PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

DAN BOWDEN

VP & CISO, SENTARA HEALTHCARE

HEADQUARTERS: Norfolk, VA

EMPLOYEES: 28,000

ANNUAL REVENUE: $6 Billion

"I knew executive leadership and the board wanted me to come in and be successful. I was assured I would be given both authority and support to make the program effective. I was ecstatic about this opportunity and all conversations about the program were very easy. From the beginning we talked about what needed improvement and what we could to do about it."

- DAN BOWDEN

BUILDING A SECURITY PROGRAM AND TEAM FROM THE GROUND UP

Dan Bowden, vice president of information security and CISO of Sentara Healthcare for over one year, had the opportunity to rebuild Sentara's cybersecurity program after significant transition of IT leadership. His current role marks his second time building a program and he continues to leverage previous experience to make an impact at Sentara. He comments, "This opportunity at Sentara appealed to me because I wanted to work in a larger scale health system and extend my professional network."

In his first interview and exposure to Sentara, Bowden began to map out how the security program rebuild would proceed. He says, "I knew executive leadership and the board wanted me to come in and be successful. I was assured I would be given both authority and support to make the program effective. I was ecstatic about this opportunity and all conversations about the program were very easy. From the beginning we talked about what needed improvement and what we could to do about it."

These initial conversations included his CIO, who Bowden describes as a business-minded, tech strategy expert. He continues, "Sentara's CIO is a brilliant technologist who brings a different cadence to the role." Strong alignment with executives, paired with emphatic support from the entire organization, provided Bowden a solid foundation for making his mark.

CREATING A TEAM IN A COMPETITIVE JOB MARKET

When Bowden first started, he was basically the only person on the information security team, however, he developed a strong plan to overcome this challenge. He says, "My biggest concern was how we would staff the team. Virginia is a very competitive market, with defense and military contractors competing in the same tight talent pool as us."

Bowden's solution was simple and clear – to grow his team organically. He explains, "I recruited a few team members from IT at Sentara to convert to information security. I also developed a pipeline of student staff from Old Dominion University, Regent University, Thomas Nelson Community College and Tidewater Community College."

He continues, "I leverage my experienced people to work on complex risk-laden tasks, while also developing the skillset of the student staff who can work on more basic day-to-day needs. The ability of the students to support us will expand as we grow with them." Currently, Bowden's team includes twenty full-time employees and ten student staff. He expects the team to grow twenty percent during each of the next two years.

Investing and growing the future cyber security workforce is important to Bowden. He encourages CISOs to tap into this well of trainable and adaptable talent. He explains, "We all know there is a shortage in the cyber security workforce, but what are we doing to fix the problem? At Sentara, we are developing student staff into the future workforce. I encourage everyone who is worried about the skills shortage to get involved with university students, and even get involved with STEM programs at the high school level. Some people believe artificial intelligence will replace everything and solve the problem. I think we will always need intelligent people exercising good judgement."

ADVICE FOR NEW CISOS BUILDING SECURITY PROGRAMS

Since he successfully architected two security programs from the ground up, Bowden offers advice to CISOs embarking on similar journeys. He says, "First, understand how the organization identifies and manages risk. Understand which data needs to be protected and how well-prepared the company is to deal with major incidents. Those are the things that should drive your early conversations."

Soon after his arrival, Bowden and his team rolled out two-factor authentication to 60,000 users in 120 days. He says the experience was a complete team effort involving the entire organization. He remarks, "Marketing and communications were heavily involved in the roll out. It was not about the technology, it was about the entire organization buying into why we needed two-factor authentication and supporting our efforts. Early successes like this are important to increase confidence and help to establish that information security is an organization-wide effort."

Now that the initial set up of the program is complete, Bowden and his team are focused on managing risk and supporting business goals. "Like others in the health care industry, we are working to provide better service to patients and plan members. Part of that is rolling out a digital mobile platform to get more, and better, information into our patients' and members' hands," he says.

Bowden ensures the actions of his team and decisions they make are directly correlated to supporting the overall business goals and priorities. He comments, "Because of the complexities within health care, our digital mobile platform is a very iterative process, and as the security team we have needed to be very flexible. Our priority is to make sure that the business can keep advancing as we continually assess risk in an efficient and timely manner."