PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

JOHN MASSERINI
CISO, MILLICOM

HEADQUARTERS: Luxembourg City, Luxembourg

EMPLOYEES: 18,000+

ANNUAL REVENUE: $6 Billion

Three-time CISO John Masserini brings in-depth experience through extensive work in all facets of information security for over twenty-four years. Throughout his career, Masserini experienced the rapid transition and impactful evolution of the role of security leadership within organizations.

He comments, “Historically, security was considered a technology problem. In some enterprises, it is still that way today. In my view, it’s about managing the risks and making sure there are strategies in place that find the spot between balancing technology risk, protecting our sensitive information, and continuing to help the business drive revenue. While my background is very technology-centric, most of my days are spent evangelizing and ensuring both business and technical risks are mitigated in the best possible way to protect our subscribers’ information and support the company’s strategic revenue objectives. At Millicom, we’ve taken the unique approach of moving the security and risk function into the Compliance and Ethics group, rather than have a direct line into the technology group. This provides a separation of duties that is often lost when CISOs report to CIOs.”

DEVISING A GLOBAL STRATEGY

The desire to come into an organization and implement a strong global strategy sparked Masserini’s interest in joining Millicom, a leading provider of cable and mobile services dedicated to emerging markets with more than 51 million customers across the globe. While each individual country has Information Security Officers in place, the organization recognized the lack of a cohesive, globally-driven security strategy. Masserini explains, “The ability to come into a place and pull together all the experts throughout the company and build a cohesive strategy was incredibly intriguing, and ultimately why I decided to join.”

He continues, “We have country operations throughout Latin America and Africa as well as back office operations in Luxembourg, London, and Miami. Each operation has different risks which they have to deal with, both from a technology perspective and from a business continuity perspective. To pull all those together and come up with a standard strategy is something that is certainly challenging, but exciting at the same time.”

Not only is establishing a strategy important, but strong intra-communication is a vital component of linking the global operations. Masserini acknowledged the importance of instilling this in his 18-month plan. He comments, “It is really about leveraging the collective experience. It is about building a communication infrastructure where we can all share ideas, experiences, and what works and what doesn’t. By being able to share awareness materials, attack and compromise signatures, third-party risk assessments, or even job descriptions, we can better utilize the existing teams to manage the evolving risk. This same approach applies just as well to

the technology side– whether it's a shared Identity Access solution or a global Security Operations Center. The goal is to leverage the best of what we already have rather than reinventing each time. That's really driving the next 18-36 months from now."

BOARDROOM BALANCING ACT

"Our executives truly feel that security is critical to the future of our success; it's something we need to not just focus on, but it needs to be part of our culture," says Masserini. Having strong support behind continuing to improve and grow information security enables Masserini and his team to set clear goals and report back on progress.

When presenting to the board, Masserini believes presentations and conversations must revolve around business risk in terms of risk management and mitigation. He typically avoids talk about specific technology products or technical alerts. He explains, "It's all about understanding risk and being able to articulate that risk to the board and to the audit committee. It's not a discussion about the technology, it's about translating the risk into what your audience cares about and the perspective they have. They want to understand the risk to our customers, a revenue stream, or the corporate reputation, regardless of the source. It doesn't matter if it's a vulnerable application, a DDoS risk, or the potential of a fire in the data center. If there is a potential of a revenue impacting event, they need to understand the potential loss and the probability of that loss occurring. They don't care how we found it, they want to understand what they can do to fix it."

Masserini advises other CISOs to approach board meetings like a balancing act. You must understand the board's perspective and keep that in mind when you are presenting or answering questions. CISOs must hit on the big items without going into technical detail to ensure a successful and productive meeting, regardless of the length of time they have to present.

TRANSFORMATION WITH THE CLOUD

A personal goal of Masserini was to work at an organization that recognized the value and importance of the cloud. It was clear to him that Millicom readily adopted the cloud, and is undergoing a transformative period that Masserini plays a key role in.

He says, "With the cloud, we can provide a common platform to all of the country operations without provisioning hardware and data center space in each location. Obviously, there are some inherent risks, but those risks are what we're working on right now. We are slowly plowing through and addressing them and making sure that we're protected contractually, protected on an insurance basis, and then protected from a technology perspective. I love how cutting edge this company is, they have very focused approaches or ideas on how we can mitigate risks without the typical, 'I would just make this password stronger' or 'throw some sort of device in'."

HOLISTIC APPROACH TO REGULATIONS

The main business lines for Millicom are in Latin America and Africa, with each country requiring specific regulations, like those of General Data Protection Regulation (GDPR). Masserini and his team are part of a corporate-wide effort, working with the Legal and External Affairs teams, to satisfy GDPR and other global requirements to adhere to the vast majority of regulations in all of their operating countries.

He explains, "Fulfilling GDPR is coming from a global perspective and not just from a local view, but there are also other things to consider. It's about building the strategy that satisfies all the different global requirements that we have. It's not just GDPR, it's a privacy and data protection program that in some ways goes further than GDPR and in some ways, is a bit more specific than GDPR requires. The idea was to build the holistic strategy, not one that's just interested in one regulation."

PERSONAL GROWTH

> "One of the most beneficial things I do from a career perspective is find ways to "peer review" projects, approaches, or initiatives. Before moving to Miami, there was a regular group of New York City CISOs who would get together for dinner where someone would present a topic or project "Chatham House Rule" style. Frank, open dialog with an understanding of total confidentiality. It's wonderfully courteous and completely professional, but make no mistake, you get grilled. It's a baptism by fire at its finest. That said, the experience leads you to understand that your perception is different than others, and what may be clear to you is something someone else may not understand. It is extremely humbling, and incredibly valuable to personal growth, especially if you're new to the CISO role or when you're dealing with a new Board."