Intraprise HEALTH
A Health Catalyst Company

Frederick Health Customer Q&A

Importance of Organizational Alignment and Clear Communication in Cyber Security

Organizational Cybersecurity Challenges

Like many healthcare organizations, Frederick Health faced challenges in securing sufficient funding to bolster its cybersecurity infrastructure, crucial for safeguarding patient information and mitigating cyber threats. In this customer profile, Frederick Health's CIO shares insights into these challenges and the strategies they used to address them.

Key Concerns:

- **Sustaining current programs and updating their technology with limited resources**
- **Escalating cybersecurity costs and management alignment made securing adequate funding challenging without affecting the organization's mission**
- **Demonstrating the value of a robust cybersecurity ecosystem to secure essential resources**
- **Selecting and working with a proven cybersecurity partner who has deep understanding of healthcare who can identify coverage gaps**

Q&A with Jackie Rice, Vice President & Chief Information Officer from Frederick Health

Q: Is the amplification of threats a unique concern when securing funding for resources and technology needed to protect data and ward off attacks?

A: Frederick Health is not alone in this challenge. We found it imperative to advocate for investments in cybersecurity. Our approach involved educating both the board and leadership about the evolving threats landscape, ensuring they grasped the significance of prioritizing these investments.

About Frederick Health

Frederick Health offers comprehensive healthcare services to Frederick County, MD residents through its extensive network:

- Founded in 1902
- 3,000+ employees, including 100 providers across 17 specialties
- Network includes – Frederick Health Medical Group, Health Employer Solutions, Home Care, Health Hospice, ambulatory care locations, a standalone cancer institute, two urgent care centers and Frederick Health Village

Cybersecurity Products in Use:

BluePrint Protect™ Integrated Risk Manager and NIST Cybersecurity Framework

Q: What is the role of Healthcare Leadership and how do you create cybersecurity advocates?

A: Leadership/board members tend to understand cybersecurity at a basic level and have a vested interest due to patient risks, liability concerns, and revenue loss, business risks (i.e. loss of patients due to a breach, lawsuits.). What prevents the right level of investment tend to be:

1. Patient care priorities
2. Complexity of cybersecurity with its own language, evolving threats, and constantly shifting best practices
3. Competing demands and limited resources We recognized the need to better educate our team members to make informed decisions about our cybersecurity investments. To address this, we brought in third-party industry experts to educate leadership and board members. Additionally, we recommended adding a board member with a cybersecurity background to enhance the organization's overall understanding of this critical area.

Q: Can you provide a little more background on the decision to adopt and use the NIST framework?

A: We adopted the NIST framework in 2022 and other solutions from Intraprise Health solutions to protect our infrastructure and data. This move signaled to patients, partners, and regulators our commitment to strong cybersecurity practices. In addition to helping build trust, credibility and reduce the likelihood of a successful breach and financial, reputational, and patient safety risks.

We selected the NIST structure because it is cost-effective and flexible to adapt to a constantly changing cybersecurity landscape.

Q: What strategies did you employ to garner support around increasing the investment in cybersecurity tools and platforms within the healthcare organization?

A: We focused on securing leadership and board alignment to support our investment by highlighting the potential repercussions of breaches on patient safety, reputation, liability, finances, operational disruptions, regulatory, and compliance, such as HIPAA. We underscored the cost-saving advantages of proactive cybersecurity investment. In addition, we also:

- Enlisted the expertise of the **American Hospital Association** group to present on the current state of cybersecurity
- Added a board member from our local community who has cybersecurity experience
- Leverage **Intraprise Health** to deliver quarterly cybersecurity market updates

Now is the time. Connect with Intraprise Health today to begin your journey to a more secure future.

Schedule a Product Demo

IntrapriseHealth.com

Securing Alignment For Cybersecurity Investments

Shared Cost-Savings Advantages of Protective Cybersecurity

Added Board Member with Cybersecurity Experience

Purchased a Cost Effective Solution Recommended by Intraprise Health

Educated Board and Leadership Team

Market Data & References

- 51% of healthcare organizations plan to invest more in cybersecurity (vs. 56% across all industries) – *Security Magazine*
- BankInfoSecurity survey reported that only 6% of IT budgets are dedicated to cybersecurity – *Becker's Health IT, Statistia, Tausight*
- 88% of boards of directors view cybersecurity as a business risk – *Gartner*
- Healthcare makes up 23% of lawsuits due to data breaches – *Healthcare Finance*
- 53% of connected devices in healthcare organizations have known critical vulnerabilities – *ht-medicaldevices.com*

About Intraprise Health, a Health Catalyst Company

Intraprise Health, healthcare's leading compliance and cybersecurity organization, provides holistic visualization of your compliance and security posture. Our comprehensive services, backed by automation, rapidly integrate in native environments, yielding a comprehensive view of risk – spanning adherence to compliance frameworks, cybersecurity vulnerabilities, and third-party risk. Eliminate blind spots with Intraprise — the fifth HITRUST assessor since 2011.

©2025 Intraprise Health.