoMT and OT growth, and expanding regulatory demands as the primary drivers of the gap.

When asked to rank their biggest barriers to cybersecurity improvement, 76 percent selected budget constraints and competing IT priorities. Sixty-one percent cited shortage of skilled cybersecurity professionals. Fifty-seven percent pointed to legacy technologies and technical debt.

The money is moving in the right direction. It is not moving fast enough.

Where Healthcare Is Weakest


Where Healthcare Cybersecurity Is Weakest

Source: Black Book 2026 Global Healthcare Cybersecurity Survey | sealdhealthcare.com

Figure 3: Cybersecurity maturity self-assessment and third-party/AI governance gaps (Black Book 2026)

The Black Book survey asked organizations to self-rate their maturity across key cybersecurity domains on a 5-point scale. The results reveal exactly where the industry is most exposed.

The strongest domains are identity and access management at 3.6, network perimeter controls at 3.5, and endpoint protection at 3.3. These are the areas where healthcare has invested the most over the past decade.

The weakest domains tell a different story. Data classification and data-loss prevention scored 2.3 out of 5. Third-party and vendor risk management scored 2.4. IoMT and OT security scored 2.6. Security awareness and human risk management came in at 2.2.

Read that again. The two lowest-scoring domains in the entire survey are data protection and human risk management. Healthcare organizations rate themselves strongest at building perimeters and weakest at protecting the data those perimeters are supposed to guard.

That inversion explains why breaches keep happening even as budgets increase. The money goes to the perimeter. The data sits exposed behind it.

The Third-Party Blind Spot

If the maturity data is concerning, the third-party risk data is alarming.

Fifty-nine percent of respondents say that half or more of their recent high-impact incidents involved a vendor, business associate, or technology intermediary. Only 27 percent have a complete and current inventory of all vendors with access to PHI or critical systems. Just 22 percent conduct continuous security monitoring of their most critical third parties. And 46 percent do not have standardized contract language requiring specific cybersecurity controls, notification timelines, or independent attestations.

Change Healthcare was the proof of concept for this risk. One platform compromised. Thousands of organizations affected. Months of disruption. And most of those organizations had no visibility into the security posture of the platform they depended on for revenue.

Seventy-one percent of organizations now list strengthening third-party risk management as a top-three governance priority for 2026 and 2027. That is the right priority. But strengthening governance over vendors you cannot control only goes so far. At some point, the question becomes: what happens to the data itself when a vendor is compromised?

If the answer is that the data is sitting in plaintext on that vendor's systems, governance did not protect it. The vendor's security posture was the only thing standing between that data and an attacker. And the attacker won.

Shadow AI: The Threat Nobody Budgeted For

The Black Book data on AI governance should concern every healthcare leader reading this.

Fifty-four percent of organizations are already using AI or machine learning tools in cybersecurity operations. Thirty-seven percent have clinical or operational AI in production. But only 19 percent have a formal AI risk and governance framework that covers both security and clinical use cases.

