CARLOS CONG

DEPUTY CISO
PAYCHEX

HEADQUARTERS: Rochester, NY

EMPLOYEES: 16,000+

REVENUE: $4.61 Billion

PROFILES IN Confidence

Carlos Cong has worked in technology for over 20 years and always been passionate about security because of the great responsibility in protecting data and availability for organizations. As part of his charge in his current role as Director of Enterprise Security at Paychex, Carlos helps protect the $4 billion company with over 700,000 customers across the globe. He says he wakes up everyday energized to tackle new risks and concerns on the horizon, mainly because he is able to work with an incredible team of talented people.

Carlos came to Paychex over ten years ago and instantly knew he would enjoy working here because he was surrounded by passionate, like-minded individuals. Over the last ten years he has had opportunities to work across technology roles, which naturally progressed into his current role working on the security side of the business. Looking back over his tenure so far at the organization, Carlos says it is exciting to see how much his work has helped modernize their environment, everything from the data center to the network, security, and beyond.

He comments, “Right now I directly oversee the Cyber Fusion Center, which includes security intelligence, detection, hunting, insider threat security, incident response, digital forensics, security assessment of vulnerability management, application security, the 24x7 security operations center, and our cyber awareness and response management program. I also serve as a Deputy CISO, Chief of Staff for our CISO, so I help to lead the security engineering, program management, and risk and compliance pillars as well within the organization.”

He continues, “I’ve been working full time in security for a little over one year. Even though I’ve been at Paychex for ten years, I haven’t been in security the entire time. When I first came to Paychex, I was on the Enterprise Technology Services team, which included a very close partnership with security, leading security initiatives lockstep with the team, and driving new technology innovation in all types of different areas. When I officially led security, I had a good grasp on the various pillars within security, but there was a lot of learning to be done and I had to spend a good six months doing a lot of research, talking to colleagues, working with my team and truly getting grounded and understanding all the various pillars, the feedback loops, the frameworks that we needed to put in place in order to scale. We’ve been hard at work doing that since.”

FOCUS AREAS – THREATS, AI, PREVENTION

Like most security practitioners, Carlos says he is focused on addressing threats in proactive and efficient ways. He explains, “Things like ransomware, data exfiltration, prevention and response are definitely always top of mind. Plus we are focused on our ability to rapidly respond to zero-day vulnerabilities and just general vulnerabilities in the environment. There’s a series of different strategies that we have out there.”

> *“AI comes with innovation and opportunity, but it’s so early on in its creation that you don’t know how the adversaries are going to take something that was meant to propel society forward, and potentially weaponize it. And we already see evidence of that.”*

From an AI perspective, Carlos considers it an emerging risk. He comments, “AI comes with innovation and opportunity, but it’s so early on in its creation that you don’t know how the adversaries are going to take something that was meant to propel society forward, and potentially weaponize it. And we already see evidence of that. You read articles about how ChatGPT and others could develop malware in them. Intellectual property is getting lost. We’re doing a lot of research. We’re working with various industry partners to see exactly how this is going to apply to Paychex from an AI perspective.”

He continues, “In the prevention bucket, there are several different things that we’re hyper-focused on, obviously identity management, zero trust, and least privilege access. Everything from the end user all the way through our workloads and applications, making sure the environment is appropriately segmented, making sure we have the appropriate detections and controls in place to prevent not only the spray and pray bad actors, but also the more mature sophisticated ones that like to slow crawl in your environment. Tactics being used are becoming more and more difficult to detect and we have to stay ahead of those things faster. Weaponization is happening daily, and we must have a processing framework in place to keep up with all these different tactics and techniques, and we have a good practice around that. Because we’re continuously doing intelligence gathering and seeing how things out there in the wild apply to our environment, it’s a continuous cycle, and it’s never ending. I don’t anticipate it to slow down. In fact, I anticipate it to speed up, and that’s really what we’re preparing for.”

EXECUTIVE SUPPORT & SERVANT LEADERSHIP

Having executive support is important to Carlos, and he says his team is fortunate to have an executive team that is fully supportive of their program. He explains, “We have the full backing of the organization when it comes down to needing to address certain risks that we have, even including our legal teams. So, it’s really a true company effort, but we have our challenges too, just like the rest of the world. Everybody has budget pressures and there are decisions that we all have to make. The good news about having a risk priority is that we know where our ‘true norths’ are, and it makes it so much easier to speak with the data and prioritize things.”

“We have the full backing of the organization when it comes down to needing to address certain risks that we have, even including our legal teams. So, it’s really a true company effort, but we have our challenges too, just like the rest of the world.”

Carlos considers himself a servant leader. He comments, “I have a few core things that are principles in mind that my team is very well familiar with. Things like doing what’s best for the business, customer or employee, those should always inform our approach from the front. Another focus is to always advocate for your team and carry the flag for security. Step up and step in. Basically, meaning if there’s a time and a place where you feel like the team is struggling in any way, we should be able to step in and assist and provide whatever knowledge or inputs is needed at the time, and then pull up and push out is more about advocating for your employees. Just making sure that you’re aware of their career goals and aspirations, and then helping them navigate how to achieve them. And that goes back to our career journey framework that allows employees to really navigate and map out exactly what the opportunities are within security and then how to get there.”

To continue and grow as a leader Carlos takes advantage of professional development opportunities. He also learns from his executive management, taking their feedback and engaging with them on a regular basis. He continues, “Industry peers are important to learn from as well, especially taking feedback from them. It’s key for me to make sure I’m showing up the right way, continuously learning, doing a lot of reading in terms of research in the space and just keeping abreast of what’s new and what’s emerging. So, there’s a variety of things that I try to do to continuously develop because it’s incredibly important. I don’t like to ever feel like I’m stagnant in any way because if I am then that means the organization isn’t moving the way that it could or should.”