A $6.87B Breach. Predicted 10 Months Early.

How the ArxNimbus Thrivaca™ Engine projected the largest confirmed cyber loss in U.S. history — 310 days before UnitedHealth Group confirmed it.

$7.87B	$6.872B	8%
Thrivaca™ projected loss exposure calculated 4/17/23 — 10 months BEFORE the breach	Confirmed actual loss per Healthcare Fin. Mgmt Assn.	Variance between predicted and confirmed loss

ORGANIZATION

UnitedHealth Group / Change Healthcare

BREACH DATE

February 2024

DATA COMPROMISED

6TB of Protected Health Data

The Bottom Line

Thrivaca™ didn't assess this risk after the fact.
It quantified the exposure ten months before the breach — proof that actuarial cyber risk quantification isn't theoretical.
It's predictive and precise to act on.

THE BREACH

In February 2024, a ransomware attack on Change Healthcare became the largest confirmed cyber loss in U.S. history.

- **A basic control gap:** the breach traced back to a server without multi-factor authentication (MFA).
- **A costly ransom:** UnitedHealth Group paid $22M in ransom for the stolen data.
- **A second extortion attempt:** the same actors resurfaced under a new ransomware name for more payment.
- **National exposure:** Senate testimony confirmed U.S. military personnel were among those affected.

THE PREDICTION

On 4/17/23 — 10 months before the breach— ArxNimbus profiled UnitedHealth Group for a cyber insurance analysis. Using its NIST-approved actuarial methodology, the model projected $7.87B in loss exposure, without knowledge of the attack to come.

THE PROOF

- **Confirmed within 8%:** HFMA now puts the total loss at $6.872B vs. Thrivaca's $7.87B projection.
- **Ten months of runway:** the projection existed 310 days before the breach was even confirmed.
- **Not a lucky guess:** the result came from a patented, NIST-reviewed actuarial data engine.
- **The cost lands on everyone:** breaches like this raise premiums and deductibles industry-wide.

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 with a complimentary exposure-quantification session.

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