GREG KYRYTSCHENKO

DEPUTY CISO
Guardian Life

HEADQUARTERS: New York, NY

EMPLOYEES: 9,500 employees + 2,700 financial representatives

REVENUE: $1.9 Billion

Greg Kyrytschenko has worked in IT and security roles for over twenty years, giving him broad exposure to every facet of the business. He comments, “I became interested in security over twenty years ago. I remember watching certain movies and solving certain problems and thinking it would be a cool career to protect networks, computers, & software. When I started, the field was very immature, people knew you had to protect computers, but no one really knew how to protect them. I began my career in IT right out of college working in credit card fraud business and solving the types of problems was very interesting to me.”

Greg has remained in the security field because it offers him the ability to continually learn and challenge himself. He explains, “My philosophy is that I always ask myself how can I make things better than when I found it, and it’s always been a mission statement for me my personal brand and character within the security field. Focusing on this as my principal compass helps me strive to build great things for the companies I’ve worked at as well as create a positive impact for the people I have the opportunity to work with.”

Greg believes security should be an enabler and not an inhibitor. He reveals, “Security is not a place of yes or no, it’s meant to be my operating approach in my partnership with the business. Security should help an organization get to where they want to be providing guardrails which allows for business velocity and insight into helping to protect from cyber threat actors.” He continually focuses on that approach in order to set proactive realistic tones between security and the business that lead to trust, collaboration, and partnership. To achieve positive outcomes he ensures to meet regularly with stakeholders to establish two-way dialog between teams.

FOCUS ON SECURITY AWARENESS

Greg runs the cybersecurity function from an operations and engineering perspective. His duties range from managing internal and external risks to running parts of the security awareness program and everything in between.

According to Greg, a strong security culture is paramount to an organization’s cyber resiliency. He explains, “Training and awareness gets people attuned to what threat actors are doing. The stronger you make the workforce, the stronger you make your organization. I believe in things like security champion programs where people help promote security awareness across the organization. They have their eyes and ears open for things that attackers may be attempting to do. It is important to make sure you have a feedback loop so that information gets back to you and your program, so you can continue to improve over time.”

He believes it takes changing the organization's culture to become more security-focused to help improve security posture. He considers regular and targeted communication as a core way to spread the mission of security, so everyone becomes invested in helping protect the organization and the workforce feels it is their duty to help protect it. Greg also believes in ensuring someone within security should help to market a company's trustworthiness to the lines of business. Building a security-minded culture is not easy and takes thoughtful planning along with strong communication and interpersonal skills. By showcasing how security protects the organization and positively impacts business outcomes, you are able to enable the business on security-related initiatives. Greg says this approach helps result in a stronger overall security posture.

THREAT ALERTS AND GOOD CYBER HYGIENE

"I always ensure stakeholders and executives are informed on threat actor motives and tactics so they have awareness for what is going on in the world and how it may impact the organization. Security should help shepherd stakeholders and executives so they can make the right decisions and judgement calls with regards to threats. To be impactful, it is all about being able to simplify and not go into the weeds. I leverage current events and simplify the facts by being a good storyteller to keep their attention focused on what's most important," comments Greg. With security constantly in the news, Greg and his team must translate those threats and how they may or may not impact the organization. Not only does security need to address current threats, but they must work hard to stay a step ahead and be proactive for what could possibly come next.

By sharing information on a regular basis, employees stay aware of current risks, and in turn, each individual department is able to make better informed decisions around their specific risk tolerance. Greg says the more impactful information you provide around risks, the better decision outcome can be made. He continues, "As we partner with people across the business and talk to them about the cyber threat landscape and different types of potential attacks, security hygiene basics must be leveraged to create a stronger defense. Just like with fitness, if you are consistent then you will live a long healthy life. Security is the same, if you continue to do the basics with good security hygiene you are setting yourself up for life-time resilience and grit to handle cyber threats. You also need to use innovation and transformation to implement strong security practices that make it transparent to end-users."

CLOUD AND SECURE ACCESS SERVICE EDGE (SASE)

With cloud security top of mind for many security professionals, Greg says investing time and resources into understanding the technology and business problems helps to implement stronger effective controls in the cloud.

For Greg, key drivers for moving toward a cloud architecture include scale, availability, and standardization in a distributed environment as many organizations move toward a hybrid work environment in the new post-covid world. He says, "You have to now plan for where people are working from (remote, off site, in-office), set up control posturing machines and make sure the computers connecting into the environment meet the standards that the organization establishes. It's important to cover how to control different aspects of cyberattack techniques which could be leveraged by insiders or external bad actors. You also must have the right levels of access, logging, and configuration management to establish cyber resilience in a remote environment."

Since achieving SASE involves networking and security teams working closely together, Greg believes in partnering as soon as possible for major initiatives to make sure teams and stakeholders are aligned around goals and necessary areas of action. He comments, "Getting IT, cloud, and security teams on board up front helps to ensure that the business problems are addressed during the design phase. Rome wasn't built in a day, so you need to set reasonable goals and milestones. I recommend building foundational controls first including resilience, control effectiveness, logging, and service failover capabilities. Then add additional capabilities over time in future phases."

Metrics are also a vital part of any cloud security initiative. Greg says it is important to ensure you create the right metrics and keep track of them as you are delivering the solution. He comments, "The more you can do with regards to demonstrating value the better the outcome. You want to be able to show how the security controls improve experience and the network resilience. You also want to show the isolation and segmentation capabilities to help drive the organization forward and create the level of mobility that might not have been there before. I recommend showing before and after imagery or graphs to help build the business case that you are in a better place now that solutions have been implemented."

ALWAYS LEARNING

"I try to learn something new each week. As leaders, we need to be continually learning whether it is on a personal, technical, or leadership level. I am always challenging myself to learn something new. The CISO community is also very important. I often have honest conversations with my peers to bounce ideas off and assess risk. Having that support structure in such a high stress environment is important so security can continue to do mature and improve security around the world. The more the community works together, the better we all become."