PROFILES IN *Confidence*

DIEGO SOUZA

GLOBAL CISO
CUMMINS, INC.

HEADQUARTERS: Columbus, Indiana

EMPLOYEES: 60,000+

REVENUE: $24 Billion

Diego Souza is currently the Global CISO for Cummins, Inc., an American multinational corporation that designs, manufactures, and distributes engines, filtration, and power generation products and is a leader in the development of clean technologies in the industry like electrified powertrains and hydrogen fuel cell solutions. As a strategic thought leader, Diego focuses on being a business enabler and strong communicator to increase security maturity and continually reduce risk. In taking the role at Cummins, Inc., Diego had an opportunity to strengthen the security program by strictly aligning with business-driven priorities. He says security is part of the organization's DNA and the cyber opportunities in place set the stage for him to help grow the business.

BUSINESS ENABLERS

Diego believes CISOs must understand that cybersecurity should not be a function that sits in the corner of the IT organization. He says security teams and their leaders must be true business enablers who discuss cyber in terms of business risk. He explains, "When we are able to communicate business risk to the board and C-level executives, they are able to see value and why cyber is an important part of the entire organization. Everybody talks about shifting to the left and bringing cybersecurity to the front. I believe cyber should be included from the beginning all the way to the end of the lifecycle. Today we have product needs, compliance needs and regulatory needs and because there are so many different phases of every single program, cyber needs to be included across the lifecycle."

He continues, "It is important to make sure senior leadership from the CEO and C-levels to the Board of Directors, understand why cybersecurity is important to the organization, not only from a response team perspective, but as a business enabler. When organizations are designing, developing, and building assume board members don't understand cyber, however it is usually not the case because executives are becoming more security savvy. He says to prepare for questions that tie back to business and operational impact. Often times, board members ask about breaches they read about in the news and if a similar incident could happen at their organization. While these discussions may pose a challenge for some security leaders, Diego believes if you focus on communicating in a way that is understandable and relatable to the board, you will build strong relationships.

BATTLEFIELD APPROACH

To enhance the visibility of his organization from a cyber standpoint, Diego says they have a battlefield approach which includes the pre, per, post, and when cyber instance.

> **"It is important to make sure senior leadership from the CEO and C-levels to the Board of Directors, understand why cybersecurity is important to the organization, not only from a response team perspective, but as a business enabler."**

He explains, “There are four phases of our cyber instances - the pre, the per, the post and the when. Out of the four, three of them we can control, but we cannot control the when. We can control the pre, per, and post. The pre is underlining infrastructure visibility, making sure we have all the necessary processes in place to be more predictive about cyber events so we can take proactive actions versus reactive ones. We are focused on moving to a predictive, proactive organization, leveraging AI capabilities, leveraging behavior solutions that can help us to predict potential incidents. The per is our ability to respond as quick as possible. The post is really making sure that we learn from events and how we fix the whole process so it doesn’t happen again.”

Diego says he never promises that an organization he works at will never get compromised, but he does tell leadership that if it does happen, they will be ready to respond as quickly as possible to minimize business impact.

ASSESSING RISK

To truly assess risk, Diego says you must start with understanding your environment and the business goals in place. First is classifying risk through a framework like NIST to evaluate the controls in place. Then is prioritizing those risks. Diego comments, “We do self-assessments to assess risk that provide us a cybersecurity score to see where we are from the traditional one to five. Self-assessments are typically conducted to monitor where we are from a maturity and risk perspective. We also bring external parties in to provide a different evaluation of our security program. They tell us where they are seeing gaps, and which areas to focus on.”

Diego says it is important to focus on the bigger risks first, especially those that impact the company from a financial or operational perspective. These might even include risks that could potentially impact the overall brand and its reputation.

Quantifying risk is vital for Diego to run a successful security program because it enables you to demonstrate direct business impact. For example, if a system goes down for a certain number of hours, the impact to the manufacturing line will be a specific dollar amount in lost revenue. He explains, “Quantifying risk helps us measure risk from the business side and drive that message back to the C-levels of the company. However, sometimes you cannot quantify risk, so you must qualify it. For instance, a potential branding impact. If a cyber incident happens at your organization and it becomes part of a news cycle, it might impact your stock price. You can’t quantify how much the stock will drop but you need to understand the impact to your business if that happens.”

> “I really focus on people. I make sure I invest in them and have open communication in my organization. There is no hierarchy from a relationship standpoint, I have an open door approach with my entire team, so they can get time with me to discuss anything.”

GROWTH

Diego classifies himself as a people-centric leader. He explains, “I really focus on people. I make sure I invest in them and have open communication in my organization. There is no hierarchy from a relationship standpoint, I have an open door approach with my entire team, so they can get time with me to discuss anything. They have reporting lines, however, they have the freedom to talk with me at any time, and I feel that building up those relationships creates a much healthier environment and people want to stay. Especially in today’s market that’s so hot for cybersecurity professionals. I joined this organization because I knew my team would be equipped with the necessary tools, knowledge and processes to execute their day-to-day work.”

To continue to grow as a leader, Diego says he focuses on being a good listener. He listens to what his team tells him and what his stakeholders tell him so he can learn and improve. He is also very engaged in the security community. Conferences are a great way for Diego to meet with peers and share information with one another, whether it is current challenges they are facing or tools they are investing in, it all helps improve the overall maturity of security.