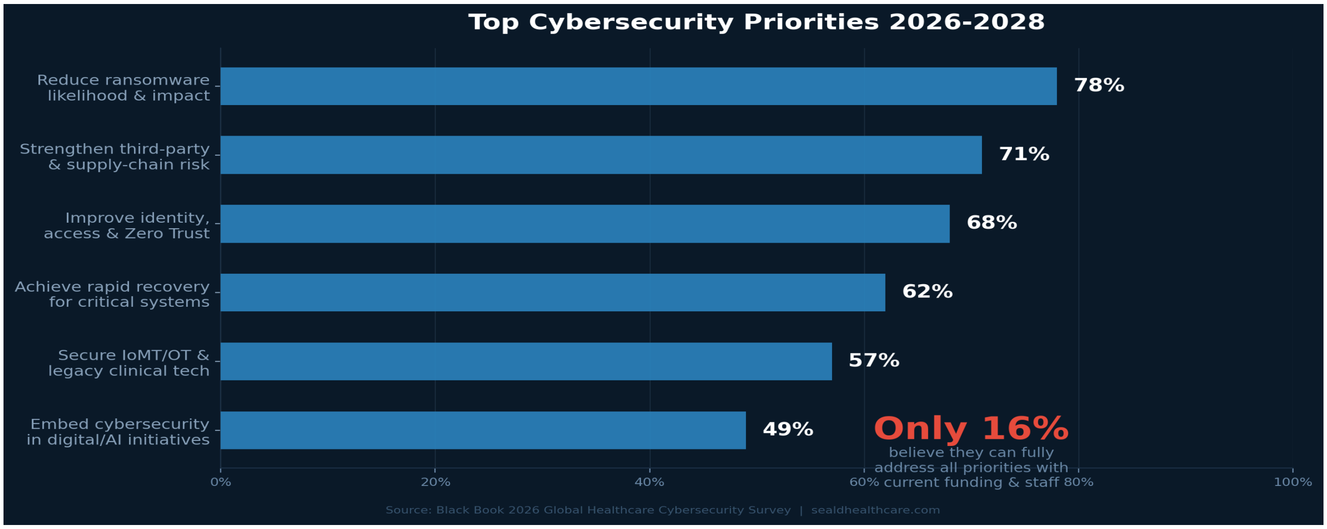
Forty-three percent acknowledge shadow AI use, staff copying data into public tools, and rate their controls over that activity as "weak" or "nonexistent."

When asked about their top AI-related cybersecurity concerns, 68 percent cited unmonitored exposure of PHI to public or external AI tools. Fifty-seven percent cited AI-generated phishing and social engineering. Forty-four percent cited integrity risks to AI models and training data.

Shadow AI is the third-party risk problem on a faster timeline. Every clinician, administrator, and billing coordinator with access to a browser can upload patient data into an external AI tool. They are not doing it maliciously. They are doing it to work faster. But the data leaves the organization's control the moment it enters that tool. It cannot be retrieved. It cannot be deleted. It cannot be audited.

This is a data protection problem, not a policy problem. Policies tell people what not to do. Data-layer encryption ensures that even when they do it, the data remains protected.

The Priorities Everyone Agrees On



Source: Black Book 2026 Global Healthcare Cybersecurity Survey | sealdhealthcare.com

Figure 4: Top cybersecurity priorities 2026-2028, with only 16% able to fully fund them (Black Book 2026)

When Black Book asked healthcare leaders to select their top cybersecurity priorities for 2026 through 2028, the responses were remarkably consistent.

Seventy-eight percent selected reducing the likelihood and impact of ransomware and extortion attacks. Seventy-one percent selected strengthening third-party and supply-chain risk programs. Sixty-eight percent selected improving identity, access, and Zero Trust maturity. Sixty-two percent selected achieving rapid recovery for critical clinical and revenue systems.

But here is the number that should keep every board member awake. Only 16 percent of organizations believe they can fully address all of their stated priorities with current funding and staffing. The rest are being forced to make trade-offs.

Those trade-offs are where the risk concentrates. When you cannot fund everything, you fund what feels most urgent. That usually means more perimeter tools, more endpoint protection, more identity controls. The data layer gets deferred. Third-party risk gets a policy update instead of a technical solution. Shadow AI gets a memo.

Meanwhile, attackers are not making trade-offs. They are targeting the weakest domains: data protection, third-party access, and human error. The exact places where healthcare scores lowest.

Protecting Data When Everything Else Fails

The pattern across every finding in the Black Book survey points to the same conclusion. Healthcare has invested heavily in perimeter and identity controls. Those investments are necessary. They are not sufficient.

When 68 percent of organizations have already experienced a material incident, the perimeter has been breached. When 59 percent of high-impact incidents involve a third party, the vendor's perimeter has been breached too. When 43 percent of organizations have uncontrolled shadow AI use, data is leaving the perimeter entirely.

