DAN BOWDEN

CISO
SENTARA HEALTH

HEADQUARTERS: Norfolk, VA

EMPLOYEES: 30,000+

REVENUE: $10 Billion

When we last interviewed Dan Bowden, CISO at Sentara Health, he was focused on rebuilding a security program, with an emphasis on developing an effective, business-aligned department. Today, he shares that security is supported and trusted across the organization. He comments, "I'm rolling up on five years at Sentara now. It's been an enjoyable time for me. I'm honestly sometimes surprised how happy I am in my position. And I think in terms of how things have changed, for myself and my team, we're more acknowledged and recognized as enabling what the organization is trying to do."

EVOLVING TEAM AND PROGRAM RESPONSIBILITIES

Bowden believes security program responsibilities may differ based on the organization's specific requirements and structure. For his specific program, he says the three core tenet areas include enterprise cybersecurity, enterprise cyber risk, and enterprise identity services.

For Bowden's enterprise cybersecurity team, they oversee enterprise threat management, and control management throughout security operations, architecture, and red team work—maturing towards a future cyber fusion center. He explains, "Along with prevention, detection and response functions, this team will mature towards on-going purple team exercises, constantly testing security posture, validating the efficacy of controls, figuring out which threats are exploitable, and how you're going to mitigate that risk. The director will have responsibility for the stack of controls and how the people, process and technology in that function is managed."

Bowden is actively looking for a Director of Enterprise Cyber Risk, someone who manages all of Governance, Risk and Compliance (GRC). He comments, "The big responsibilities include vendor risk management, developing organizational information security policy, standards, and procedures, then mapping those into what our business requirements are and the regulatory requirements that we have. What are our contractual obligations? What are our internal policy obligations? And how do these align with applicable frameworks? And if we are audited, either from a regulatory, contractual, or an internal audit perspective, are we accounting for the frameworks that will be used in that audit? There's a lot on that person's plate in terms of managing a $10 billion health system. HIPAA is very challenging to manage from a regulatory perspective, but on our health plan side, some of the contractual obligations are equally if not sometimes more challenging for securing data than even HIPAA."

The third tenet of the program is enterprise identity services.

The director of this program manages the governance platform, how that platform interacts with HR and ERP, and how it is mapped into driving workflow into various systems. This includes where people's credentials will need to be created and entitlements added or deprecated, depending on how their roles change in the organization. Also, they may need to occasionally terminate access for people as they leave, and then workflow to manage segregation of duties and some of their more high-risk applications.

Bowden says, "That's how I'm going to organize my team strategically going through 2022 and the upcoming years is those three directors. And as we develop the amount of work, what drives work, what creates work, how do we prioritize things, that will then inform how we model the teams that report to them. I delegate a lot. I ask a lot of questions. How is work getting done? How is performance being managed? But for the most part, I don't really tell the directors specifically how to model their teams. The next couple of years will be interesting because we'll be changing our org model a little bit, and we will be increasing the total breadth of the services that we offer to the organization."

FOCUS ON IDENTITY GOVERNANCE AND DETECTION & RESPONSE

The top two areas Bowden and his team will be focusing on are identity governance and detection and response capabilities.

He says they are trying to align their investment in a new identity governance platform with the deployment of their enterprise resource planning (ERP). He explains, "We have a new leader in our digital innovation area. What we'll be doing is making sure that the investment we make for identity governance, for identity proofing, for onboarding workforce and consumers, that we have a really good partnership. Identity is a really big one in 2022."

An important consideration when investing resources in an identity governance platform is ensuring it is integrated with their ERP project and some other key projects the organization is focusing on. He says it is crucial to focus on alignment with other departments and ensure integration with their workflows and processes.

Increasing their detection and response capabilities is the other key area Bowden's team is focusing on. He explains, "We also will be investing in increasing our detection and response capabilities. We've had great support building up a very solid protective preventive control posture, and as we've assessed ourselves and had red team assessments, we've had to look at how we are going to detect and stop adversaries once they do get in—or, how we discover insider threats. It's tough to find good controls that give high fidelity and actionable event information, and we'll be spending a considerable amount of time on how we find the right tools and capabilities for detection. And we've done a lot of homework on detection and learned about some better internal preventive and protective controls. In particular, a much more granular segmentation inside our network that's even more robust than we've done before."

> *"The cybersecurity problem is ubiquitous and omnipresent, and everybody in an organization sees it all day every day. And I believe everyone in the organization wants to help the CISO prevent a major cyber incident."*

DEFINING A TEAM ACROSS THE ORGANIZATION

With intimate experience restructuring and building security programs from the ground up, Bowden believes in focusing on people, communication, and alignment as keys to success. He believes in defining who should be on your team when looking outside of the security department. There are different levels or degrees of a team starting with peer business leaders. He encourages CISOs to find out who the CTO, IT Director, Chief Counsel, Privacy Officer, Chief of Internal Audit, and the like are, in order to make sure they are part of your team and core stakeholders in security. Then, he suggests finding a strong oversight committee which might include the COO, someone from brand engagement, and people from other parts of the business.

Bowden says, "My point is, don't look too hard at the org chart under you until you've gotten to know people across the organization, especially who your peers are. And it's hard. It takes a lot of work. It takes a lot of time. It takes us out of our comfort zone. A lot of us IT people and security people are introverts. We play extroverts when we're at work. If you are restructuring, look to your peer set first. These peers are the people you need to consider as part of your team. You help them win, and they help you win. I'm tired of hearing CISOs saying nobody cares. I just don't believe that anymore. If you're hearing nobody cares, I would wager that you didn't talk to anyone. The cybersecurity problem is ubiquitous and omnipresent, and everybody in an organization sees it all day every day. And I believe everyone in the organization wants to help the CISO prevent a major cyber incident."