Cyber Security Business - Episode 3: "Identity and Access Management" with John Masserini, CISO, Millicom

Kevin West: Welcome to Cyber Security Business with Kevin & Kevin. I'm Kevin West, the CEO of K logix and I'm here with Kevin Pouche, our COO. In our podcast, we interview CISOs and other security leaders to hear their advice about the business of information security. This podcast gives our listeners actionable takeaways to help them increase the effectiveness of their security program.

Kevin Pouche: Thanks KW. So the game plan for today will be to discuss identity and access management. We're joined by John Masserini, the CISO of Millicom. John, welcome to the podcast.

John Masserini: Thank you very much gentlemen.

KW: So John, before we get into the topic of today and we definitely are looking for your advice and your effective leadership specifically in identity and access management, but we want to give our listeners a little bit of context. Can you tell us a little bit about Millicom?

JM: Sure. Millicom is a global telecommunications cell phone provider, primarily in Latin America and Africa. We offer not only a mobile cell phone service, but also cable to the home and a lot of mobile financial payment services as well.

KW: Great, and tell us what your vision for your security program is at Millicom?

JM: So the vision here, quite honestly, it's a little bit different than historically what I'm accustomed to. We have 14 operations throughout Latin America and Africa, each with their own local requirements, local business drivers, and local challenges. The program here from a global perspective is very much around providing a guidance and a direction globally for all of the operations while still providing a capability for them to have enough flexibility and freedom to do what they need to for their local businesses, local regulations, and local risk and security challenges.

KW: A global operation like that must be hard to manage from a security standpoint. So leadership, I'm sure, is very important.

JM: Exactly. And that's the reality, it's about having a cohesive strategy, whether it's managed security services, whether it's identity access management, vulnerability management. It's really about being able to find a common level for all of the operations and really bring together a global view of overall risk and understand how it impacts the company as a whole as well as the local operations of business travelers.

KP: Thanks John. Let's jump into why we're here and that's discussing identity and access management. So I think we'd like to hear from your perspective why this is important in and then further, why it's a challenge. In terms of why this is important, if I'm your CEO, why do I care?

JM: Great question. Why do you care? Why do I care? The reality is, as all of these operations and enterprises really lose the perimeter, and when I come into an operation like this, or a lot of operations these days, between managed services, cloud services, third party relationships, really understanding who your users are, what access they have and the rights they have is kind of foundational for applying a

solid security model throughout the organization now. We're years away from being able to say, “the old M&M model,” the hard-outer shell. We trusted everybody on the inside and kind of knew what was going on. That's fundamentally gone. It's been years since we've been able to really rely on that model.

So when you look at everything we base our decisions on, it’s really around the access to the right environments, the right applications, the right data elements. And that's all really founded on identity and access management. We have to understand who our users are, whether they're our employees, our service providers, third party partners who are just providing some random service, really be able to understand and really validate and monitor the access they have. In this day and age, when we look at the access or the attacks that we're seeing these days, it's really around people trying to get those privileged accounts. Whether they start off with a regular account and eventually escalate, whether they're able to get root or admin somewhere, it's really about those credentials and that identity is really gold for them.

When we look at mitigating our risk, and when I look at my board and my CEO and talk about risk mitigation, it really is around understanding who has access to what. It's not about firewalls. It's not about graphs or IDS or any of that kind of stuff anymore. It's really about allowing our businesses, especially in an environment like this to have access that they need when they need it, but only what they need to get their jobs done.

KW: So is that something that an executive understands? It seems pretty logical in order to secure and reduce risk.

JM: Most executives understand the need for partnerships. They understand how we're not a self-contained business any longer. They're pretty accustomed to, whether it's office 365 or Google or whatever shared service that a lot of us use in our personal lives, they can relate to that. Getting them to understand conceptually how we have partners and providers that work in that same model isn't a stretch the way it was five years ago. It really is something that you can relate to their personal aspects. Getting them to understand that you have controls over who can see your google docs drive, when you relate that to the infrastructure here, how we might have competitors in our environment, I'm doing two different things, but we need to make sure they can both do their jobs that we've hired them to do, but yet not necessarily cross those boundaries. They get that. They understand it because you can really, in this day and age, relate it to what they do on a personal level.

KP: So you had alluded to this being more of a program than a function of technology. I think that's what I heard. Does this require full time people and should those people be in security, a different department, or does this cross pollinate between departments?

