PROFILES IN *Confidence*

MATTHEW MUDRY

CISO
HOMESERVE NORTH AMERICA

HEADQUARTERS: Norwalk, CT (US Headquarters)

EMPLOYEES: 2,500+

REVENUE: $800 Million

Matthew Mudry's interest in technology began at an early age when he started physically building computers, and modifying how the operating systems and applications behaved, to better understand their limits and capabilities. Over time this interest shifted from a hobby into a prosperous career. Today, with over twenty years' experience in IT and security, Matthew continues to be deeply passionate about his work.

Early in his career, Matthew worked in areas such as desktop support engineering, server/storage support, and networking. Matthew's most recent work includes six years at Castleton Commodities International as Vice President of IT Architecture and Security. He helped build a successful security team/program from the ground up, implementing many new technologies and numerous processes and procedures to maintain a safe and secure environment. During this role, Matthew initially oversaw the infrastructure side, with security being a component of that, but the CIO at the time said they were separating infrastructure and building a security team, and asked Matthew to choose which side he would prefer to work on. Matthew explains, "This was about twelve years ago, and without much hesitation, I told him I wanted to switch over to security because I felt it was the right time and I wanted to grow my knowledge in that space. I was excited to go down the security road and that's where my career in security really took off."

Matthew then moved to CareCentix for two years as the Vice President of Information Security. Here, he provided oversight and leadership for both security and networking and was responsible for evolving and maintaining the program, while maintaining HIPAA compliance and working towards and eventually achieving HITRUST certification.

Matthew is currently the CISO at the North American arm of HomeServe, a global provider of home repair and installation services with 4.6 million customers across the US and Canada. He is responsible for the confidentially, integrity and availability of the global systems, the accompanying data and the overall safety of the personnel. His responsibilities include maintaining PCI compliance, continuous improvement to the security posture and integration with newly acquired entities into the business/network.

FOCUSING ON THE CLOUD

As most businesses continue to transform, Matthew's work at HomeServe addresses this trend as they shift to the cloud. He comments, "When it comes to cloud my focus is on securing the data and the systems within it, without jeopardizing its functionality, performance or purpose. The shift to cloud has significantly altered the landscape and changed the way many individuals and businesses approach security. We went from building a number of fortresses, with many layers of security, where all our systems and data sat behind, to securing each individual application and/or creating many smaller secured bubbles so information can be accessed seamlessly and securely from anywhere in the world. The challenge is always around achieving the same level of security, or better, in the cloud without adding too much complexity or impacting its ability to function as expected."

Matthew's approach is to focus more on the endpoint because there are limited protected networks when moving to the cloud. He explains, "To protect your assets, or your crown jewels, whether it's PII, PCI, or other sensitive data, it is important to monitor and manage the endpoint with the least

"When it comes to cloud my focus is on securing the data and the systems within it, without jeopardizing its functionality, performance or purpose. The shift to cloud has significantly altered the landscape and changed the way many individuals and businesses approach security."

amount of impact. Previously you had firewalls, and intrusion detection/prevention systems, network detection and response (NDR) solutions, where you monitor the traffic traversing between the endpoint and your applications/systems, whereas now you need an agent on the endpoint to do all these things. In my mind, it's finding not one product that does it all, but it's finding a few complimentary agents that can solve all these problems."

API security poses a challenge for Matthew because he says with so many different cloud solutions in place, there are often APIs hooking into them, all coming from various locations. He says, "Once in a while you might get an alert, or find a rogue API connection, that was configured by an application owner or system administrator but didn't go through all the necessary channels. Therefore, while we've validated it is in place for legitimate business purposes, it is missing the necessary restrictions or limitations it should have potentially causing harm. Getting our arms around APIs and where they're being leveraged and used, is a bigger problem than actually securing the APIs themselves."

CONNECTING WITH THE BUSINESS

To achieve a strong connection with the business, Matthew believes in always assessing the risk, coming in with a plan, and ensuring you execute and maintain that plan while remaining aligned to the businesses goals and objectives. He says, "You must have a plan and instill a mindset with your leadership that you are going to do things that are in the best interest of the business and address the areas of the most significant risk first. You must also show leadership exactly why security is important. The plan should include what you've identified as a weakness or risk, how you plan to fix it, and how much money or resources it will require."

Matthew says when coming into a new organization, CISOs need to get in front of each business unit and have productive conversations to understand their line of work, goals, and challenges. He explains, "Sometimes it takes working from the bottom up. Getting ahold of the underlying leadership team in the right way. Not the C-level, but the other people that run the organization and the infrastructure or the application heads and start building processes out that are required."

To effectively communicate with the business, Matthew advises ensuring you have a seat at the table, whether it is with C-levels, other executives, or the board. This could mean scheduling 30-minute meetings to get in front of them and have proactive conversations. Before meetings, Matthew recommends being prepared and tailoring the conversation to your exact audience. He comments, "Understand where your risks are from a business and security perspective. Then take the next step and identify how that impacts your business. Identify what your business is truly trying to protect – is it the brand? Is it the data? Is it the systems? What is it that the business trying to protect? And then pull all that together. Before you even set up a call with the executive team, come up with solutions and say this is where I find the areas of biggest business risk and this is how we are going to address it through avoidance, mitigation acceptance and/or transferal. "

LEADING BY EXAMPLE

"I'm a big fan of team-ship, I need people who are passionate about security, but also I need my team talking, having fun and trusting one another. Most, if not all decisions are made as a team, so that they feel and know their input is valued. I truly feel effective teams disagree with one another from time to time and having a culture that embraces this difference of opinion and encourages respectful debate is extremely important and healthy. That's when great decisions are made. I'm very much against micromanagement and I try to have an open, honest and transparent leadership style. Always being present/available and having regular touchpoints with each team member is critical to make sure they know exactly how well they are performing, so there are no surprises come review time. And if/when they knock it out of the park, I truly enjoy being able to reward them for a job/task well done. A true leader takes pride in the accomplishments and successes of their team members and motivates them to continually better themselves and strive for greatness/perfection, while being empathetic and compassionate during the difficult or trying times."