Selling IT Security to the Health Industry:

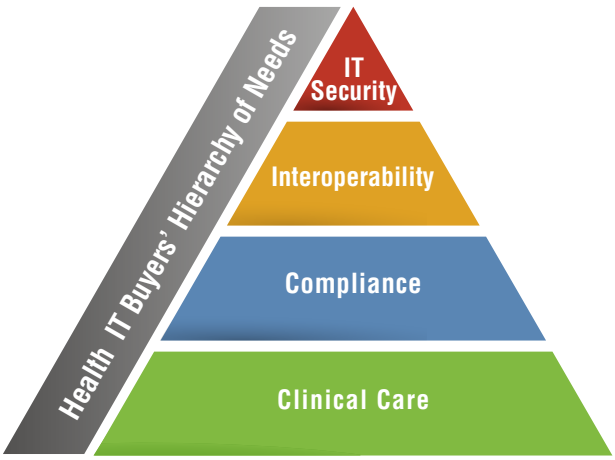
The Anthem Hack Changes Nothing

FEBRUARY 2015

Christopher Meissner, Senior Associate
Chris Haley, Consultant

If there were ever a time for the healthcare industry to rally for stronger IT security, it should be in the aftermath of the industry's largest-ever information breach at Anthem. In other sectors where privacy and confidentiality are foundational, the reported involvement of Chinese state hackers might trigger comprehensive reform so such a heist could never happen again. Not so for healthcare.

Patient care always comes first, and IT security has historically been an afterthought. The healthcare industry typically makes purchases that will satisfy the minimum safeguards required for regulatory compliance. Sadly for patients and providers alike, the status quo will persist unless security providers – from vendors to integrators – can better understand this unique customer environment to realize adoption of much-needed security solutions.



Effectively addressing security means finding ways to reconcile the core missions of healthcare and IT security professionals. That requires grasping three key challenges when selling to the health industry:

> **"Doctors will buy new products, not with security but with medical advances in mind, if it offers them new ways to treat patients better, more efficiently, and at lower cost."** – *Security Manager at a Top 10 U.S. Non-Profit Health System*

1) **Clinical Care Needs Trump Security**: Leaders in hospital C-suites prioritize care delivery above all else. Solutions that deliver patient care better, faster, or at lower cost resonate with them, even if security suffers in the process. Simply put: additional protection cannot impede patient care.

- *Demonstrate Mission Understanding*: To be successful, security providers should recognize the overriding patient focus, and position their products in this context.
- *Make Stronger Security Easy*: Solutions must make security painless for healthcare providers by avoiding unnecessary complexity and ensuring it in no way interferes with care delivery.

2) **Regulation Drives Buyers to Compliance**: HIPAA, FDA, and other regulations create strict requirements for hospitals and solution providers alike. Security teams at health organizations routinely dedicate scarce resources to compliance-focused activities, leaving little to spend on more rigorous protection.

- *Offer Smarter Approaches to Compliance Challenges*: Security companies can begin by understanding and recasting the compliance challenge faced by customers.
- *Price Competitively*: Price-points need to be competitive with traditional compliance solutions. Health organizations rarely pay a premium for security.
- *Have Patience*: The slow pace of software adoption drives much longer sales channels in healthcare than in other industries. Establishing long-term, trust-based relationships with customers is likely to be more successful than transactional business-development efforts.

3) **Uniquely Complex and Dynamic IT Architectures**: Hospitals increasingly have hundreds of disparate devices connecting to electronic health record databases, each of which introduces new vulnerabilities to the system. This challenge is exacerbated by the 24/7/365 uptime requirements that are ubiquitous in the industry.

- *Capture Opportunities from Health IT Upgrades*: ACA and MU continue to create new opportunities in healthcare. Upgrades to underlying IT are an optimal time to sell security, especially if offerings can be seamlessly integrated into the process.
- *Dedicate Health Sales Leads*: Security providers should create dedicated sales leads who understand the unique challenges in the health IT environment. Generalists will rarely suffice.
- *Focus on Channel Strategies*: Alternative distribution channels or partnerships with EHR vendors and device manufacturers – in lieu of direct approaches – can also help drive sales.

Barriers to robust healthcare IT security are significant, but vendors must learn to overcome them because the next big breach is never far off. In the wake of the Anthem breach, the security industry has an opportunity to take the initiative in protecting prospective healthcare customers so they can focus on their core mission: delivering clinical care.

Chris Meissner leads Avascent's IT Security practice, specializing in growth strategies for technology companies operating across customer verticals. Chris has nearly a decade of experience analyzing voice of customer demand, developing sales channel strategies and positioning vendors, integrators and their financial sponsors for growth.

Chris Haley is a Consultant at Avascent, where he provides strategy and market research in the healthcare, defense, and information technology industries. Prior to joining Avascent, Chris was a Project Manager and technology architect for Cerner Corporation, where he led delivery of health IT solutions to hospitals across the US and Canada. He also served four years in the United States Marine Corps Reserves as a tactical communications NCO.