Intraprise HEALTH

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

Intraprise Health recently spoke with Devin Shirley, CISO at Arkansas Blue Cross Blue Shield and a seasoned security leader. The conversation highlights the value of the NIST CSF and Devin's experience leading a health plan through adoption, implementation, and greater security maturity. His sound perspective provides food for thought and ideas that resonate as best practices for any healthcare organization to succeed.

Q: Why did you and your organization choose the NIST CSF?

Devin: There are tons of frameworks out there. A major reason was because of regulatory requirements, but also organizations may have third-party requirements. Many contracts focus on NIST. And while we had implemented the HITRUST CSF, this driver brought a good opportunity to evolve from that framework to NIST.

What's the path of least resistance to get the best outcome? NIST is flexible and adaptable, as well as cost-effective. NIST can provide a baseline for all healthcare organizations, regardless of size.

Q: What opportunities did adopting the NIST assessment reveal?

Devin: It's a growth tool that gets you where you need to be long-term. While the assessment is a project, the opportunity isn't to fix things but to mature the organization's cybersecurity program. The framework reveals what's in place and the delta to achieve a more mature state.

What's our view of cybersecurity maturity? It's not a one-and-done but an evolution. The NIST CSF Core provides the structure, rigor, and flexibility to see the program's maturity evolve and improve

Q: How were you able to achieve organizational alignment?

Devin: It's key to reach across the organization. If it's run out of security, for security, by security, you're not going to get very far with it if you haven't engaged all relevant stakeholders. This is a journey whose goal is to improve over time, and people need to resonate with that. You don't have to accomplish the entire journey today.

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

"After all our vetting, I chose Intraprise Health as our NIST assessor not only because of their singular focus on health-care cybersecurity, but because they have the proven expertise plus software solutions that make the process easier now and for the future. We learned alongside their experts, which will have a long-term impact on our security maturity."

— Devin Shirley

To achieve organizational alignment, ask yourself: What aspects of our culture, process, and resources must I account for in achieving alignment? Who should be engaged, included, and updated at what cadence and in what form to achieve and maintain alignment now and for the long term? As a far-reaching project, sharing a common goal and sustaining awareness is crucial. Hidden surprises are what people like least, particularly related to security.

Q: What approach did you take to adopt the NIST framework and assessment?

Devin: From a project management perspective, we determined our desired outcomes, timeline, resources, process, contracting, and legal. From a NIST compliance approach, we started looking into documents, policies, and processes and moved into capability analysis.

The three phases of the NIST assessment break down into tools, skillsets, and technology so that we can ensure that we have what we need to effectively and efficiently work through the process but also what we need to change. I wanted to know where we were stronger and understand where we needed support.

Does your chosen framework keep up with techniques and the threat landscape? Over the long term, how will you translate this NIST assessment project into a security program so that it's sustainable in the organization? Do you have enough capability to achieve the change we want?

Q: What support did you find useful in your NIST journey?

Devin: There were three options for us to achieve our NIST goals. We could be internally driven and do it all ourselves, outsource everything through total external support, or take a hybrid approach. I chose a hybrid approach so that we could leverage our strengths, utilize our capacity internally, but also validate what we thought. Additionally, other requirements called for an external review of our first NIST CSF assessment. We brought internal resources alongside external support to support and learn for next time. Going forward, we'll use third-party validation some years and take on the assessment ourselves in other years.

Do you have enough capabilities, capacity, and NIST CSF knowledge to make the project internally driven? Do any of your customer, investor, or partner contracting require outside validation or review? It's best to determine your needs based on your organization's posture and design. Outside support can save a lot of time and frustration by helping prioritize focus and meet outcomes and deadlines.

Q: How did you tackle scoping and baselining?

Devin: Because I wanted evidence-based validation, we used our HITRUST assessment as a baseline or foundation and leveraged that work towards NIST. While HITRUST is very prescriptive, which is helpful, NIST provides lots of flexibility. I'm really trying to move more and more to that test once and cover many approach. Ideally, we want one assessment each year that gives us a much smaller landscape from an assessor's standpoint.

