ROBERT MICILLO

CISO
MetroPlusHealth

HEADQUARTERS: New York, NY

EMPLOYEES: 1,500

REVENUE: $3.7 Billion

Robert Micillo has over twenty years of experience working in the healthcare industry, which prepared him well for his role at MetroPlusHealth providing quality, affordable health insurance benefits to over 625,000 New Yorkers. He says, “When I was being interviewed, it was apparent that although they had security measures in place, they needed someone who could come in to create and implement a more comprehensive security program that met all the new, emerging regulations. It became a very natural conversation as I was able to map out for them a security program that fit their needs.”

Micillo’s core responsibility when joining MetroPlusHealth was to define an information security program in order to reduce risk, protect the organization, meet regulatory requirements, and safeguard membership data. By establishing a strong, comprehensive approach to security, he ensured goals would be met and the organization would be positively impacted by the growth of the security program. Initially, Micillo completed a risk-based assessment of their current security posture and tools, worked to rewrite their policies, completed a staff assessment to map out the positions and requirements to put together a team, and defined and delineated roles between information security and technology support.

His goal from the onset was to provide the necessary means to protect the assets and data, while maintaining operational efficiencies. He explains, “The MetroPlusHealth Cybersecurity program must strike the right amount of security measures to protect customer privacy and our assets while ensuring operational efficiencies for our business units. It’s kind of a balancing act, because I can add security measures that can lock down things so tightly that we start losing operational efficiency and vice versa. We may gain so much operational efficiency that we lose track of maintaining and securing our digital assets. So, I find it to be a true balancing act, and we do it fairly well.”

CORE RESPONSIBILITIES

Micillo has six program areas covered by his department – security operations, risk management, security awareness and training, business continuity, policy and governance, and security architecting and engineering.

Security Operations – The security operations team focuses on having 24/7 visibility. Micillo says, “We’re pulling in as many raw logs as we can from as many sources as we are able to, to identify anomalies, to identify brute force attacks, to recognize whether what we’re seeing is real, or an anomaly, acceptable and expected behavior or a false positive.”

Risk Management – He explains, “From a risk management perspective we’re monitoring and assessing technical and

operational risk regularly. We're currently focusing on, and this is very important, evaluating and measuring third-party risk. We share our data with a lot of business associates out there, and we are able to do some degree of due diligence and monitoring on what those third parties do for us, how they handle our data, and what the propensity of their security program looks like. We want to identify if they maintain a strong, medium, or low security posture over time through increased visibility into their security practices." This is an area of focused concentration in the third-party risk management roadmap for the organization.

Security Awareness and Training – Micillo and his team focus on security awareness and education across the MetroPlusHealth staff in order to minimize risk. He acknowledges that their employees are the first line of defense in many cases and an integral part of maintaining good security habits. Ultimately Micillo acknowledges they are only as strong as their weakest behavior and therefore allocate ample resources on training and education, and provide employees with a simple and easy way to report suspicious activity.

Business Continuity – They have a comprehensive business continuity program where they work with the organization's units to identify their tolerance levels. Micillo continues, "Depending on the interruption of business, we want to identify what the next best move would be and how it would be triggered. And we put all those plans together for the departments as a whole. I have a dedicated team who gathers that intelligence and understands the RTO and RPO requirements behind what their needs are to maintain business and keep the wheels of motion going."

Policy and Governance – Micillo comments, "It's always my goal to separate policies from procedure. Procedures can contain steps that may change rapidly based on new standards while policies should not change that quickly or easily, and should be amended based on requirements from regulator and compliance sources. So there's a lot of work that goes into policy development. And the key to good policy is obviously one that employees can understand and meet. We strive to ensure that our policies are meeting compliance, are comprehensible, achievable and that they're not so stringent that we cannot comply with them."

Security Architecture & Engineering – Security team members are dedicated to innovative initiatives taking place within the organization to make sure they are secure. Robert says, "API management is a very hot topic right now as we're going through a lot of transformation, and that requires a specific technical strength that I don't find in every engineer that I run across. That onto itself is a very important piece of the puzzle here."

TRANSPARENCY WITH EXECUTIVES TO JUSTIFY BUDGET

"I think that the most important thing that I've done is to provide the executive team complete transparency. I don't sugarcoat anything. I'm a very transparent person. I want to be completely clear on where we are today, relative to where we need to be, and what some of the dangers are by not addressing specific areas of concern. The aim is to reduce risk to an acceptable level to prevent a breach, so when presenting cost benefit analysis it is often weighed against the cost of breach potential. When you talk about a breach, we need to be cognizant of several things that people don't easily see. Reputational damage within the industry and fines are top of mind, but what you may not recognize are the costs involved well beyond the framework of government fines. There are residual mitigation costs and consider public confidence—the minute you lose public confidence, you're losing membership," says Micillo.

He believes in bringing these important issues to the forefront because if you are not able to make them apparent, budget decision makers may not express buy-in with your decisioning. When he first started, Micillo outlined 30-to-40 initiatives he believed the security program needed to accomplish within one year, something which is often unprecedented in the security realm, especially with compliance requirements and regulations that drive organizational decisions.

He explains, "I came in with a plan. If you don't have a plan to create a program that can identify all of these things, I think it becomes that much more difficult to justify the funding. I think that I was able to accomplish it. I was very fortunate because I really understand the business and the dilemma that MetroPlusHealth was facing at the time. And the stars aligned from that perspective that I was in the right place at the right time for the right situation. And I'll tell you, I think that we have an extraordinarily strong program. I know for a fact that the Board of Directors and the CEO are extremely proud of what we've accomplished. I've only been with MetroPlusHealth since 2017 and that's not a long time to put something together that is this formidable and I'm very proud of it."