PROFILES IN **CONFIDENCE**

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

SUMIT SEHGAL

CISO, **BOSTON MEDICAL CENTER**

HEADQUARTERS: BOSTON, MA

WORKFORCE: 10,000 +

ANNUAL REVENUE: $4.1 BILLION

TODAY IS ABOUT **PEOPLE**

Sumit Sehgal, the CISO at Boston Medical Center (BMC) has seen many changes in the last ten years in Information Security. “Years ago, the priority was to set up point security solutions to get an adequate idea of what was going on in your network. Over time, the focus for me was less on tools and more on how we influence and change behavior to improve security – the human side of security.”

Sehgal and his team do not rely on presentations and “top down” security awareness training. They work to make security more relatable and personal for the workforce at BMC. “We give them a choice, and we engage with departments to customize training to their interests, needs, and requirements.” He believes they are more receptive to the training, creating effective results. “Each member of the workforce has the option to complete 3 out of 5 security training modules per year, allowing them their own choice,” he says. The modules focus equally on security at home and security at work, including topics like social media and cyber bullying. When the workforce learns about things that apply to their personal life, it increases their engagement in what they need to learn professionally.

He also believes it is important to partner with organizational influencers, not just executives and business leaders. “Find those people who have an infectious cloud around them, and engage them. They will help foster the message in the community. When it is presented this way people take security precautions because they want to, not because they have to do so.”

THE FUTURE: **CONTEXTUAL ADAPTIVE RISK**

While people will always be the most important part of the security equation, Sehgal states that emerging technology will play a big role in the next evolution of security. He is interested in the impact technology innovation will have on the future of security efforts, specifically whether artificial intelligence technology has the ability to help with contextual adaptive risk, or the idea of real-time awareness of the specific risks data is exposed to at any point in time. Sehgal believes the next innovation will be security systems agile enough to communicate changes to the risk threshold based on changes to the data in the environment.

HOW TO GET **THINGS DONE**

Sehgal has this advice for newcomers to the CISO role:

PRIORITIZE

Focus on no more than two priorities at a time. "Anything more than two priorities is too noisy. Some organizations do not even have the appetite to address two, maybe one is all they can handle," says Sehgal. Also, be flexible and adaptable with your priorities. Sehgal suggests aligning your priorities with business goals. If priority number three is a bigger priority for other executives in the company, then work to achieve that goal, because it is likely to help you in the long run, both with your other priorities and to engender loyalty and trust with the other executives.

INFLUENCE

"Take the time to know who the influencers [in your company] are. Talk to peers, talk to leaders, and network with the people who make stuff happen. Once you have established their trust, they will help you."

ROADMAP

CISOs that need a guide for their first 100 days should look at the SANS 20 CSC as it is a good roadmap of things to think about and evaluate. "SANS covers the breath of everything a CISO should consider from a control perspective and it will help you prioritize your efforts."

KEEP CALM & REMEMBER WHY

"I have had very good mentors from a leadership perspective. They helped guide me and understand how the business functions. I've been in healthcare my entire career. My mentors helped me learn to focus less on the minutia of security and instead remember why we are doing this. We do this because someone is getting treatment here. We need to care for them, and part of that is safeguarding their personal information. Stuff [incidents] happens. Things break. People will get upset. Focus on the solution, not the anger. My first motto is 'keep calm.'"