What's the most straightforward path that maximizes outcomes? How can you leverage existing assessments you have a history with, like SOC1 and SOC2, or HITRUST? Look at your critical systems and your environment as part of scoping to ensure you address the most valuable systems and infrastructure to the organization.

Q: What role did foundational controls play in your security program and the NIST project?

Devin: Foundational controls help you leverage the NIST framework as a springboard toward a much greater level of maturity. I used my Krav Maga teaching experience here because we always say that you have to address the immediate danger. The foundational controls help you get perspective on where to focus.

> "It was vital to look at this journey from a business perspective. You must understand your business thoroughly, be clear on your purpose for a more mature security posture and accept that you may not be able to do 100% of what you want. The end game is to secure the business but allow the business to be able to function. That balance is crucial and will go a long way towards executive, board, and team support."
>
> *— Devin Shirley*

How well do you know the NIST foundational controls? Understanding these is an exercise in understanding your basic cyber hygiene activities as well. You're building or reinforcing the foundation of your cybersecurity program as well.

Q: Do you set cybersecurity maturity goals? If so, how?

Devin: You have to accept that it's a moving target. Get realistic about where you are now and where you want to go in one, three, or five years. Goals are about embarking on a process. You can't fix vulnerabilities if you don't first have a vulnerability scan to identity the vulnerabilities and the prioritize. Identify the vulnerabilities and then prioritize them with a risk-based lens. Your maturity goals will change as you mature because this journey is about continuous improvement.

Are you clear about your vulnerabilities, or do you sense more lurking out there? Has your approach to security in the past been one of checking the box? Or, could taking an evidence-based, maturity-building approach improve your organizational security goals? Ensure all stakeholders understand that maturity is dynamic. Being realistic and maturing is much more effective than focusing on a scoring level.

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

Devin: From my military experience, one philosophy pertains to security. Always improve your defensive position. No matter how good we are, we are never happy, and we're always focused on growing to the next level. We adapt as frameworks evolve.

Related to findings validation and sharing those results, there shouldn't be any real surprises. Before the final results are in, you want to set the stage with your executives and board. It's most important to communicate findings: "Here's where we are, and here's the plan to close these gaps and mature to this level." We want to focus on remediation and keep the focus on this as a positive opportunity for the business.

Here, again, communicate often and be sure to give teams adequate time to close gaps. Set the plan with some flexibility and focus on achieving 20% communication and 80% execution.

How can you balance improved security maturity and enhancing and supporting business functions and goals? Next, what is your plan for ensuring positive, regular communication and focusing on action that improves security maturity?

Q: What is your ideal NIST journey?

Devin: The NIST CSF is not a simple checklist of security controls. It is designed to help organizations accurately and honestly assess their current security maturity. When appropriately implemented, the NIST CSF provides visibility and insight into systems, infrastructure, and data continually. Once organizations have a firm grasp of where they are, the framework helps plot a path to more robust security. Devin's experience as a health plan CISO provides real-world best practices that made his NIST assessment successful for his organization.

What takeaways from his journey should you consider, implement, or revisit? Intraprise Health has a team of security framework and assessment experts and solutions to achieve greater maturity with your program.

To learn more, visit www.intraprisehealth.com/nist.

ABOUT INTRAPRISE HEALTH

Intraprise Health is an industry-leading "tech-enabled" healthcare cybersecurity and risk management services provider. One of the longest tenured HITRUST Assessors in the industry, our broad range of information security, privacy and compliance services include: HITRUST Certification, Third-Party Risk Management, NIST Cybersecurity Framework Adoption, Advisory and Planning Services, Remediation Management, Incident Response and Business Continuity. We deliver HIPAA Security/Privacy Risk Assessments and Workforce Training via our HIPAA One® platform. Our next-generation BluePrint Protect™ platform, based on the NIST Risk Management Framework, provides intelligent monitoring, workflow management and collaboration capabilities.