JM: It's absolutely a program. Obviously technology plays a role, but it's not in the case where we can throw a piece of technology in there and assume it's fixed and walk away. This is a program that has, from a security perspective, people who monitor it and manage it. The whole identity access scope really does permeate the company. We have a great relationship with our human resources team because when they're onboarding employees, offboarding employees, it's critical that as they update the HR system, all of that flows right into an identity management system. So they really have to understand what they're doing and the importance of roles in their system.

When all of that flows over, there's still a process that occurs with our corporate IT staff. They're creating accounts. They might be adding different roles depending upon what the manager has requested or a specific job function that couldn't automatically be provisioned. There's definitely a cross pollination, in my case, there's even an aspect of it that happens locally at each operation. The bulk of the work will come from HR, we'll get corporate IT involved as well, who will do the provisioning. And then the final part is done by the local operations. If they're in Bolivia or Paraguay, that team will ensure that they have all of their local privileges that we don't necessarily control at the corporate level. I would argue that identity and access management is probably the best use case when it comes to the cross pollination throughout the company. My HR team was kind of excited when we started sitting and talking about it because they usually don't get that interaction, where here, we're going to rely pretty heavily on the job they do to make the whole rest of the process more streamlined.

It's definitely a program. The folks on my team spend more time on the managing and monitoring it, making sure that the roles are provisioned right, making sure the manager attestation and workflows are followed correctly. IAM plays a large part of SOCs, so when you look at people coming in doing an audit to make sure we're SOC compliant, they want to see the evidence that the manager approved the roles, that it was done as automated as possible, but there is also an attestation afterwards that the roles were reviewed and set up correctly. So it's absolutely a program as well as multifaceted throughout the organization.

KW: So you said something pretty interesting that HR got excited at the possibility of a workflow like this, was your team instrumental in bringing this to HR or did HR come to you with a problem? How did that come about?

JM: Yeah it was kind of mutual, to be honest with you. We knew we had to take a bigger picture approach at the problem rather than just throwing more people at it to turn the requests around more or to do the scrubbing or to do the cleanup. It was more of a root core problem. At the same time the HR team was going through an effort of identifying a new platform, really modernizing their entire technology infrastructure. So in the effort of building the whole global security program, during one of my conversations with the HR team, we got on the same page and we have a real opportunity here to fix this at a very foundational level. That actually led to a lot of excitement, a lot of dialogue. They are on my project team, I am on their project team. It's actually created a really unique working relationship that I can't say I've really had in other organizations. There's a lot of excitement around it.

KP: This problem, it's a big problem. It's talked about in multiple departments. In a less mature organization or potentially a new CISO coming into an organization that hasn't yet tackled this problem, where do they start and what do you think the building blocks for a strong program are?

JM: Wow, great question. The building blocks and where do you start are really around trying to understand and put an effort into really knowing where your identities are. When you walk into an organization, the presumption would be most organizations don't have a very mature identity management program in place. There's typically a centralized area where the email accounts and network access are stored. But once you get away from that, things get very disparate very quickly, whether it's two factor authentications run by the networking team or some local application where you have to set up and maintain your standalone credentials, whatever it is. It's really about spending time to understand where they all are.

We're not just talking about user accounts, we're talking all the way down to SSH keys. There's a very good possibility that if your admins are using SSH, that there are keys on servers that probably have never been updated or renewed or folks have left and their keys are still on the environment. So understanding everything about your identity space takes time. It really does. It's not an easy thing to get ahold of. It really is around making sure that those responsible for the applications for the network, in a lot of ways it's not different from an asset inventory system. You know what assets you have, you need to know what users you have. Building that takes time, just like an asset inventory does. It's a painful process to be honest with you.

KW: A lot of people are challenged. A lot of CISOs that we've interviewed for our magazine and in general conversation, identifying assets in applications is a big challenge for mid to large enterprise organizations. But the thing I wonder out of what I heard is when do you know or how do you know if your identity and access management program is at peak maturity? Since a component of it is the hard work in the weeds. How do you know when it's really matured from a process and an operationalization standpoint?

JM: I don't know if I would ever consider something like that mature. I really don't. As I said, there are resources in my team that are dedicated to constantly making sure that we identify and uncover those outliers. We have 14 different operations. We're a $7,000,000,000 company. Understanding what every operation does is super challenging. Even with the local teams. There are incidents you have to deal with. There are projects being rolled out. There's a whole litany of things that those teams are focused on other than identity. Finding the time to do that is always a challenge, which is one of the reasons it's centrally located, right? Making sure that there is a person and having the conviction to be able to defend that resource. Everybody has budget cuts, everybody is challenged with resourcing right now, but really having the conviction to make sure there's someone dedicated to doing that.

