CISO **SPOTLIGHT**

We check-in with CISOs we previously featured and profiled in our magazine.

Learn about how their roles have changed, how they've grown as leaders, and their accomplishments.

Read Q&As from:

Michael Newborn, CISO McKinsey Digital Labs

Sue Schade, Principal, StarBridge Advisors

Darren Death, CISO, ASRC Federal

What has been the biggest change since we last spoke in 2015?

I left Bloomberg in 2016, and a little later in the year started at McKinsey in two distinct roles. I'm the CISO for one of the practices here, similar to previous roles I've had where I manage the cyber risk program for the organization, and I'm an associate partner serving global clients, primarily on the topic of cybersecurity. Although I've only been here for two years, it feels like a decade – I've been introduced to a wide range of companies, domestic and foreign, across many industries.

How has your alignment with executives changed?

In the past couple of years here, I've been exposed to a broad range of challenges executives face and the complexity involved in their decision making. It has helped me better understand the business perspective – and enables me to take a more holistic approach across technology, business strategy, and compliance. This includes everything from top-of-mind cyberrisk issues and improving digital resiliency, to social engineering and how you effectively build and operate a cyber risk management program for a company – and how you approach all of this as it changes based on company size.

What industry changes have you experienced over the last few years?

Over the past couple of years, our industry has seen everything from election tampering to the rise of ransomware. We're also seeing an increase in the average person's understanding and awareness that there are real cyber risks out there that don't just impact big companies, they can impact all of us as individuals. I think that's also driven an increased awareness within organizations' senior leadership, a realization that cybersecurity still needs to remain top of mind. It's not going away. This increased awareness has led to a demand that is greater than ever for cybersecurity talent. There's a noticeable gap between demand for jobs and the number of people available for them.

In terms of trends, I've seen an increase in cloud adoption, yet too often, basic security controls aren't effectively being met. It's the same thing with patching. We've had to patch things for years, yet getting to a 90+ percent patch compliance rate seems to be very challenging for most organizations.

We've also seen a big proliferation of Internet of Things (IoT) devices, whether it's home automation, semi-automated cars, baby cameras, etc. I think over the past few years, we've seen a significant number of attacks with IoT devices and I think that trend will continue.

How do industry trends impact your approach to cybersecurity?

We stay on top of the latest trends and help develop industry knowledge. Earlier this year, I co-authored a paper, *Making a secure transition to the public cloud*. We interviewed 100 organizations over a six-month period. The report offers a perspective on how to build an operating model around public cloud adoption to make sure security is part of the process from the beginning. It considers what organizations need to know if they're using IoT devices – including where the devices are, since many organizations have them in wide use. Often times, organizations don't make it a priority or don't have an easy way to classify and identify those assets to ensure they're being protected and segmented properly.

What has been the biggest challenge since we featured you in the magazine in 2015?

I have served as interim CIO in two different organizations in the past few years. One of the first areas a new CIO, whether permanent or interim, looks at is security. The strength of the IT security leadership and maturity of the overall security program. In one organization, we had a very strong CISO and had just opened a SOC – security operations center. In the other organization, we were strong on user education, policies and procedures but needed some work on the technical side of our program. Figuring out your security gaps, gaining executive and financial support to address, and then implementing necessary changes is critical in your first 90 days.

How has your executive alignment changed?

Executives in both of the organizations where I served as interim were supportive of continuing to strengthen the security program. The CIO and CISO must be able to educate, without fear mongering, the executive team on security risks and gain their support for necessary changes that may be unpopular or viewed as too restrictive by end users.

How has the industry changed and what impact has that had on your security program?

My new health IT advisory firm, StarBridge Advisors, provides IT consulting and interim management. As I work with CIOs I am seeing an increased demand for experienced CISOs overall in healthcare. For small organizations with low budgets, security programs have not been invested in to the extent needed. Discussions with those CIOs often include security assessments and either part-time or virtual CISO options. Overall I see an increased awareness by boards and the C-suite as cybersecurity risks increase.

Also, I'm encouraged that more women and men are willing to talk about the challenges facing women in the workplace and the need for more women in STEM fields. I'm currently working on developing coaching services for women at different stages of their career.

What has changed most from a personal perspective since we profiled you?

I made a decision in early 2016 to leave my permanent position at the University of Michigan Health System (now called Michigan Medicine) to live near family in New England where I now have four grandchildren and to become an entrepreneur doing IT consulting, interim management and leadership coaching. I wanted more flexibility in my career at this point.

What has changed most from a professional perspective since we profiled you?

As my first interim CIO engagement ended in the fall of 2016, I formed StarBridge Advisors with two colleagues. We just celebrated our two year anniversary as a firm and are providing a range of health IT advisory services to healthcare organizations, including security assessments and interim CISOs.

What has been the biggest challenge since we featured you in the magazine in 2015?

My biggest challenge has been implementing a full scope Information Security program while implementing major Information Security frameworks. My team and I delivered ASRC Federal's fully compliant rating with NIST SP 800-171 on 09/29/2017. This rating was delivered $2 million dollars under budget and three months ahead of the government mandate. The team and I also brought ASRC Federal into compliance with the Center for Internet Security (CIS) – Consensus Security Controls (CSC) on 07/26/2018 with minimal financial impact to the organization. I am currently bringing ASRC Federal into compliance with ISO27001 and planning to achieve ISO27001 compliance by the second Quarter of 2019.

How has your executive alignment changed?

I still report to the CIO of our organization. We have a great relationship and this certainly benefits the team and the organization. The big difference now is that I brief my company's senior leadership quarterly regarding cyber risks and information security program status.

How has the industry changed and what impact has that had on your security program?

The federal government and private sector customers require a lot more out of their vendors in terms of security offerings and postures. This has been great for the information security programs as it justifies the needed work that every organization should be implementing.

What has changed most from a personal perspective since we profiled you?

I can now stand on my paddle board without falling in, which is fantastic. Everyone in the family has a paddle board and we go out on the water often.

What has changed most from a professional perspective since we profiled you?

I completed my master's degree and I am currently working towards the completion of my Doctoral Degree in Cyber Security.

I wrote a book in 2017: *Information Security Handbook: Develop a threat model and incident response strategy to build a strong information security framework* and in 2018 I've had eight articles published, including Forbes, SecurityCurrent, CIOReview, and CIO Applications.