ArxNimbus ▪ CASE STUDY ▪ NON-PROFIT HEALTH

Two Debts, Priced: Turning a $386.8M Blind Spot Into a Board-Funded Plan

How a $1.46B health system put a dollar figure on its technology debt and its security debt, then cut exposure 27% in six months.

$386.8M	1/3	75%	27%
Total exposure uncovered through actuarial mapping	Of the technology environment on outdated, high-risk hardware	Below industry-benchmark security spend	Cut in risk exposure in six months

ORGANIZATION

A $1.46B non-profit health system

ENVIRONMENT

4-person security team

1/3 of the estate on outdated, high-risk hardware

PATIENT RECORDS

11M

The Bottom Line

Neither debt was a maintenance problem. Both were unpriced liabilities.

Aging hardware (technology debt) and a security budget 75% below benchmark (security debt) had been treated as IT housekeeping. Once leadership could see what both were worth in dollars, the board funded a dollar-ranked plan to pay them down:

proof that a resource-strapped team can protect what matters once leadership can see the real number.

SITUATION

A $1.46B non-profit health system was carrying two kinds of debt it couldn't see in dollars: security debt from years of underinvestment, and technology debt in an estate that had aged past what a small team could defend.

- **Severely underfunded:** a $1.48M security budget, 0.10% of revenue, sat 75% below the 0.40–0.64% industry benchmark.
- **Critically understaffed:** just 4 security professionals covered an organization where peers average 5x the headcount.
- **Technology debt:** a third of the technology environment still ran on outdated, high-risk hardware.
- **Underinsured:** commercial cyber coverage was roughly 5% of the organization's real exposure.
- **Massive exposure at stake:** 11 million patient records sat behind a four-person team.

SOLUTION

ArxNimbus built a baseline risk profile from 47,000 threat-vulnerability pairings, then modeled seven digital-twin scenarios, from budget to hardware, showing exactly which investments cut the most risk per dollar. For the first time, both debts sat on the same dollar scale, so the board could weigh a hardware refresh against new hires or more coverage.

IMPACT

- **27% less risk in six months:** total exposure fell 27% against the original baseline.
- **Technology debt retired:** $3M dedicated to retiring technology debt, with board approval of 100% of the needed capital within weeks.
- **Budget tripled:** an immediate 3x increase moved spend toward industry-benchmark levels.
- **Multi-year commitment:** the board committed to a multi-year plan to right-size budget and staffing.
- **Insurance doubled:** coverage doubled immediately, with a plan to reach 4x over several years.

WHY THIS MATTERS NOW

When PHP2Shell hit in October 2026, Qualys found 71% of PHP installations across its customer base running end-of-life branches that will never get an official patch. For most enterprises the choice became upgrade, isolate or retire, each with a different cost. **This health system had already priced that choice.**

ArxNimbus
Secure the business.

Cyber and AI exposure are already on the balance sheet. The question is whether leadership can see the number.

Controls matter. But strategy changes when exposure is translated into dollars your CFO, board, cyber insurers, and governance teams can act on.

ArxNimbus helps organizations move beyond static scorecards and subjective color-coded scores to a prioritized action plan, quantifying cyber and AI exposure as defensible financial intelligence.

See what your own exposure number would be: Request an Executive Briefing at arxnimbus.com

It's not magic. It's math. **#ProtectYourEBITDA**

©2026 ArxNimbus LLC · arxnimbus.com · info@arxnimbus.com