Tying things in, whether it's IP allocation, whether it's tying in with your network team to find new URLs that are being rolled out into your environment through DNS or whatever. There always seems to be a way to find the projects that kind of go around the process. That's where your bigger problem is, you can put the process in, you can be that monitor and say, "oh new application, new database, you're going to need users for that." Tracking, that's almost the easier part than the outliers. You get the emails going, "by the way, we just added this new URL. What do you want to do with it?" It's imperative to build those kinds of relationships. We're never going to be perfect. I've given up on being perfect many years ago. It's really about helping people understand and honestly, you're going to get to a point where people don't want to go around the process because it's more painful to go around it then it is to follow up. So hopefully we get to that point soon.

KW: In everything that has been covered in these last 20 minutes, what haven't we asked? What do people need to know? People in your position that maybe are just starting to enter into this conversation and this program? With a new set of rules, the perimeter gone, digital transformation accelerating, what haven't we asked or covered that they should really think about?

JM: Identity is more than just active directory. I think that's something that gets lost pretty quickly. I've seen some organizations brush their hands and go, hey we have AD and we're at that 50 or 60 percent mark and we're good. Really understanding your privileged accounts, if it's not the highest priority, it's probably just a step under it. That's the super critical aspect of it. Again, the bad guys can do some damage if they get a secretary's email account and send a spam for the whole company, but they really want that admin's account. They really want to understand and figure out how they can get elevated

privileges on those critical servers. So what are you doing about privilege? It's not one or the other. That's part of the maturity process, to be honest with you. I'm really trying to figure out how to tie privilege into the whole IAM solution. It's critical.

I would say don't forget about your cloud or AWS or Google environments. There's no real reason that they should be out of scope for any IAM project. Yes, it's a touch more complicated to make sure that they're under the guise of your IAM program. But it's not anything that's insurmountable. It takes a little bit of focus, a little bit of understanding, but it's just as critical as everything that's on the inside of your infrastructure. Lastly, I would say from a technology perspective, there's a lot of value in pulling those logs into your SIM, really wanting to understand what happens when someone hits that five or eight or 10 attempt limit, and after three or four attempts, they finally get in.

User behavior analytics is nice, but you need to start at a decent spot before they really provide the value. There are some very fundamental things that you can do from a pure log management side that can alert you to identities being either attacked or used inappropriately. So I would say don't overlook the simple things, if you go out and buy this big old tool, it's not necessarily going to solve those problems. You probably have plenty of data, plenty of logs and plenty of logic and your tools are ready to at least give you some heads up onto how your identities are being used or abused.

KP: That's good insight. So we have one last question for you, John. If you look into your personal crystal ball, how do you see the future of identity and access management evolving?

JM: Well, I hope it gets easier. That's for darn sure. We are building on 20 years, 30 years of eight-character passwords and all that other stuff. Seeing identities evolve into a common shared identity, the reality is, I don't necessarily want to add my third-party partners or consultants to my environment if I can't trust the environment they're coming from. How do we figure out how we can truly associate an identity to a person rather than a user? That's what I'm looking for because then we can do things like true real time adaptive authentication.

If my CEO is checking his email from Columbia one day and an hour later he's checking his email from Miami, something's wrong. That's the stuff I want to be able to find immediately. Being able to do adaptive authentication and really bringing AI or machine learning into doing some of that is where I think we're heading. I think people are getting wound about up being good enough right now and building some manual models. But that's where I see the industry going, really being able to pull all this together and give me that information about usage behavior in a real-world immediate response. If I look at what I want right now, if I have an admin logging in at 3:00 AM in the morning, I want to make sure it's them, whether it's from a ticket being punched or an alert being raised, it's out of the norm. I want to be able to react to that. I envision it's going there. There's a lot of excitement around some user behavior analytic vendors that are pushing in that direction, if they don't get sidetracked. So hopefully that's the way we'll see things evolve over the next three to five years.

KW: Well if there's one thing I know, vendors tend to get sidetracked, so hopefully that doesn't happen. John, if there's not anything else, we greatly appreciate your time today and your insight and for those of you listening, you can learn more about this episode and our other CISO interviews on our website, klogixsecurity.com\podcast.