CASE STUDY

Intraprise HEALTH

A Healthcare CISO's Journey through NIST CSF Adoption & Implementation

An interview with: Devin Shirley, C-CISO, CISSP, CRISC Chief Information Security Officer, Arkansas Blue Cross Blue Shield

Question & Answer

Q: Why should an organization choose the NIST CSF?

A: There are many frameworks out there. Regulatory requirements can be a major reason, but organizations may also have third-party requirements. Many contracts focus on NIST. While you may have implemented the HITRUST CSF, this driver can provide a good opportunity to evolve from that framework to NIST.

My view of cybersecurity maturity is that it's an ongoing evolution, not a one-time effort. The NIST CSF Core offers the structure, rigor, and flexibility needed to evolve and improve any program's maturity continuously.

Q: What steps do you recommend to achieve organizational alignment in cybersecurity?

A: It's crucial to involve the entire organization. If cybersecurity is managed solely by the security team, it won't be effective. Engaging all relevant stakeholders is essential. This journey is about continuous improvement; everyone must understand and resonate. You don't have to achieve everything simultaneously; it's an ongoing process.

Q: What type of support do you feel is the most beneficial during the NIST journey?

A: You have three options: Handling everything internally, outsourcing completely, or using a hybrid approach. I prefer the hybrid approach to leverage internal strengths and capacity while validating existing efforts. Additionally, an organization may have requirements that necessitate an external review of their NIST CSF assessment. I think combining internal resources with external support enhances the learning and better prepares for the future. The approach I like is to alternate between third-party validation and conducting the assessments ourselves.

Devin Shirley, CISO at Arkansas Blue Cross Blue Shield, provides insights and best practices for improving cybersecurity maturity in healthcare organizations.

Devin Shirley

"When choosing an assessor for your NIST efforts, you can not only consider industry focus, such as healthcare cybersecurity, but also the assessor's proven expertise with software solutions. This can make the process easier both now and in the future. Having experts you can learn alongside with will have a positive impact on the maturity of your security program."

Q: What do you recommend to approach scoping and baselining?

A: If you have another assessment or audit, such as a HITRUST assessment, you can use that as a baseline HITRUST is good because it provides evidence-based validation. But, while HITRUST is very prescriptive, NIST offers much more flexibility. This allows you to adopt a "test once, cover many" approach, as moving towards a single annual assessment reduces the scope from an assessor's standpoint.

Q: What role do foundational controls play in an organizational security program and the NIST project?

A: Foundational controls are crucial in leveraging the NIST framework as a springboard to achieve a higher level of maturity. Drawing from my Krav Maga teaching experience, I always emphasize addressing the immediate danger first. Similarly, foundational controls provide perspective on where to focus efforts.

Q: How do you set cybersecurity maturity goals?

A: You have to recognize that cybersecurity maturity is a moving target. It's important to be realistic about your current state and where you want to be in one, three, or five years. Setting goals is about embarking on a continuous improvement process. You can't address vulnerabilities without first conducting a vulnerability scan to identify and prioritize them. As you mature, your goals will evolve because the journey is about ongoing improvement.

Q: What are the highlights and learnings from your experience with NIST CSF assessment implementation?

A: Highlights and learnings from assessment implementations I've been a part of include always striving to improve your defensive position, a philosophy I adopted from my military experience. No matter how good you are, you should focus on growing to the next level and adapting as frameworks evolve. Validating the findings and sharing results with no surprises is key.

Before finalizing results, setting the stage with executives and the board is crucial. Communicating findings effectively is essential: "Here's where we are, and here's the plan to close these gaps and mature to this level." You should focus on remediation and view results as a positive opportunity for the business.

Again, you must communicate often and give teams adequate time to close gaps. Set the plan flexibly and focus on achieving 20% communication and 80% execution.

Key Questions for Healthcare Cybersecurity Alignment

To safeguard patient data and sensitive information, aligning the organization around shared cybersecurity goals is essential. This ensures everyone knows their role in maintaining strong security.

Ask these questions to evaluate your organization's cybersecurity alignment:

Culture, Process, and Resources:
How can cybersecurity be integrated into our healthcare culture, processes, and resource allocation?

Engagement and Communication:
Who are the key stakeholders, and how can we keep them aligned with cybersecurity efforts?

Framework Relevance:
Is our cybersecurity framework suitable for the evolving threats and risks healthcare organizations face?

Capability Assessment:
Do we have the technical skills, personnel, and financial resources to support our cybersecurity program?

Maximizing Outcomes:

- What is the most efficient way to improve our security posture?
- Can existing assessments like SOC1, SOC2, or HITRUST help strengthen current controls?
- Have we prioritized critical systems for protection through a risk assessment?

Vulnerability Assessment:

- Have we identified vulnerabilities, including in legacy systems and third-party integrations?
- Are there hidden risks that need to be addressed?

These questions help guide healthcare organizations toward a more secure future.

Connect with Us

IntrapriseHealth.com

About Intraprise Health

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.