NICOLE KINNEY

Business Information Security Officer
Fifth Third Bank

HEADQUARTERS: Cincinnati, OH

EMPLOYEES: ~20,000

REVENUE: $8 Billion
(Reflective of Fifth Third Bancorp, the indirect parent company of Fifth Third Bank, National Association)

Nicole Kinney did not have a traditional path into technology or security, but her vast business background enabled her to drive positive changes across organizations throughout her career. In her undergraduate studies at UMass Amherst, she studied areas of management and building construction technology, design, and psychology. She gained a highly versatile interdisciplinary education and landed her first job as a project manager at a technology organization serving the Farm Credit Banking industry. Here, she had an opportunity to self-educate on many different technology topics and wear multiple hats outside of project management. She explains, "I gained exposure to relationship management, configuration management, test plan development, and things like transitioning the organization from a waterfall approach to agile software development methodologies. With all that, I got a bug for technology and ended up moving to a large insurance organization in their rotational technology leadership program and continued to really expand on that broad discipline of different skillsets."

While working in the rotational leadership program, Nicole was part of rotations in areas such as quality assurance where she built out a team working on their billing systems, as well as identity and access management, bringing transparency into who has access to what, and setting up initial risk assessment and risk management work. She explains, "I also focused on the business where I embedded myself at a program management level to understand their technology portfolio and how I could help move that along to serve their different business needs and strategies. Coming out of that program, I wanted to really push myself to grow my technical skillset because I felt that I needed to have a stronger technical foundation and experience as a practitioner to be a more effective technology leader."

During this time, Nicole was exposed to information security when she worked on a team focused on email and web cyber security controls. She began as a technologist on that team and worked to grow her technical skillset from implementing changes, configuring different systems, and managing the vendor relationships. Over the next several years, she worked her way into a team management position where she led a team and programs such as helping the organization move from completely on-prem email filtering infrastructure to a cloud-based solution. She comments, "It was a multi-year multimillion-dollar program that was really satisfying to see complete, and work through all the complexities of doing a project like that in a very large multi-national organization."

After spending more than nine years at the insurance organization, Nicole moved to her current role, Business Information Security Officer at Fifth Third Bank. A little over one month into her new role, Nicole says she is excited for the opportunity to shift towards a different type of leadership with exposure across the entire enterprise leveraging her soft

> *"What I value most is open, honest, respectful communication, I think getting that dialogue going, making sure that everyone has a voice, is part of the conversation and is included is so important."*

and technical competencies.

IMPORTANCE OF SHIFTING LEFT

After working on projects during her career related to cloud migrations, Nicole strongly believes in the value of a focus on shifting left by getting security involved in development from the beginning. She explains, "It's an unfortunate experience when you've got a technical team that has developed, coded, worked up, and created something, then they're at the end of that journey and ready to go use it, and you find out that security was left out. You are now facing the possibility of having to do a lot of re-work and you're not able to responsibly publish something to market knowing there are risks or gaps that could cause security problems. I think that's something that all organizations are really working on doing, and part of why the role that I'm in now is so important to me. I really have a chance to continue to bring that security mindset upfront and partner with the technology teams across the organization to help provide guidance and consultancy, to enable them to do their best work."

One of Nicole's mentors had the motto that 'security isn't no, it is how', something she believes perfectly sums up the shift left mentality. She sees her charge as a security professional to be a resource, understand what other departments are trying to do, and help them do so in the most secure way possible.

LEADING WITH PURPOSE

Nicole says her goal is to strive for continuous improvement and always find ways to make the areas she has influence over incrementally better. She found the key to enacting that kind of change is to invite open communication and listen to feedback. By hearing what people have to say, then working with them to experiment and try out different changes, you move toward an ideal state progressively, and together.

She continues, "What I value most is open, honest, respectful communication, I think getting that dialogue going, making sure that everyone has a voice, is part of the conversation and is included is so important. For me, people and relationships really matter most, it's not about what you're doing, it's about how you get it done, and making sure you do that in a way that really focuses on your customers, your network of people involved and all the stakeholders. I believe in the servant leadership concept. I'm very service-oriented and focused on enablement and how I can give my team what they need to be successful. I also really value the concept of going slow to go fast and making sure you have a clear strategy and vision of what everyone is driving towards before you just rush into implementing. This is important because it helps prevent a lot of confusion or wheel spinning. Most importantly, I believe in trying to have a little fun wherever you can. Our work is very, very serious, it's important, and it can be very stressful and anxiety-provoking at times, so trying to manage that stress by finding ways to bring enjoyment and some fun to the work wherever possible can really go a long way."

To continue to grow and learn, Nicole believes in plugging into different professional networks, peer groups, as well as dedicating time to independent reading and research.

Attending conferences are also a valuable tool for Nicole to network and learn, she comments, "Conferences are great for staying up to date on all the different products and tools that are out there, and now they're starting to be in-person again. One of my favorite parts of going to conferences is the interaction you get with your peer groups and being able to strike up casual conversation with people across different industries and from different companies and hear how they're doing things. One of the more recent conferences that I was at had many talks on how the criminal enterprises work just like a company. They're working within a network, they're working together and sharing information and we need to do the same. The more you can share information and knowledge across different peers and different networks, the better for getting a sense of what kind of attacks are happening and what kind of targets are sought after."

SECURE ACCESS SERVICE EDGE (SASE)

"SASE is a little bit of a buzzword, and a current trend. It goes back to the fact that the same security principles apply, whether you are operating on-prem or in the cloud. It's about defining those trust perimeters and understanding what is trusted versus what isn't, and how you manage that as the culture of technology is evolving to have even more sharing and connectedness. It comes back to enabling that increased sharing and connectedness while being able to have the right switches to turn on and off to protect what is yours, or quickly identify and contain if something were to be compromised or get out of control, it is a tool you can use to make sure that you're protected from that kind of threat activity and that it doesn't have free access to move across your technical ecosystem."