The question is no longer how to stop every breach. It is how to ensure that when a breach happens, the data is useless to the attacker.

That is what record-level encryption with persistent access policies is built to do. When PHI is encrypted at the source, before it enters any system, with access policies that travel with the data and are enforced at the point of decryption, the calculus changes. A compromised vendor cannot read data they were never authorized to decrypt. A shadow AI tool receives ciphertext instead of patient records. A ransomware attacker who exfiltrates encrypted data has nothing to sell, nothing to exploit, and nothing to report.

Under HIPAA's Breach Notification Rule, encrypted data that meets NIST standards and is compromised does not trigger breach notification obligations. That is not a technicality. For an industry where the average major incident costs $9.2 million and 19 percent of ransomware victims are diverting patients, it is a strategic imperative.

What the CFO Needs to Hear

The CFOs who called Change Healthcare the moment everything changed were right. Cybersecurity is a financial risk, an operational risk, and a patient safety risk simultaneously. It belongs on the performance dashboard alongside days in AR, operating margin, and patient satisfaction.

But the conversation cannot stop at awareness. Eighty-one percent awareness with 39 percent confidence in funding is not progress. It is a gap that attackers will exploit.

Here is what every healthcare CFO, CEO, and board member should be asking right now.

When our perimeter fails, and the data says it will, what protects the data itself? If the answer is "nothing," you have the most expensive vulnerability in your organization. If the answer is record-level encryption with persistent access policies and tamper-evident audit trails, you have a defense that works even when everything else does not.

The breach heard around the world already happened. The question is whether your organization is still building its defenses around the assumption that it will not happen to you.

Eighty-one percent of executives say cybersecurity is a top-three risk. Only 16 percent believe they can fully address it. The data could not be clearer. Act accordingly.

About Seald Healthcare — Seald Healthcare secures PHI at the data layer. Our SDKs and APIs encrypt data at the record level with persistent access policies and an AI policy engine that lets teams write governance rules in plain English. Every access event is logged in tamper-evident audit trails. No intermediary, including Seald Healthcare, can access the plaintext data. Works with EHRs, patient portals, telehealth, messaging, file sharing, and custom applications. Complements AWS, Google Cloud, and Azure environments. Learn more at sealdhealthcare.com.

Sources

Black Book Research, *State of Global Healthcare Cybersecurity 2026: Resource Manual & Playbook*, 2026.

Fortified Health Security, *2026 Horizon Report: The State of Cybersecurity in Healthcare*, 2026.

U.S. Department of Health and Human Services, Office for Civil Rights, Breach Portal (breaches affecting 500 or more individuals), https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

UnitedHealth Group / Change Healthcare incident disclosures and SEC filings, 2024–2025.

HIPAA Journal, *Healthcare Data Breach Statistics*, https://www.hipaajournal.com/healthcare-data-breach-statistics/

IBM Security, *Cost of a Data Breach Report 2025*, 2025.

Health-ISAC, *2026 Global Health Sector Threat Landscape Report*, 2026.

HIPAA Breach Notification Rule, 45 CFR §§ 164.400–414; HHS Guidance on encryption safe harbor under §164.402(2).

NIST Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices*; NIST SP 800-175B, *Guideline for Using Cryptographic Standards in the Federal Government*.

Healthcare and Public Health Sector Coordinating Council (HSCC), *Model Contract Language for MedTech Cybersecurity (MC2 v2)*, November 2025.

CMS Interoperability and Prior Authorization Final Rule (CMS-0057-F), effective January 2026.

HHS/OCR Notice of Proposed Rulemaking, *HIPAA Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information*, January 6, 2025.

ECRI, *Top 10 Health Technology Hazards for 2026*, 2025.

JAMA Network Open, Seh et al., *Healthcare Data Breaches: Insights and Implications*, 2020 (with updated OCR data through 2024).

Fortified Health Security, *2025 Healthcare Cybersecurity Survey* (U.S. healthcare organizations, referenced in 2026 Horizon Report).