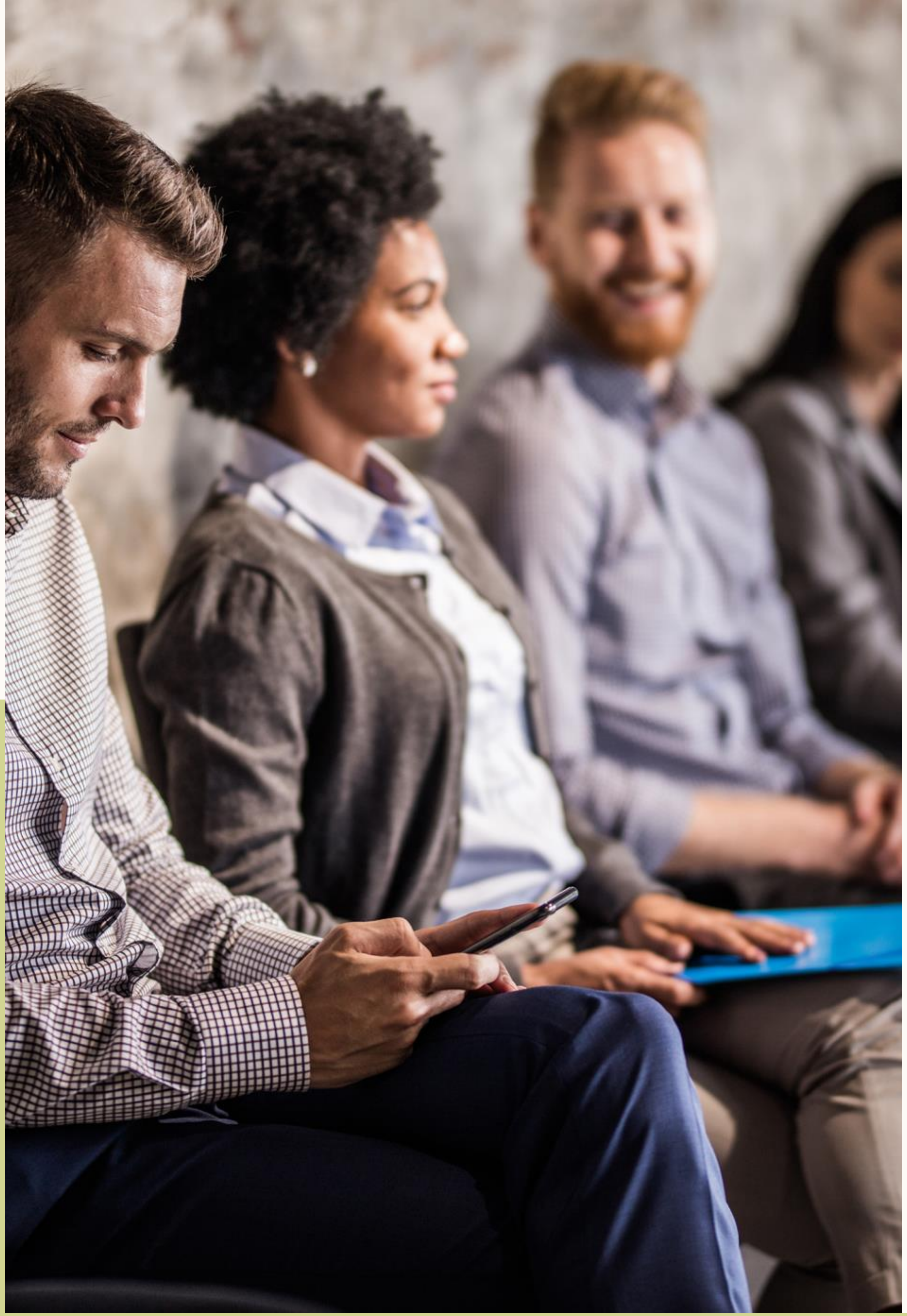
STRATEGIES TO COMBAT CYBER SECURITY THREATS IN HEALTHCARE

Chris Milligan, Chief Revenue Officer

AGENDA

- Overview / Objective
- What Happened & Why
- Vendor Consolidation Pros & Cons
- Building Your Strategy
- Questions



OVERVIEW

PROVIDE A THIRD-PARTY PERSPECTIVE OF WHAT REALLY HAPPENED WITH THE CHANGE HEALTHCARE CYBER ATTACK AND WHAT WE AS PROVIDERS CAN DO TO MINIMIZE FUTURE RISK.

WHAT HAPPENED & WHY

WHAT REALLY HAPPENED

- **February 21, 2024** – Change Healthcare (CH) shuts down entire network
- **February 29, 2024** – CH confirms attack was ransomware
- **March 4, 2024** – UnitedHealthcare pays $22M in ransom
- **March 13, 2024** – logistical & support issues remain, remediation begins
- **March 28, 2024** – U.S. government posts a $10M bounty
- **April 15, 2024** – A second ransom is made, using the same data
- **April 22, 20124** – United Healthcare publicly comments on the size of the breach
- **May 1, 2024** – CEO testifies cyber security was “not up to standard”
- **June 20, 2024** – UHC notifies affected hospitals
- **July 29, 2024** – CH notifies patients of potential data breach
- **October 24, 2024** – UHC confirms over 100 million people affected
- **December 2025** – UHC CEO is assassinated
- **March 2025** – CH updates impact to 190M people and over $3B

WHY IT HAPPENED

1. Sub-par cyber security in place (last review was 2005)
2. Federal Government did not require cyber security review for CH/UHC merger (October 2022)
3. Merger made CH/UHC largest "depository of patient information"
4. At the time, CH/UHC was in over 85% of healthcare providers
5. Stockholders didn't prioritize investing in cyber security
6. Ransomware criminals prioritized healthcare providers….***Why?***
7. Industry-wide issues, not just a CH issues; bottom line, ***Could Have Happened To Anyone***
8. Providers realized they had "all their eggs in one basket"

VENDOR CONSOLIDATION

PROS & CONS

PROS

- Less vendors to manage
- Streamline process
- Less data files / transfers
- More volume = better rate?
- Less diversification
- Stronger contract terms

CONS

- More reliant on one vendor
- Complicated process
- More data files to manage
- Higher cost?
- Diversification
- Weaker contract terms

There isn’t a single "best practice" for every provider. It's essential to prioritize what's most important and develop a vendor strategy tailored to your specific needs.

BUILDING YOUR STRATEGY

- Determine your risk / tolerance
- Cost / performance balance
- Stronger contract terms / insurance levels
- IT / security assessment for all vendors
- Regular performance / contract reviews
- Avoid focusing only on vendors!
- Internal IT / security assessment is critical

QUESTIONS

THANK YOU

Chris Milligan
216-965-2718
cmilligan@net-revenue.com