PROFILES IN *Confidence*

JESSICA SICA

HEAD OF SECURITY
WEAVE

HEADQUARTERS: Lehi, Utah

EMPLOYEES: 800+

REVENUE: $142.1 Million (as of December 2022)

Jessica Sica did not follow the typical track of most CISOs, she went to college for broadcasting, did not finish her four-year degree until two years ago, and gained her security skills through hands-on experience. She used her innate skills for security, knack for problem solving, and natural leadership skills, to become the successful security leader she is today.

Her interest in security piqued early in her career as a network engineer working on firewall projects. After seeing the impact and importance of security, she began to transition into security-focused roles. Since then, her career has spanned many titles and industries, giving her a broad array of expertise and skills. After growing into more leadership roles with added responsibility, she realized she wanted to continue on this trajectory. She explains, "About 10 years ago I started to realize that my path involved leadership and working my way up the leadership ladder. I worked as a manager, director and then got my first CISO role, as CISO of Petco."

After working as CISO at Petco and gaining a vast amount of experience leading a team, aligning with the business and maturing the security program, Jessica had an opportunity to join Weave, a growing company offering a software platform that brings together phone systems and a suite of communication tools. Jessica comments, "Weave was a challenge to me because they're a growing company coming out of a start-up phase, and they needed somebody to come in and help direct and lead the security program. They had a strong baseline in place which was fantastic. I didn't really have to start from scratch, I had an opportunity to evolve and bring them out of a startup phase into a big growing company. It was really appealing to me, especially the culture they have. A lot of companies preach their own cultures, but Weave really does it. Having been here going on nine months, I can confirm that Weave definitely puts employees first, and really cares about who's working there, which is pretty valuable in a company."

GROWING A SECURITY PROGRAM

Jessica spent her first month at Weave meeting other key business leaders and better understanding their position on security to figure out their concerns around risk. By doing this, she assessed where the business is willing, and not willing, to accept risk. She was able to gain a vision of what the security culture is like at the organization and continue to build relationships with her business counterparts. It was important to Jessica that this was done before she began working on her move-forward strategy and roadmap, because without understanding how the business operates and clearly defining risk levels, her program would not be set up for success. She explains, "It's really important to understand the security culture at a company when you come in before you do anything. A lot of times, companies want you to make a 30-60-90 day plan, but you can't start that plan for a few months because you have to understand what the companies sense of risk is and what they're willing to do, or not do, before you can start making your

"A lot of companies preach their own cultures, but Weave really does it. Having been here going on nine months, I can confirm that Weave definitely puts employees first, and really cares about who's working there, which is pretty valuable in a company."

plan about where to go and how to mature the program."

One of the initial focus areas was aligning the company with the NIST CSF security framework to ensure they identify any gaps and determine areas of strength. This involved laying a lot of groundwork, ensuring certain processes were established, and gaining a clear picture into the overall security plan. She was then be able to solidify a two-to-three-year plan and identify key initiatives to mature the organization as the business continues to follow their growth plans. Not only does she need to ensure her team is on board, but she must educate executives and relevant boards to gain buy-in and track progress. She explains, "We've identified opportunities for improvement that we're going to try to capitalize on with some spend in 2024. But a lot of our focus is on maturing processes, company security culture, and continuing things like regular training and phishing."

When investing in new tools, Jessica believes in smart, strategic spending, and ensuring there is direct alignment with specific needs of the security program to ensure no budget is wasted. She says, "When investing in a tool, you must understand what risk is it really protecting you against? And can you measure the success of that risk once you put this tool in place to show the effectiveness of it? Because the board and audit committee really like to see what security is doing and if what you're spending is actually helping. And if you buy something and you don't have a way to show if it's helping or not, you're going to have a difficult time justifying that purchase and justifying future budget."

With a multitude of vendors in the security marketspace, Jessica believes it is important to lean on your network to ask for referrals and learn through other security leaders' experiences. She also says establishing trust with a vendor is key, their marketing message must match what their product actually offers because there are no silver bullets in security. It is important to genuinely understand your challenge and what you need from a vendor to address it.

AI, THIRD PARTY RISK, AND PASSWORDLESS SECURITY

Jessica attends conferences and meets with security groups to continue to grow and learn. Recently, she says Artificial Intelligence (AI), third and fourth party risk, and passwordless security are top conversation topics.

She says AI is going to change the tech world, especially altering the way security is approached. She comments, "AI is getting really good at fooling people with images, videos, and phishing campaigns. It's not quite there yet, but it's going to get there. And I think it's going to make it easier to trick your employees. So, you're going to need better training. You're going to be better awareness. You're going to need better safety rules in place because your employees might fall more victim to this kind of stuff. Hopefully there are security companies that will help detect AI and prevent AI phishing and things like that. The security industry needs to keep up with that as well."

Third and fourth party risk continues to be a focus area for many security professionals according to Jessica. She explains, "I don't think most companies do it well. It's hard because you have to put a lot of resources into it. Companies use many vendors, and these vendors use vendors and it's difficult to button up that risk 100% all of the time, so I don't think that problem is going away anytime soon."

Another area of discussion is around passwords, Jessica states, "They've been saying passwords are dead for a long time, and they're really going to be in the next couple of years. I think companies need to start moving away from that or there's going to be a problem in the future."

LEADERSHIP STYLE

Taking a relatively hands-off approach to leadership while still being a coach has boded well for Jessica in her sizable experience leading effective teams. She explains, "I want to find ways to help my team grow. I think it's important as a leader to help your employees grow if that's what they want to do, even if it means that ultimately they're going to grow out of that position or out of that company. Not everybody stays at the company they're at for various different reasons, and that's okay. If somebody grows and gets promoted and gets smarter than they were before and they move on to another company, that says a lot about what that company has to offer that got them there."

She continues, "I also believe it's important to have a hands-off approach in the sense that you know you're generally working with pretty mature people in the field. And you trust that they're going to get their work done and that they know what they're doing. And if they're not, then they're probably not the right person for the job anyway. I'm not a micromanager, I believe in letting people get the work done. I think their work speaks for itself and the results speak for themselves. And I think you can manage a remote workforce; you don't need butts in seats to make sure that the job is done. You don't need to see that; you need to see results and that's what is most important. If results are getting done and your security program is advancing and your security team is growing, then you're being a successful leader."