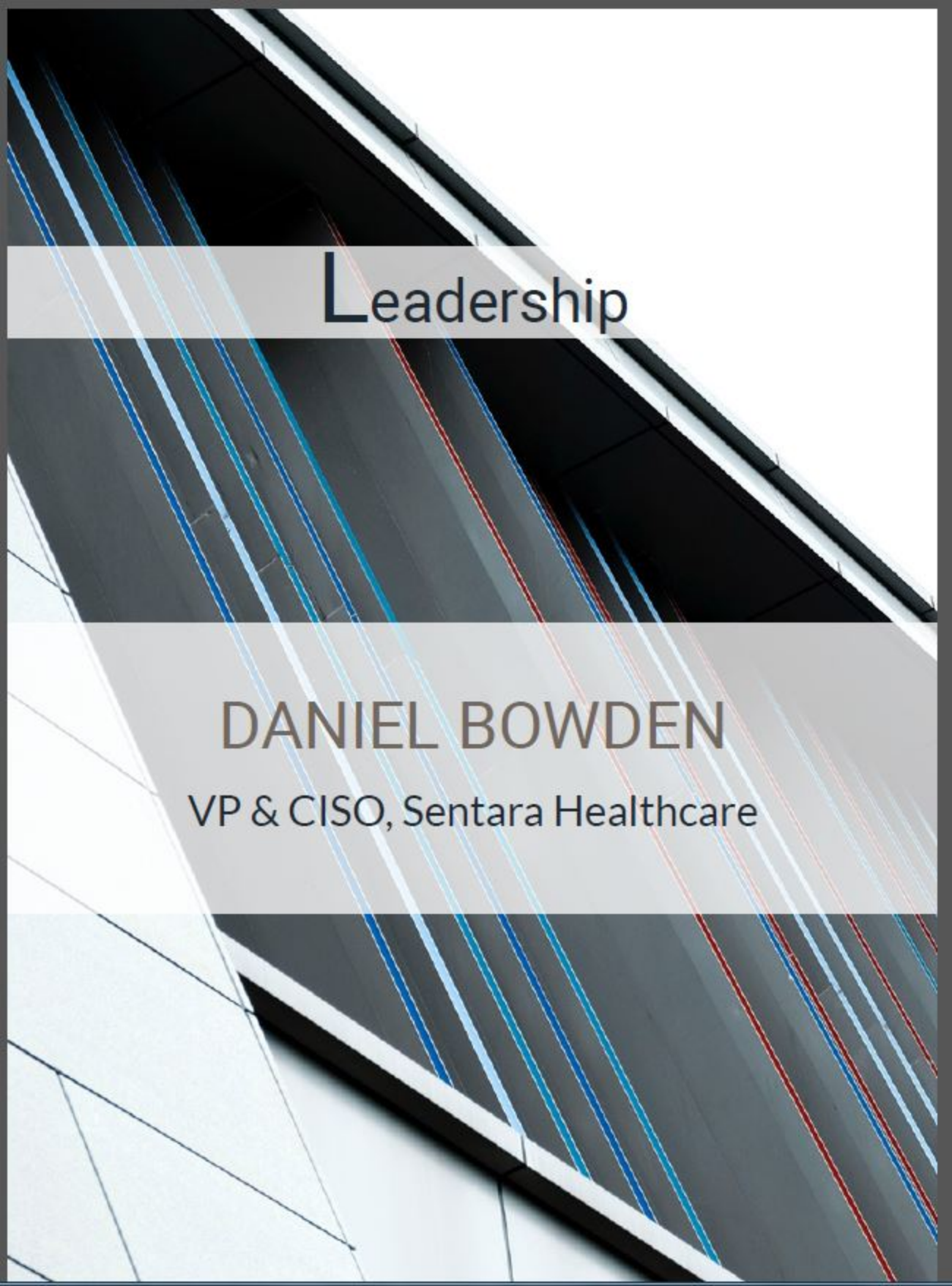
Leadership
DANIEL BOWDEN
VP & CISO, Sentara Healthcare

Daniel Bowden

VP & CISO, Sentara Healthcare

Dan Bowden is VP and CISO at Sentara Healthcare. Dan has led cybersecurity and technology programs for healthcare, higher education, banking, retail, and the military.

Dan is active with the Health Sector Coordinating Council Cybersecurity Work Group, collaborating with several top healthcare cybersecurity pros on documented guidance for all health systems to improve cybersecurity practices.

Dan's current professional focus areas include: cybersecurity workforce of the future, program strategies for protecting cloud and digital platforms, the development and patenting of a blockchain-based health utility network, and delivering cost-effective cybersecurity services for medium and small health systems.

The CISO's role is a very high-pressure, high-stakes job. What is the right profile for this job?

I've seen several people promoted to CISO because they were the best security geek on the cybersecurity team—then ultimately fail because they weren't equipped with the leadership and influencing skills to get peer leaders to buy-in. Being the most cyber-tech savvy only gets you so far—and isn't a translatable skill for becoming a successful executive in your organization.

The right profile is somewhat difficult to point directly at, because as I look at many of the successful CISO out there, we did not all follow a specific path to here.

