Fortified HEALTH SECURITY

Fortifying Healthcare's Bottom Line

Cybersecurity Priorities for CFOs

By Greg Breetz // Chief Financial Officer, Fortified Health Security

INTRODUCTION

Cyber Risk Is a Strategic Financial Issue in Healthcare

Cyber risk has become a **patient safety, financial, and operational crisis.**

Cybercrime has become so common, we've all been victims at this point. In healthcare the stakes go far beyond stolen data or financial loss. When critical systems are locked or disabled, the result isn't just downtime, it's delayed diagnostics, canceled procedures, and risks to patient safety.

At the same time, the financial impact is staggering.

- In 2024, the cost of a breach averaged $10.1 million per breach.
- By mid-2025, the U.S. Department of Health and Human Services Office for Civil Right (OCR) reports show 311 breach incidents already logged (affecting 500+ individuals), impacting **nearly 1.9 million people in May 2025 alone.**
- The Change Healthcare ransomware attack alone disrupted care nationwide, exposed **more** than 190 million records, and caused losses of **$100 million per day.**
- Smaller providers often cannot absorb the blow, with some closing permanently after a single "devastating" attack.

For CFOs, the message is clear: cybersecurity is both a financial safeguard and a patient safety imperative. This guide outlines the threat landscape, regulatory shifts, and action steps financial leaders must take heading into 2026 to protect margins and, more importantly, protect patients.

In 2024, more than

275 Million

records were exposed

$10.1 Million

average cost **per breach**

The HIPAA Journal and *Recorded Future News*

Cybersecurity is both a **financial safeguard** and a patient **safety imperative.**

The Threat Landscape Healthcare CFOs Must Track

THREAT VECTOR	HEALTHCARE-SPECIFIC INSIGHTS *(2024–Mid 2025)*
Mega Breaches & Ransomware	The Change Healthcare breach (2024) remains the largest in history, with more than 190M records compromised. Ransom demands across industries averaged $5.2M in 2024, and healthcare is consistently among the highest-targeted sectors.
Phishing & Social Engineering	In healthcare, phishing-related incidents average $9.77M per breach.
Scale of Records Breached	275M records exposed in 2024; another 1.9M impacted in May 2025 ALONE. (and that's what's just been reported to HHS)
Long Dwell Times	Breaches take 279 days on average to contain. That's five weeks longer than other industries, inflating downtime and remediation costs.
Regulatory & Legal Exposure	As of April 2025, OCR was investigating 554 hacking-related breaches, most involving providers. In 2025, we're seeing steeper penalties from $75k to $3M+ in single cases (e.g., $600K settlement with PIH Health over risk assessment gaps.) For reference, in 2023, the total of all enforcement for the year was just over $4M.
Cost Trends	Healthcare remains the most expensive sector: $10.1M average cost per breach in the U.S., up more than 50% since 2020.

Evolving Regulatory Landscape

For CFOs, compliance gaps now translate directly into financial liability.

- **OCR Enforcement:** Hundreds of active investigations confirm heightened scrutiny around risk assessments, vendor oversight, and safeguards.
- **HIPAA Security Rule NPRM (Jan 2025):** Proposes requirements for asset inventories, MFA, encryption, incident planning, vendor oversight, and segmentation.
- **Healthcare Cybersecurity Act of 2025:** Expands federal coordination, intelligence sharing, and free technical assistance.

Fortified CFO Action Plan for 2026

1. **Map Cyber Risk to Financial Statements:** Quantify downtime's impact on revenue and cash flow. A 48-hour outage can reduce EBITDA measurably.
2. **Embed Finance in Incident Response:** CFOs must practice sourcing liquidity, coordinating insurer payouts, and managing emergency vendor payments during tabletop drills.
3. **Create a Cyber IR Reserve:** Allocate 1–2% of operating expenses for breach response, OCR penalties, and uninsured costs.
4. **Tighten Vendor Oversight:** With dozens of vendor-related breaches under OCR investigation, demand SOC 2/ISO 27001 attestations, breach-notification clauses, and proof of cyber insurance.
5. **Use Cyber Insurance Strategically:** Premiums remain high but stabilizing. Secure business interruption coverage tailored to healthcare billing and claims risks.
6. **Invest in AI + Human Defenses:** AI can flag anomalies and fraudulent invoices, but training remains essential to stop phishing and BEC schemes targeting finance staff.
7. **Budget Smarter for Security:**
   - **CapEx:** Zero-trust, IAM, network segmentation.
   - **OpEx:** Continuous pen testing, awareness training, threat hunting, crisis PR.
   - **ROI Framing:** A $1M security upgrade could mitigate $750K/year in expected fraud or downtime losses.
   - **Partner With the Right Vendors:** Find a company who supports your specific needs.
   - **Sign Multi-Year Contracts:** A multi-deal contract with the right vendor is the best way to get a deal on services. One-year deals aren't enough to establish a partnership and see value.

Board & Investor Communication

- **Frame Quantitatively:** "A 72-hour outage could reduce EBITDA by X%."
- **Show Metrics:** Report mean time to detect, recover, and restore billing.
- **Benchmark Spend:** Compare security investments against industry averages and insurer expectations.
- **Roadmap Clarity:** Make a detailed plan to move security up and to the right.

Looking Ahead: CFO + CISO Alignment by 2026

- **AI Arms Race:** Threat actors deploy AI for phishing, deepfakes, and ransomware against finance systems and all employees.
- **Regulatory Cadence:** Expect quarterly cyber attestations demanded by auditors and insurers.
- **Joint Governance:** CFOs and CISOs will increasingly share accountability for resilience, capital allocation, and compliance.

Key CFO Takeaways for 2026

Cyber incidents have proven themselves to be both a patient safety and a financial crisis. A single attack can drain millions from operating budgets while simultaneously delaying treatments, diagnostics, and procedures.

- **Financial Disruption:** Beyond breach costs, outages cut into cash flow, slow reimbursements, and threaten long-term solvency, especially for smaller providers.
- **Patient Impact:** Healthcare systems attacked by cybercriminals result in direct care delays. When scheduling, billing, or imaging platforms go dark, patients feel the consequences immediately.
- **Shared Accountability:** CFOs can no longer treat cybersecurity as discretionary IT spend. Alignment with CISOs ensures that budgets reflect both resilience and safety.
- **Action Mandate:** Map cyber risk to financial statements, embed finance in incident response, and invest in both technology and training. These are not optional. They are critical commitments to organizational stability and patient care.

For financial leaders, the takeaway is clear: protecting margins and protecting patients are inseparable, and both should be the center of every 2026 strategy.

> Protecting **margins** and protecting **patients** are ***inseparable***

FortifiedHealthSecurity.com