Q&A with John Masserini, Chief Information Security Officer at Millicom

sailpoint.com/blog/qa-with-john-masserini-chief-information-security-officer-at-millicom

George Hulme May 6, 2019

In this Q&A we spoke with John Masserini, chief information security officer at international telecommunications provider Millicom. Millicom is a leading provider of cable and mobile services in Latin America and Africa under the brand name Tigo. As of the end of 2018, Millicom's operations employed more than 21,000 employees and provided mobile services to about 48 million customers. Millicom was founded in 1992 and is headquartered in Luxembourg. Masserini talks with us about his interesting career path in information security, cloud security, and identity management. Here's an edited version of our conversation.

Could you tell us a little about Millicom?

Millicom is one of the largest mobile and cable service providers in Latin America where +90% of our business comes from. We pride ourselves on enabling the digital highways for our 48 million customers so they can live and enjoy a digital lifestyle. All the countries we focus on are up-and-coming economies throughout Central and South America. These economies are still emerging in a lot of ways, but are certainly putting everything in place to become very strong economic players in the future.

We also pride ourselves in being able to enable purpose-driven connectivity in the communities where we operate. Our digital highways help customers and communities overcome obstacles to access the digital, interconnected world. Every day we see countless stories of customers who, because they own a cell phone and have access to Tigo's Internet service, they can run a delivery service or an e-commerce store; and they're the first person to have a job in four generations of their family. They're supporting their whole family with this and it's simply because they're able to take micropayments or take credit cards on their mobile device. Additionally, Tigo provides cable TV and internet services to over 10 million homes throughout Latin America. In fact, one in three households is a Tigo customer in the countries where we operate.

There's a tremendous amount of pride and a true feeling that we are improving people's lives, something we internally call Sangre Tigo. Through our digital highways we are changing people's lives fundamentally, as they have access to a digital economy.

And we do this in a responsible manner. This is where the Information Security team comes in. By building a culture of security among all of the employees and by facilitating a robust, scalable, and secure network infrastructure, we ensure that both our customers and our company are protected.

How did you get started with your career in information security?

Out of high school I took a job running nightly operations for a small bank in Princeton, New Jersey. I really enjoyed the programming and technology side of the industry, and honestly, security wasn't even a career path at that point. Eventually, I ended up at EDS, one of the largest service providers in the world back in the early '90's. As the application development manager, I ran a team of developers for a data center where we serviced about 35 financial institutions.

Because we ran the operations of dozens of financial institutions, we would have a different federal auditor come in every month as part of the routine inspection process. They wanted to understand our controls and how we protected the bank's information. I took the risk and control side of the responsibilities, and it worked out really well for us as we helped to get these banks through their audits.

Things changed for me when my boss was transferred to Charlotte, North Carolina. He called me and said they were working on building an internet stock trading platform and needed somebody to help them with security. He offered me that role.

The rest is basically history. I relocated to Charlotte and spent some time there. Years later, I spent time working with a couple of startups and consulting between Boston, D.C., and New York.

After about eight years, I took the opportunity to take a CISO role at Dow Jones and the Wall Street Journal. That was the first time I actually faced identity challenges. I spent six years there and learned everything I could about information security and business continuity. Once Dow Jones was bought by News Corp, I even owned compliance and audit, which was a little strange, but it worked. After Dow Jones I spent the next six years building an equity options exchange in Princeton, New Jersey.

At the exchange, I helped build the entire infrastructure from the ground up. I'm very proud of what we did there. We won several awards for the security program we built; and we were able to drive a lot of business to the exchange based upon our continually excellent audit reviews and security practices. But just very much like Dow Jones, it got to a point where it was very much on autopilot.

Then the opportunity presented itself to build another security program here, and I took it. That's what I'm doing now, building a global program and coordinating the local teams in each country. I'm developing a strategy and setting the tone for where we want to go as a company and helping all of the local country operations.

Looking back when you were at Dow Jones in 2005 to 2011, that's the timeframe when we first started talking about cloud seriously for large enterprises, outside of the Netflix's and Amazon's of the world. Since then the tools to manage cloud seem to have changed considerably. What changed with the tools that made you so comfortable with cloud?

If you look at the cloud providers out there, they now integrate with a lot of those tools. They didn't have open API's before, where we could monitor and manage what was happening in the cloud environment or get the logs out of the environment for analysis.

Now, there's finally a willingness for these providers to be open. I think they've realized they have to be in order to be successful. I look at what Amazon is doing, and they now have this entire security platform that integrates with what we need. Ten years ago, that never would have existed.

That's a lot of the change. I think it is the pressure that the businesses have put on providers. They pressured them to open up.

How does identity help in your security efforts?

Identity is a very fundamental practice. Identity governance provides a way to automate menial tasks so that we can audit and report properly to hold people accountable. When I look at identity, that's what I look at. Look at the attacks that we know about over the years—they all involve identity and account takeovers. If an attacker can hide while acting like an employee, it's incredibly valuable to them.

It's so important—if an organization doesn't have a solid identity program, everything else they do is somewhat useless. It's a zero trust world and the last protective control you have is the identity.

We are rolling out SailPoint now, and it's critical to make sure we roll it out in a way that's effective. Because we just listed on Nasdaq this year, we have very specific reporting deadlines that we must meet. Identity absolutely plays an important role in our Sarbanes compliance and it's a priority to hit those regulatory deadlines.