Considering the right profile for handling the pressure, the CISO has to be an outstanding communicator, and use this skill to lead by influence. Most CISOs don't have the luxury of imposing their will via the org chart. They must influence other key influencers in the organization to help drive better cybersecurity practices. They must be able to speak, write, and present—and do these things at times with very little notice. Becoming a great communicator is a challenge. I've improved a lot over the years by constantly assessing risk and remediation strategies in my mind, then writing about them, talking out loud about it (even to myself at times) and creating presentation content about it.

A good CISO can create and deliver an impactful and concise statement about any of the major threats to their organization at an executive or technical level on the fly.

When speaking the language of business to their boards, are there certain phrases CISOs should be using?

> **"Seek first to understand, then to be understood—I think Covey said that. The first thing I did at Sentara was to listen to the board and executive leadership."**

Seek first to understand, then to be understood—I think Covey said that. The first thing I did at Sentara was to listen to the board and executive leadership. They were very clear about the concerns they had with cybersecurity before my arrival and what measures would ease those concerns.

When my time came to speak, I led with the key measures they wanted, in the language they speak. Things like "benchmarks against peers", assessments of "likelihood and impact", negotiating "risk tolerance", and creating a "culture of cybersecurity".

My first two years at Sentara have been very successful. I attribute a lot of it to our board and executive leaders defining what they wanted, in the language they wanted it. I organized the program around this, our team put in the work, and then we reported the results.

Almost everybody agrees that organizations need a culture of security. How can security leaders help facilitate that type of culture?

This is easy. Something interesting I've watched the past several years—cybersecurity threats have become ubiquitous in business, life and society. We can hardly watch a movie where cybersecurity isn't part of the plot, we hear about it on the news every day, often multiple times. In a way we've become this cool, mysterious group of people that others really do want to associate with—a huge shift from 10 years ago!

I've learned that everyone wants to be involved, so I just let them. My team creates the messages, and distributes them for others to share—and they do it! I think too many CISOs are bent on always being the messenger. They want to be giving all the presentations and doing all the talking. Frankly, I feel a CISO's tenure is based on building and burning goodwill—and every minute they spend telling people what to do, they are burning it. I'd argue that messages about cybersecurity from the CEO, COO, HR director, etc. are orders of magnitude more powerful than coming from the CISO.

In a way, everyone wants to be "like a CISO". Let them do what they think is the fun part—go out and talk about it. It builds the culture we're after.

What are the biggest challenges you face in the year ahead?

For me, the ever expanding threat surface. Like many health systems, we're advancing our consumer engagement capabilities: mobile apps, better web portals, public cloud infrastructure, wearable internet of medical things, and collaboration in blockchain networks.

We'll have multiples of increased devices and people to manage risk around. The team will expend a lot of resources understanding threats and vulnerabilities with a completely new set of countermeasures—we've learned none of our "on premise" security controls work optimally in public cloud, infrastructure as code. My team now runs two process and control sets simultaneously. Over the next few years we'll have most of our infrastructure in cloud, so things will normalize to a new norm.

How can CISOs balance security and innovation?

In 2019, I think CISOs must be innovators, and looked at as such. In healthcare, most of the provider health systems have been cloud averse—which has made no sense to me, especially since most of the aversion has been about security. My point: read the news, health systems are frequently having breaches in their own infrastructure and none have successfully pinned blame on a cloud provider. I've been all in favor of cloud because we get a "do over" to implement better configuration standards and process—which are a key ingredient to good security.

Another prevailing innovation topic in healthcare is blockchain. CISOs are often cynical about this because in some organizations it becomes a technology "hammer" and everything else looks like a nail. Big issue for CISOs because there is no native security in blockchain—you have to bring your own. At Sentara, I was invited to the table early on. We've had a great couple of years doing research and will be joining some very promising partners in creating business value for provider and payer organizations.

CISOs should take the initiative to be involved with innovation. If you don't take a place at the table, you may end up on the menu.

> "CISOs should take the initiative to be involved with innovation. If you don't take a place at the table, you may end up on the menu."

How has industry cooperation made an impact on cybersecurity?

In healthcare, it has been huge. Go check out www.phe.gove/405d.

I've been in healthcare ten years now. Five years ago, there was basically nothing but HIPAA and NIST for health systems to reference. This was a huge problem for 80% of health systems without CISOs. It is amazing to me that the fallout from Wannacry and NotPetya wasn't much worse for healthcare.

Now we have the Health Sector Coordinating Council, Joint Cybersecurity Working Group. There used to be a complete vacuum of activity. Now I have conflicting opportunities to collaborate with peers in healthcare. We also subscribe to H-ISAC which has improved immensely the past three years.

I have a great extended professional network of CISO peers. I was lucky to be invited to a collaboration channel with what most people would call the best CISOs across any sector. I learn a great deal just reading the posts as they go by during the day.

My organization also supports a great partnership in a formal Information Sharing and Analysis Organization (ISAO) with seven other premier health systems. We have weekly threat/incident calls, and monthly CISO calls where we compare benchmarks, strategies and new technology adoption.

> "The best cybersecurity practices and solutions are those driven by business outcomes."

The best cybersecurity practices and solutions are those driven by business outcomes. Good CISOs know, cybersecurity isn't "the show"--successful business outcomes are Effective cybersecurity is a crucial enabler for business.